International Journal of Security and Its Applications
Vol. 12, No. 1 (2018), pp.1-20
http://dx.doi.org/10.14257/ijsia.2018.12.1.01

# Cyber Defense Budget Assessment in Smart Grid Based on Reliability Evaluation Considering Practical Data of HV Substation

Noorollah Fardad[1], Soodabeh Soleymani[2*] and Faramarz Faghihi[3]

[1,2,3]*Department of Electrical Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran*
[1]*n.fardad@srbiau.ac.ir*, [2]*s.soleymani@srbiau.ac.ir*,
[3]*faramarz.faghihi@srbiau.ac.ir*

***Abstract***

*Communication and control in the smart grid without any disturbance is the primary task of High Voltage (HV) substation. The nature of electrical network obliges constructing and operating the functions of substations in remote areas far from urban centers. This can cause increasing of concerns about their security. Thus, HV substation designers have focused on defensive algorithms for decreasing these concerns. This paper deals with four cyber defense approaches, including hardware, software, communication shielded cable, and optimized cable route. The defense budget has been estimated via Fuzzy Analytic Hierarchy Process (FAHP) as a function of hardware, software, and communication shielded cable and optimized cable route. Knowledge and experience of experts help to extract mathematical relations between these four approaches. These relations are the base of optimization of attack and defense budget. In the proposed algorithm, "loss of load expectation (LOLE)" as a reliability index is utilized to optimize cyber defense budget of each part of studying network (one supervisory control and data acquisition (SCADA) center and nine HV substations). By comparing the LOLE with a permitted design threshold value, optimal budget of each item is determined. The accuracy of proposed methods has been validated by implementing to a case study real network.*

***Keywords****: Defense Algorithm, Reliability, Cyber Defense, Shielding, Fuzzy Analytic Hierarchy Process, Loss of Load Expectation*

## 1. Introduction

Cyber-attacks affect the reliability of the power system by changing of messages or signals in communication channels. False status or command signals can lead to tripping circuit breakers of generators, transmission lines and load side [1]. The cyber adversary may manipulate information by false data in grid management database and Remote Terminal Units (RTUs) to push the system toward blackout [2]. For more understanding of cyber intrusion, it is essential to model detection activities.

The attacker uses various methods to identify the system's weak points and take the substation under control with the aim of manipulating Intelligent Electronic Devices (IEDs), injecting false data, interfering with intrusion detection system (IDS) or anomaly detection system (ADS). In this regards, identifying the system's weak points is considered as the main core of successful intrusion, and on the contrary, any shortage in this area is equal to an unsuccessful cyber intrusion. Attackers may not have dominant

Received (June 4, 2017), Review Result (October 25, 2017), Accepted (December 18, 2017)
* Corresponding Author

ISSN: 1738-9976 IJSIA

knowledge over the system's drawbacks before the cyber-attack. Therefore, the attacker analyze the level of substation controllability through probability analysis [3].

Attacker and defender consider optimal policies for the worst assumptions. Moreover, defender shall continue until the threat clearance. It assumes that defense is time-consuming; hence defender shall consider more budget. Defenders shall allocate limited defense budget to achieve maximum resistivity in the smart grid against cyber-attacks, as well as the improved operation of the system with minimum vulnerable points [4].

Cyber-attack for the tripping of breakers and lines in substations may not diagnose unless SCADA center authenticates the measurements based on receiving data from substations [5]. It is essential to define optimum cyber defense schemes minimizing the impact of cyber-attacks.

The short-term and long-term study is performed to mitigate the risk of cyber-attacks. In the short-term analysis, the focus of research is on the intrusion diagnosis and the control strategies prior to any threat to the components. While in the long-term study, researchers concentrate on vulnerability analysis, mitigation and reliability via optimization of the cyber network. To this end, it is recommended to establish cyber defense through firewalls, Virtual Private Network (VPN) and protection from disruptive intrusion [6]. Firewalls should be utilized in a distributed manner in communication channels of substations and external networks to detect the anomaly and to mitigate cyber-attack potentials [7-8].

VPN and router help to improve security measures by secure communication and transfer of information packets between control centers via IEC60870-5-104 TCP/IP [9]. Suppliers have already produced other devices, *e.g.*, gateways and demilitarized zone (DMZ) which include regulation of utilization [10].

The game theory is one of the mathematical models for cyber interaction between attacker and defender. Both of them should maximize their profits in a non-coalitional game. In such a communication, minimum resources should be used in a random sequence by the defender to minimize risk in the power system [11-12]. While various cyber-attacks on the system components impact reliability index [13], risk and reliability analysis are calculated based on load curtailment, so some index has introduced for the reliability of the system under attack [14]. Monte Carlo Simulation (MCS) has been widely utilized to analyze reliability under cyber-attacks [15]. "Loss of load expectation (LOLE)" index via MCS is used to estimate the risk of system situation changing from a normal state to critical condition due to the lack of supply or loss of load initiated by equipment mal-operation [16-17].

This paper presents a cyber-security structure for smart HV substations according to their application and cyber-attack impacts. One may use various methods for cyber defense in HV substation. These methods depend on the form, the amount and the location of vulnerability which should consider in cyber security analysis. Shielding of communication cables is chiefly used to nullify the effects of waves from electromagnetic fields on transferring data. Also, optimized route of communication cables in HV substation will minimize the impacts of electromagnetic interference (EMI) and disturbed field attacks. Electromagnetic interference decreases using conduit in the locations with high-intensity electromagnetic fields. In automation level, hardware such as firewall, VPN, router, switch, and the gateway is used to provide reliable transfer of communication data and to stop any illegal intrusion in communication channels. Besides, software solutions, *e.g.*, high order complexity cryptographic schemes, authentication methods, coding algorithms, help to transfer high volumes of data during detection of attacker intrusion.

The primary goal of this paper is to determine optimal selection of cyber defense equipment for an electric network including HV substation considering reliability which is assessed by LOLE index. The aim of the proposed method is achieving this goal based

 

on the reliability indices of the typical network. LOLE index should compare with a threshold value as a condition criteria for determining defense budget.

The rest of this paper has organized into seven sections. Section 2 encompasses various cyber defense methods in HV substation. Section 3 presents a classification of HV substations according to their application and cyber security status. The next Section formulizes cyber-attack and defense budget. The proposed algorithm is the central core of Section 4 which deals with the evaluation and the optimization of the defensive budget by considering the limitations in HV substation. Simulation of proposed algorithm and analysis of the results will be offered in Sections 6 and 7, respectively.

## 2. Classification of Cyber Defense Methods

Cyber threats have increased due to augmented communication and remote access facilities for substation control. Based on Figure 1, HV substation has different potentials of cyber threats based on the type and application. The location of attackers is a useful factor in vulnerability evaluation of substations in the smart grid. Thus, the utilized defensive algorithm should provide a comprehensive approach to cyber defense and electrical network defense (*i.e.*, physical defense). Main operational methods which increase the security level of HV substation summarize as below.

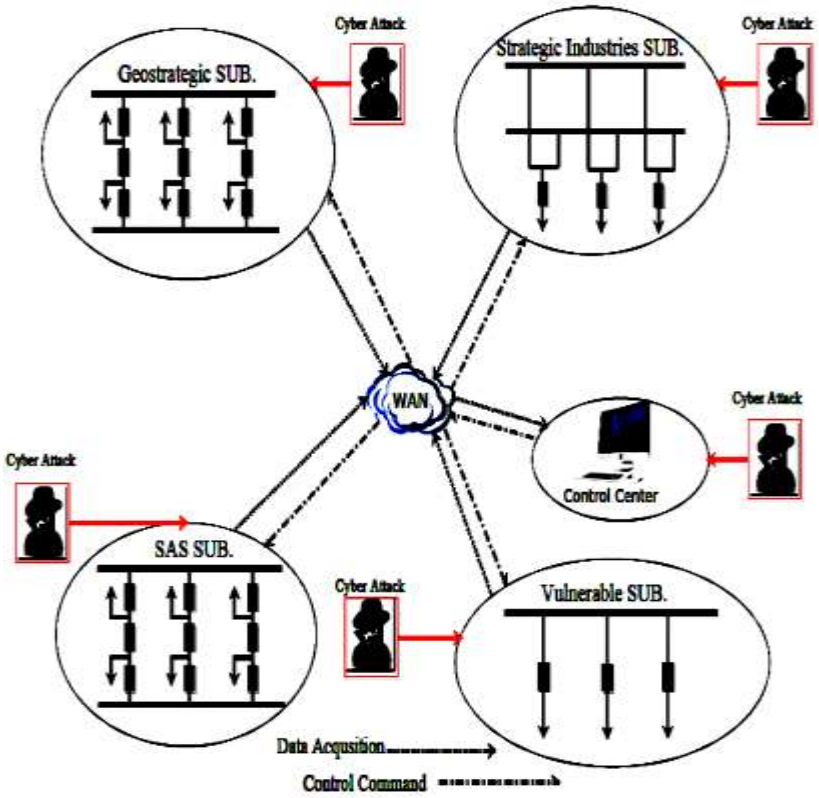


**Figure 1. Potential Cyber Threats Based on their Application**

### 2.1. Shielding

Electromagnetic pulses are fields of energy which may damage electric and electronic circuits through voltage induction, noise hazard, change and degradation of digital information. Unpredicted electromagnetic fields cause high current flow in the network elements and consequently interfere with the operation of sensitive devices via voltage induction in control, protection and communication conductors. The relation of electromagnetic compatibility with stray fields can write as:

 

$$EMC \propto \frac{\sum_{k=1}^{p}\left[\left(B_{pu,max}^{k} - \Delta B_{pu,max}^{k}\right)\times a_{1k} + \left(B_{pu,avg}^{k} - \Delta B_{pu,avg}^{k}\right)\times a_{2k}\right]}{\left[\left(a_{1\max}\right)_{Selected} + \left(a_{2max}\right)_{Selected}\right]} \quad (1)$$

where $B_{avg}$ and $B_{max}$ are average, and a maximum value of interference of the flux density of disturbed fields which is obtained from point to point measurement around victim cables or simulation results respectively. Also, $k$ refers to the number of cables, and $a_1$, $a_2$ are correction factors according to the application where $\alpha_2 \le \alpha_1, \alpha \le 10, 1 \le \alpha_2 \le 5$.

Shielding effectiveness (*SE*) is a parameter which defines as the ratio of the electric field or magnetic field strength at a cable or conductor before and after applying a shield [18].

When an electromagnetic weapon that places inside a bag is close to sensitive electronic circuits, an electromagnetic interference threat can generate. Because of the nature of the threat, disturbance and damage to the equipment can occur without any symptoms. By displacing the strong electromagnetic weapon in the substation, the attacker would be able to disrupt the operation of a variety of devices. Therefore, shielding of control and communication cables in HV substations are used [19].

### 2.2. Software

There are numerous security software solutions in HV substation automation system to increase cyber defense levels. (*e.g.*, Antivirus, Firmware, Intrusion Detection, Anomaly Detection, Firewall and Router software, Coding, Cryptography, Authentication, *etc.*). Hash functions are used to determine any changes in data transmission. The probability of cyber threats that produce noise and fault in information channels makes channel coding is essential to reduce fault rate. In a communication channel with signal power *S* (in Watt) and noise power *N* (in Watt) and channel bandwidth *W* (in Hz), channel capacity is calculated by the Shannon formula as [20]:

$$C = W \log_2\left(1 + \frac{S}{N}\right) \qquad \left(\frac{bits}{second}\right) \quad (2)$$

### 2.3. Hardware

This type of cyber defense solutions for HV substations classifies as below: Firewall: Generally, a firewall is a network security device which filters the traffic that flows into the network. Firewalls not only prohibit illegal communication, but also they allow certified traffic, according to user-defined rules and configuration.

Virtual Private Network (VPN): A VPN uses encryption to provide data confidentiality and develop reliable encrypted communication. Routers, Ethernet switches, gateways are other tools to prevent from unauthorized intrusion.

### 2.4. Optimized Route Selection

Optimized route selection is performed in HV substations based on further assumptions.

(1) The selected route must be far from supply sources of interference fields, *e.g.*, power transformers (2) the shortest path calculated by considering price and voltage drop (3) selected routes should be designed based on minimum EMI especially for switching states to avoid over/under voltage and over current phenomena.

The optimal route for communication cables is calculated by the simulation of interference field intensity (IFI) and identification of field attenuated regions [18].

 

## 3. Classification of HV Substation Based on Cyber Security Consideration

HV substations are used for electricity supplement of the strategic area with a different security level. Therefore they have different priorities in smart power grid as illustrated in Figure 1. One substation may utilize firewall, IDS, and cryptography and the other may just use firewalls. Assessment of substations security levels and their influence on smart power grid allows the attacker to infect desired substations with the purpose of initiating cascading events [21]. It is evident that the increase in security levels will augment the cost. Classification of substations according to their strategic application are summarized as below:

### 3.1. Geostrategic Substation

Geostrategic Substation operates in particular geographic and strategic locations like borders, Iceland, *etc*. Their distance to the urban centers makes them favorable targets for attackers, especially via electromagnetic threats. The dominant methods of cyber defense are communication devices shielding and optimal route selection.

### 3.2. Industrial Strategic Substation

This group includes substations for oil, gas and petrochemical plants, power plants and transmission levels. The increase in the cyber defense budget, especially for hardware and software solutions will strengthen defense levels. Power plant substations which control the network frequency and industrial substations which supply energy of several factories always face the cyber threats.

### 3.3. Substations Based on Control and Automation System

There are two main types of the control system in substations. In the conventional solution, control and monitoring devices concentrate in control room, and copper cables provide communication. In the second solution, substation automation system (SAS) utilizes fiber optic to communicate with smart devices. Due to the use of information technology (IT) in the substation automation, they are susceptible to cyber-attacks, and it is essential that the protective equipment used in them.

### 3.4. Vulnerable Substations

These categories of the substations are vulnerable because they locate under robust disturbance signaling and electromagnetic waves. They have been classified based on the vulnerability level resulting from the number, sensitivity and centralize of communication equipment. The defense budget for these substations includes an optimal route selection of communication cables, shielding, and software solutions, *e.g.*, coding, cryptography, and authentication.

The proposed method calculates the minimum defense budget based on the above classification. Multi-criteria decision making (MCDM) implement via several ways. Fuzzy Analytic Hierarchy Process (FAHP) as one of the most important among them. A complex structure is decomposed into smaller parts, and then they put in a hierarchy structure. The subjective decisions regarding the importance of each variable assign to a defined criteria. Consequently, the most significant variable extract. The hierarchical model of substations for a typical network has three distinct layers as shown in Figure 2.

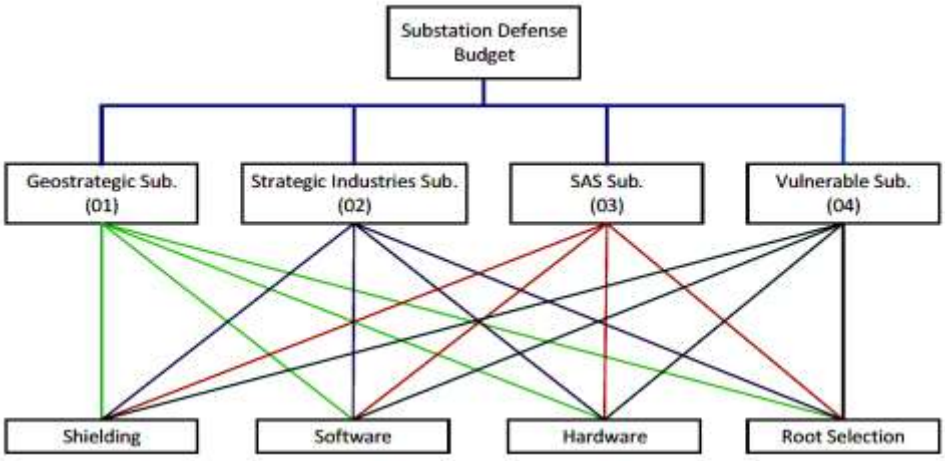


**Figure 2. Hierarchy Tree for Calculation of Substation Defense Budget**

According to the pairwise comparison matrix of criteria and alternative, the weights are assigned based on substations ranking for defense budget allocation as shown in Figure 3. (Appendix for better understanding).

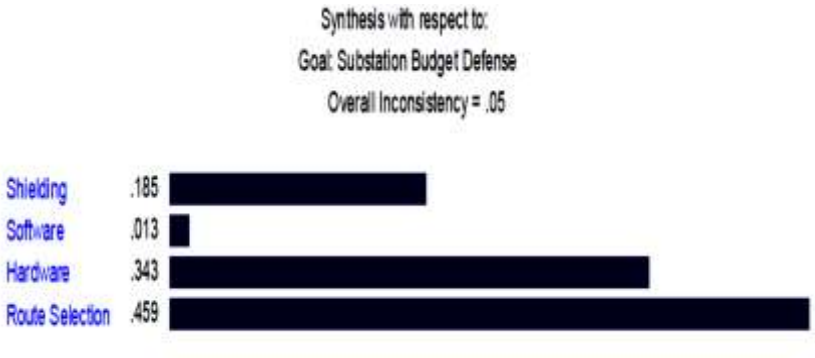


**Figure 3. Final Weight of Alternatives Compared to the Criteria**

## 4. Cyber Attack and Defense Budget Formulation

Cyber-attack has a random nature, so that smart grid operators are not able to predict the time of cyber-attacks. For the system under attack, the attackers can only threaten the system with a probability that depends on the cyber defense devices. A success probability function includes attacker and defender's actions [22-23]. The attacker has attack budget (*BA*) as the attack resource while the defender has a defense budget (*BD*) as the defense resource. With the allocation of *BA* and *BD* to *N* assumption target, the probability of a successful attack calculates. We suppose that cyber vulnerability is the probability of target destruction of investment. Thus attacker increase vulnerability such that (3)

$$P_i^{att}(A_i) = 1 - e^{-\gamma_i A_i} \qquad 0 < P_i^{att}(A_i) \le 1 \tag{3}$$

where $A_i$ is the attack budget allocated to target $i$ by the attackers representing their capability. Where $\gamma_i$ is the vulnerability factor that shows attack complexity level, and it is calculated based on the countermeasures (*i.e.*, defensive actions) in each step of the attack. In equation (3) the success probability of attack is increased by network vulnerability and attack resource considering cyber security rules. In defender

 

perspective, the successful attack probability decreases by defense budget growth, which it has an exponential trend:

$$P_i^{def}(D_i) = e^{-\alpha_i D_i} \qquad 0 < P_i^{def}(D_i) \le 1 \tag{4}$$

Where $D_i$ and $a_i$ are the allocated defense budget and the vulnerability factor, respectively, both from the defender's perspective. The joint probability of a successful attack is produced of equations (3) and (4) for the target ($i$):

$$P_i(A_i, D_i) = \left(1 - e^{-\gamma_i A_i}\right)\left(e^{-\alpha_i D_i}\right) \tag{5}$$

The total risk of the system is:

$$R(A_i, D_i) = \sum_{i=1}^{N} P_i(A_i, D_i).d_i = \sum_{i=1}^{N}\left(1 - e^{-\gamma_i A_i}\right)\left(e^{-\alpha_i D_i}\right).d_i \tag{6}$$

Where $d_i$ is the impact on the target $i$ after a successful attack, it can be as an expected damage of the target $i$. The total risk of desired network has a reverse relationship with defender resource $D_i$, but it is proportional to attacker's resource $A_i$. The objective function defined as below:

$$\min_{D_i}\left[\max_{A_i} R(A_i, D_i)\right] = \min_{D_i}\left[\max_{A_i}\left\{\sum_{i=1}^{N}\left(1 - e^{-\gamma_i A_i}\right)\left(e^{-\alpha_i D_i}\right).d_i\right\}\right] \tag{7}$$

$$\sum_{i=1}^{N} A_i = BA \qquad , h(A_i): \sum_{i=1}^{N} A_i - BA \qquad , A_i \ge 0 \tag{8}$$

$$\sum_{i=1}^{N} D_i = BD \qquad , h(D_i): \sum_{i=1}^{N} D_i - BD \qquad , D_i \ge 0 \tag{9}$$

In order to extract optimal resource allocation that satisfy equations (7-9), the Lagrange multipliers method is used.

$$\mathcal{L}(A_i, D_i, \lambda_1, \lambda_2) = R(A_i, D_i) + \lambda_1\left[h(D_i)\right] - \lambda_2\left[h(A_i)\right] \tag{10}$$

$$\mathrm{L}_{D_i} = \frac{\partial \mathrm{L}}{\partial D_i} = \frac{\partial R(A_i\ D_i)}{\partial D_i} + \lambda_1 = 0 \tag{11}$$

$$\mathrm{L}_{A_i} = \frac{\partial \mathrm{L}}{\partial A_i} = \frac{\partial R(A_i\ D_i)}{\partial A_i} + \lambda_2 = 0 \tag{12}$$

$$\mathrm{L}_{\lambda_1} = \frac{\partial \mathrm{L}}{\partial \lambda_1} = h(D_i) = 0 \tag{13}$$

$$\mathrm{L}_{\lambda_2} = \frac{\partial \mathrm{L}}{\partial \lambda_2} = h(A_i) = 0 \tag{14}$$

Equations (15)-(16) derives from (11) - (12):

$$\ln \lambda_1 - \ln[\alpha_i((1 - e^{-\gamma_i A_i})d_i] + \alpha_i D_i = 0 \tag{15}$$

$$\ln \lambda_2 - \ln[\gamma_i ((e^{-\alpha_i D_i})d_i] + \gamma_i A_i = 0 \quad (16)$$

Using $D_i$ and $A_i$ from relations (15) and (16) and by substituting them in relations (13) and (14), below relationships can be derived.

$$\sum_{i=1}^{N} \left\{ \frac{\ln\left[\alpha_i \left(1-e^{-\gamma_i A_i}\right)d_i\right] - ln\lambda_1}{\alpha_i} \right\} - BD = 0 \quad (17)$$

$$\sum_{i=1}^{N} \left\{ \frac{\ln\left[\gamma_i \left(e^{-\alpha_i D_i}\right)d_i\right] - ln\lambda_2}{\gamma_i} \right\} - BA = 0 \quad (18)$$

The optimal values of $D_i$ and $A_i$ and the Lagrange multipliers $\lambda_1$, $\lambda_2$ will be calculated by solving relations (15) to (18) simultaneously.

## 5. Analysis of Optimal Defense Allocated Budget According to the Practical Data in Substations

The relations of section 4 theoretically define optimal defense and attack allocations. The functional data of HV substation imposes limitations on the cyber defense structure. These constraints lead to mathematical relations which are described in this section to achieve an accurate estimation of optimal values. The total defense budget for each target (*i.e.*, substation) is a function of several variables:

$$D_i = f\left(Sh, Sft\left(cd, cry, aut\right), Hde, Rtsl\right) \quad (19)$$

a) *Sh*: Shielding (i.e. Communication cable shielding)
b) *St*: Software(i.e. cd: coding, cry: cryptography and aut: authentication)
c) *HE*: Hardware equipment (i.e. firewall, VPN switch, router, gateway)
d) *RS*: Route selection

Defense budget values of the above schemes are indicated by $D_{Sh_i}$, $D_{St_i}$, $D_{HE_i}$ and $D_{RS_i}$ respectively.

Total defense budget or $BD = \sum_{i=1}^{N} D_i$ is the defense budget of each solution in target i, therefore BD is calculated as below equation:

$$BD = \sum_{i=1}^{N} d_{1_i}\left(D_{Sh_i}\right) + d_{2_i}\left(D_{St_i}\right) + d_{3_i}\left(D_{HE_i}\right) + d_{4_i}\left(D_{RS_i}\right) \quad (20)$$

Based on the general relation for BD in equation (20) in conjunction with the fuzzy analytic hierarchy process by applying results of the third section, the below coefficients are used to optimize the cyber defense solutions.

$$d_{1_i} = 0.185,\ d_{2_i} = 0.013,\ d_{3_i} = 0.343,\ d_{4_i} = 0.459$$

$$BD = \sum_{i=1}^{N} 0.185\left(D_{Sh_i}\right) + 0.013\left(D_{St_i}\right) + 0343\left(D_{HE_i}\right) + 0.459\left(D_{RS_i}\right) \quad (21)$$

After data collecting from expert persons and completing questionnaires, the curve for relationship between $D_{Sh_i}$, $D_{St_i}$, $D_{HE_i}$ and $D_{RS_i}$ parameters in the pairwise or triple form is drawn. The best equations which can describe those curves give as equations (22)-(24). As far as the authors are aware, there are no equations in this way for good judgment achievement.

 

$$DSft_i = \frac{-10^5}{k_1(DHde_i)} + k_{2?} \tag{22}$$

$$0.02 \le k_1 \le 0.05\ ,\ 2000 \le k_2 \le 3000$$

$$DSft_i = k_{3?}(DSft_i) + k\ \ (Hde_i)^m \tag{23}$$

$$1 \le m \le 3,\ 0.6 \le k_3 \le 0.8,\ 2\times10^{-5} \le k_4 \le 6\times10^{-5}$$

$$DRtsl_i = DSh_i + k_5 (Dsft_i)^{k_6} \tag{24}$$

$$6\times10^4 \le k_5 \le 8\times10^4, 1 \le k_6 \le 2$$

Regarding the relation (21), it can be mention that in a typical substation, based on getting information and experiences of experts, by increasing in hardware defense, the software budget decreases and vice versa. Such approach helps to define the relation of shielding, software, and hardware in relation (23). Communication cables shielding has a specified weight in each substation. Also, type of hardware equipment is well known which lead to the relationship of their budgets. Communication cable route selection and shielding are used to prevent the effects of EMI. However, the optimal route selection will be more effective in this regard. On the other hand, security software also has a smaller budget than these two items; therefore the relation (24) is presented.

LOLE as a necessary reliability index uses in the assessment of the adequacy of the power system. LOLE is the average of days or hours in a specific period in which daily peak load or hourly peak load may go beyond supply. Here, LOLE via MCS is analyzed. The vector $G_{ik}$ indicates the state of supply unit ($i$) in sampling stage $k$ and $m$ is the number of supply units.

$$\{G_{ik}, i = 1, \ldots, m\} \tag{25}$$

For the given load $D$, not supplied demand due to shortages in supply capacity in $K_{th}$ sampling stage is [24]:

$$DNS_k = max\left\{0, D - \sum_{i=1}^{m} G_{ik}\right\}; \tag{26}$$

Reliability index, LOLE, for $NS$ years of sampling is calculated by [24]:

$$LOLE = \frac{\sum_{k=1}^{NS} I_k (DNS_k)}{NS} \times 8760 \left(\frac{hr}{yr}\right) \tag{27}$$

Which $I_k$ is indicator variable:

$$I_k = \begin{cases} 0 & if\ DNS_k = 0 \\ 1 & if\ DNS_k \neq 0 \end{cases}$$

Figures (4) – (5) show the proposed method for reliability analysis. The primary budget defense is considered for each substation and SCADA system according to their importance for studying network. The cyber security designer determines the priorities of substations. MCS approach calculates LOLE, and it compares with the design criteria value. If LOLE does not satisfy the design criteria, the values of the defense budget will increase, and the new LOLE calculate. When LOLE meets the design threshold, the

defense budget is updated according to the real cost values of each defense item. The final budget defense values can be used to design of cyber security of studying network.

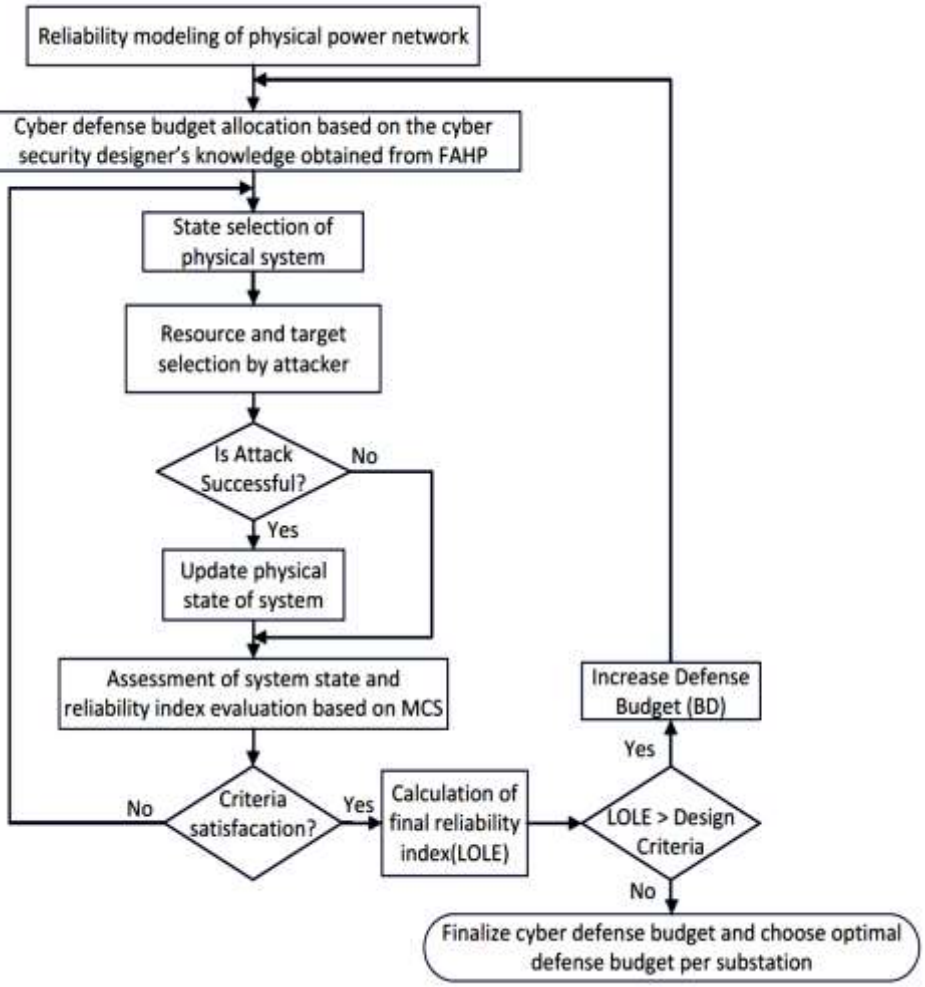


**Figure 4. Flowchart of Proposed Method**

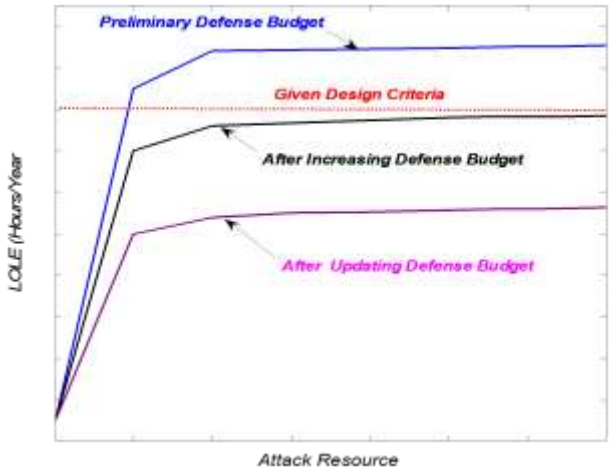


**Figure 5. General Description of Proposed Algorithm for Optimal Budget Allocation**

## 6. Analysis and Simulation of Proposed Algorithm

Figure 6. Shows physical and cyber layers of studying network. The physical system consists of three units of power plant (reliability index is given in Table 1.), a local SCADA system and nine substations to supply the demand. Cyber system consists of user-interface, information and communication technology (ICT) network, protective devices and IEDs (IEC61850 based). Information relating to the coefficients and values of the vulnerability of each node for the investigating system introduce in Table 2.

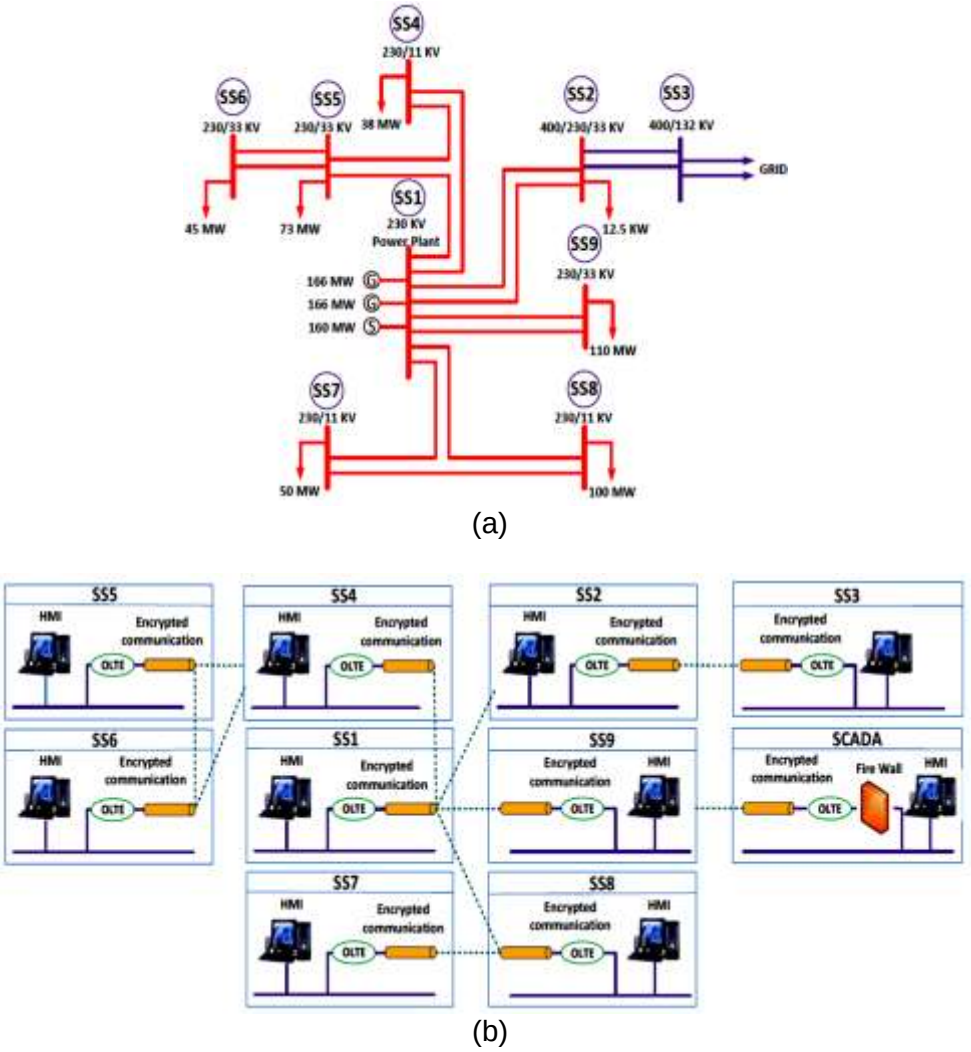


**Figure 6. (a): Connection Diagram of Substations (b): Defensive Solutions for Communication Scheme**

**Table 1. Generating Unit Reliability Data**

| Unit Size(MW) | MTTF(hrs) | TTR(hrs) |
|---|---|---|
| 166 | 960 | 50 |
| 166 | 960 | 50 |
| 160 | 950 | 40 |

Communication and data transferring with a control center and remote access points can be done through hardware and software equipment (*e.g.*, firewall, gateway) installed on SAS.

**Table 2. Coefficients and Cost of Vulnerability for Investigated Network**

| Substation/ Vulnerability | SCADA | SS1 | SS2 | SS3 | SS4 | SS5 | SS6 | SS7 | SS8 | SS9 |
|---|---|---|---|---|---|---|---|---|---|---|
| $d_i$ | 700 | 400 | 200 | 400 | 100 | 200 | 100 | 125 | 150 | 300 |
| $\alpha_i$ | 0.001 | 0.002 | 0.006 | 0.002 | 0.012 | 0.006 | 0.012 | 0.009 | 0.007 | 0.004 |
| $\gamma_i$ | 0.005 | 0.01 | 0.027 | 0.01 | 0.054 | 0.027 | 0.054 | 0.04 | 0.032 | 0.016 |

The investigated network has been selected based on the below assumptions:

- Common oil field
- Near borders geostrategic substations
- Both conventional substation (CS) and distributed control system (DCS)
- Vulnerable to signaling and telecommunication attack

According to the mentioned criteria, one may allocate an initial attack and defense budget such that:

- Control center or SCADA system has a maximum vulnerability due to a cyber attack
- Substations have the second level of vulnerability
- The next challenge of vulnerability is strategic substation
- Substations near oil fields are such a crucial category to be an attractive target for cyber intruders

Based on the above assumptions, as well as the values assumed in Tbale3 for a range of defense budget of each item, including hardware, software, and optimal route of communication cables and shielding, assigning coefficients for equations (22)-(24) for investigating network are shown in Table 5. Cyber security designers can choose initial defense budget of each substation for sample network. The selection method is done according to the designer's knowledge and the security requirements of the studied network, which is described in the third section as shown in Table 5.

**Table 3. Assumption Cyber Defense Expenses of Typical Network**

| Defense Item | Min-max costs based on information extracted from the references($) |
|---|---|
| Hardware equipment (Firewall: 3000$, Gateway: 3000$ ,Router switch: 2000$) | 2000-8000 |
| Related software for firewall, coding, encryption, authentication, … | 1000-2000 |
| Communication cable routing for EMC | 2000-7000 |
| Communication cable shielding | 1000-4000 |

**Table 4. Assumption for Coefficients of Practical Equations in Section 5**

| Coefficient | K1 | K2 | K3 | K4 | K5 | K6 | m |
|---|---|---|---|---|---|---|---|
| **Quantity** | 0.02 | 3000 | 0.7 | $4\times10^{-5}$ | 3 | 1 | 2 |

 

**Table 5. Initial Cyber Defense for Studied Network**

| SCADA/ Substation | Defense Design, Defense Equipment | Actual Budget Defense $(D_1)_i$ ($) | Defense Budget Via equation (21) $(D_2)_i$ ($) |
|---|---|---|---|
| SACDA | Hardware(Firewall),Software | 4000* | 1042** |
| SS1(PP) | Software, Shielding | 2000 | 198 |
| SS2 | Software | 1000 | 13 |
| SS3 | Software | 1000 | 13 |
| SS4 | Software | 1000 | 13 |
| SS5 | Software | 1000 | 13 |
| SS6 | Software | 1000 | 13 |
| SS7 | Software | 1000 | 13 |
| SS8 | Software | 1000 | 13 |
| SS9 | Software | 1000 | 13 |
| | | $BD1=\sum_{i=1}^{N}(D_1)_i$ =14000 $ | $BD2=\sum_{i=1}^{N}(D_2)_i$ =1344 $ |

* Firewall (3000$) +Software (1000$) =4000 $
** according to equation (21): (3000×0.343+1000×0.013) =1042 $

In this case, based on the vulnerability level as well as the importance of each substation, the SCADA center, and SS1 power plant substation have more defense items than the other substations. For SCADA center, firewall and security software are considered in the automation system. For SS1, security software and shielding of communication cables should be noticed. Due to the minimum importance of the other substations, only security software can be applied in their control and automation system, and thus for the investigated network, the total defense budget is 14000 USD. The calculation shows that total optimal budget of 1344 USD could provide the proper level of the defense. Therefore, the reliability index "LOLE" is calculated by 1344 USD based on equation (21). According to research reports and cited references, 2.4 hr/year of loss of load is a useful index of the reliable network [25]. Because of the high priority of selected sample network for this paper, we choose 2 hours/year for LOLE. Based on Table 2, since SS4 and SS6 have the least vulnerability cost, they are allocated to the least defensive budget, then they are applied to calculate the probability of a successful attack and LOLE. Figure 7 illustrates the simulation result of LOLE calculation for different attack resources.

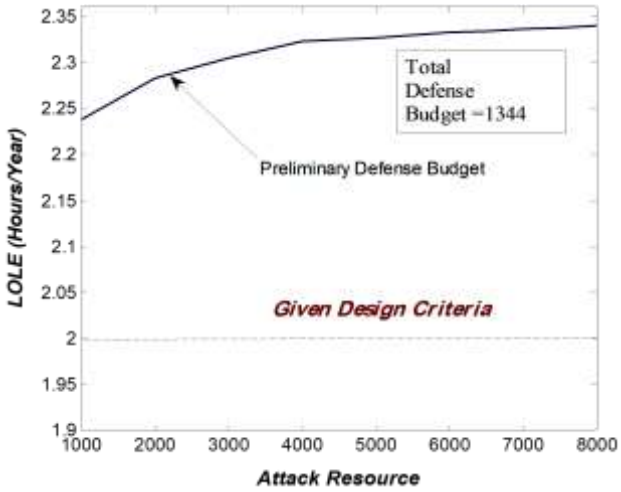


**Figure 7. LOLE Curve with Preliminary Budget Defense**

It is clear that the initial budget does not satisfy the LOLE criteria of 2 hours/year, hence cyber defense budget of substations is increased. The question is that which station for the network has the priority to meet the first increase in budget. In this step, the defense budget of the same substations in the previous step is increased by the designer. Also designer can consider new defense solutions for other substations.

Looking again at the single line diagram of Figure 6 reveals that SCADA center, SS3, and SS9 have the highest priority for the others. Due to the importance of the SCADA center, shielding of communication cables is added to it; thus the size of the security software budget is increased to the maximum amount. For SS9 that provides communication and data transfer route from all substations to SCADA center, security software budget is considered with maximum values. Moreover, due to the connection of SS3 to the national grid, it has the high vulnerability, and the budget of optimal communication cable route is added to SS3. LOLE index is calculated for new budget allocation based on Table 6.

**Table 6. New Cyber Defense Allocation for the Network**

| SCADA/ Substation | Defense Design, Defense Equipment | Actual Budget Defense $(D_1)_i$ (\$) | Defense Budget Via equation (21) $(D_2)_i$ (\$) |
|---|---|---|---|
| SACDA | Hardware (Firewall), Software, Shielding | 6000* | 1240** |
| SS1(PP) | Software, Shielding | 2000 | 198 |
| SS2 | Software | 1000 | 13 |
| SS3 | Software, Optimized cable Route | 4000 | 1390 |
| SS4 | Software | 1000 | 13 |
| SS5 | Software | 1000 | 13 |
| SS6 | Software | 1000 | 13 |
| SS7 | Software | 1000 | 13 |
| SS8 | Software | 1000 | 13 |
| SS9 | Software | 2000 | 26 |
| | | $BD1=\sum_{i=1}^{N}(D_1)_i$ =20000 \$ | $BD2=\sum_{i=1}^{N}(D_2)_i$ =2932 \$ |

* Firewall (3000\$) +Software (2000\$) +Shielding (1000\$) =6000\$
** according to (21): (3000×0.343+2000×0.013+1000×0.185) =1240\$

After increasing the defense budget for the studied network, LOLE values compute. The results compared with the design criteria is given in Figure 8.

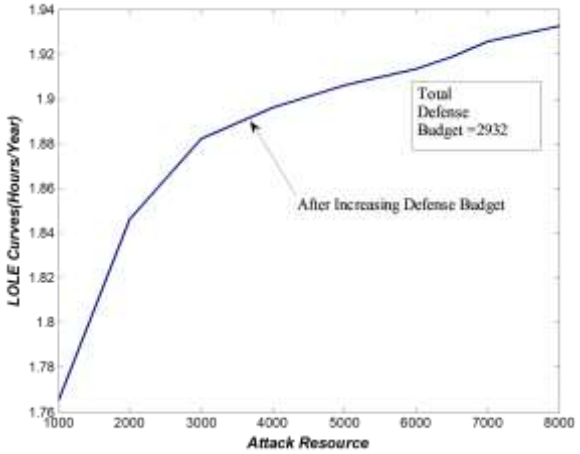


**Figure 8. LOLE for New Cyber Defense Allocation**

 

When LOLE is satisfied by design criteria, the designer will update the defense budget of each substation based on his knowledge and optimal assigned defense budget in the previous step. The results are shown in Figure 9, and Figure 10.

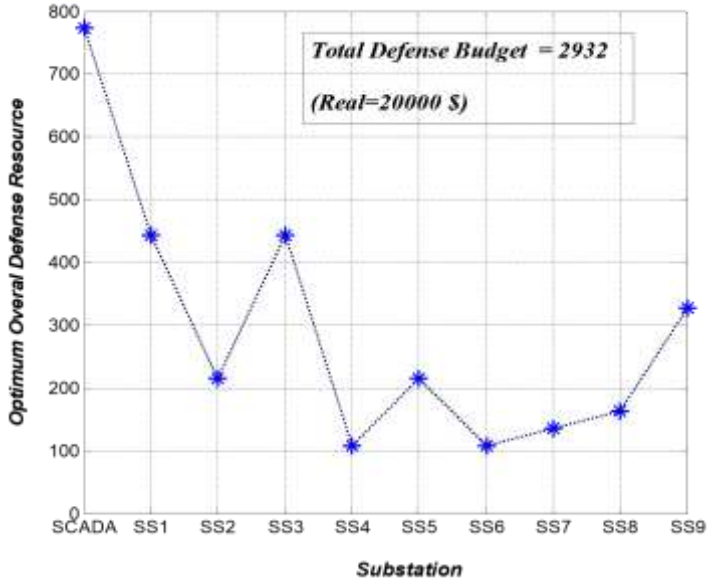


**Figure 9. Optimal Total Defense Budget per Substation**

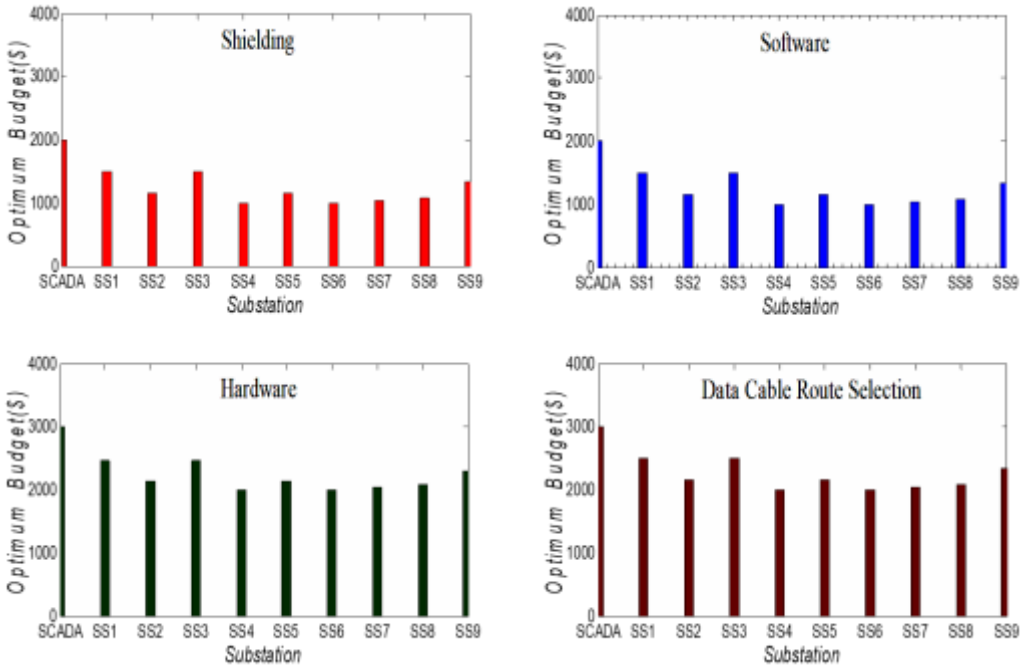


**Figure 10. Optimal Defense Budget per Solution for Each Substation**

Reviewing the allocated optimum budget in Figure 9. and Figure 10. illustrates that the budget is proportional to substation vulnerability level. The budget of SCADA and SS3 substation increased in the previous step, however, in the last iteration, the defense budget will reduce to them. Due to their importance, this budget is kept constant, and then the other substations defense budget is increased. New allocated budgets are given in Table 7.

**Table 7. Cyber Solution Budget Allocation for Each Solution**

| SCADA/ Substation | Defense Design, Defense Equipment | Actual Budget Defense $(D_1)_i$ ($) | Defense Budget Via equation (21) $(D_2)_i$ ($) |
|---|---|---|---|
| SACDA | Hardware (Firewall), Software, Shielding | 6000 | 1240 |
| SS1(PP) | Software, Shielding | 4500 | 488.5 |
| SS2 | Software | 3000 | 211 |
| SS3 | Software, Optimized cable Route | 4000 | 1390 |
| SS4 | Software, Shielding | 2000 | 198 |
| SS5 | Software, Shielding | 3000 | 211 |
| SS6 | Software, Shielding | 2000 | 198 |
| SS7 | Software, Shielding | 2000 | 198 |
| SS8 | Software, Shielding | 2000 | 198 |
| SS9 | Software, Shielding | 3600 | 322 |
| | | $BD1=\sum_{i=1}^{N}(D_1)_i$ =32100 $ | $BD2=\sum_{i=1}^{N}(D_2)_i$ =4654.5 $ |

Security software and communication shielded cable consider in SS2 and SS9 substations with the maximum defense budget. Security software and communication shielded cables are considered for (SS4-SS8). The budget of 1600 USD for communication shielded cable in addition to previous 2000 USD of software for SS9 is increased. Assuming there is no need to implement a practical defense solution in a network, the budget would allocate to other solutions. In case each item's budget violates the assumed ranges, it would be modified accordingly. These modifications lead the calculations to the total budget of 4654 USD which keep LOLE constraints, although the budget may be updated, indeed depends on the network owners (*i.e.*, overall budget of cyber defense). The updated defense budget values in Table 7 are again used to calculate final LOLE curve as shown in Figure 11.

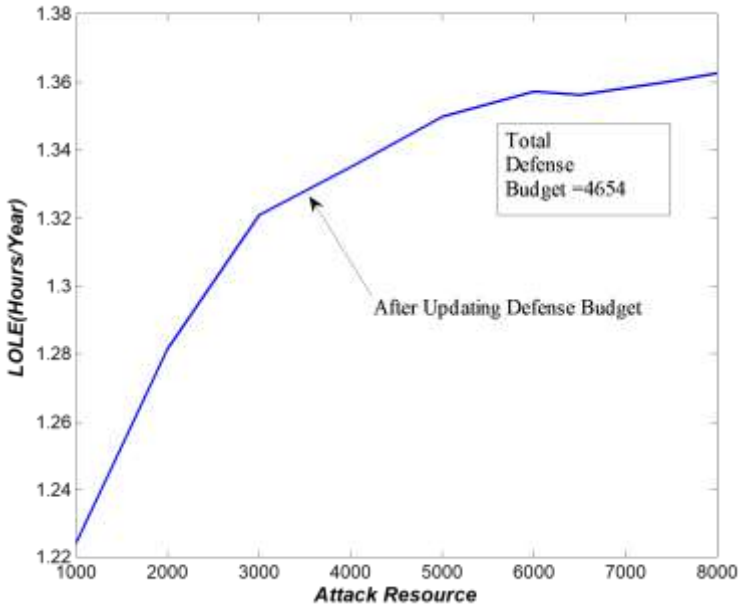


**Figure 11. LOLE Calculation after Updating Budget Defense**

 

According to the recommended defense budget values in the simulation results satisfying the allowable LOLE and about the applied real defensive equipment, the suitable total budget for security design of studied network will be 32100$. It is possible to achieve a different allocation of the defense budget in the network depending on the importance of various parts of network and designer's thoughts. Figure 12 shows the probability of successful attack at every defense budget. By increasing attack resources and assigning a minimum defense budget, the probability of a successful attack is increased. It is found that after allocation of 3000$ for attack resource and each three defense budget, the probability rate of successful attack almost will be constant. The reason for this matter is that the target of an attacker is specific and he will be able to make a successful attack unless the defender reduces the probability of successful attack by increasing the defense budget.

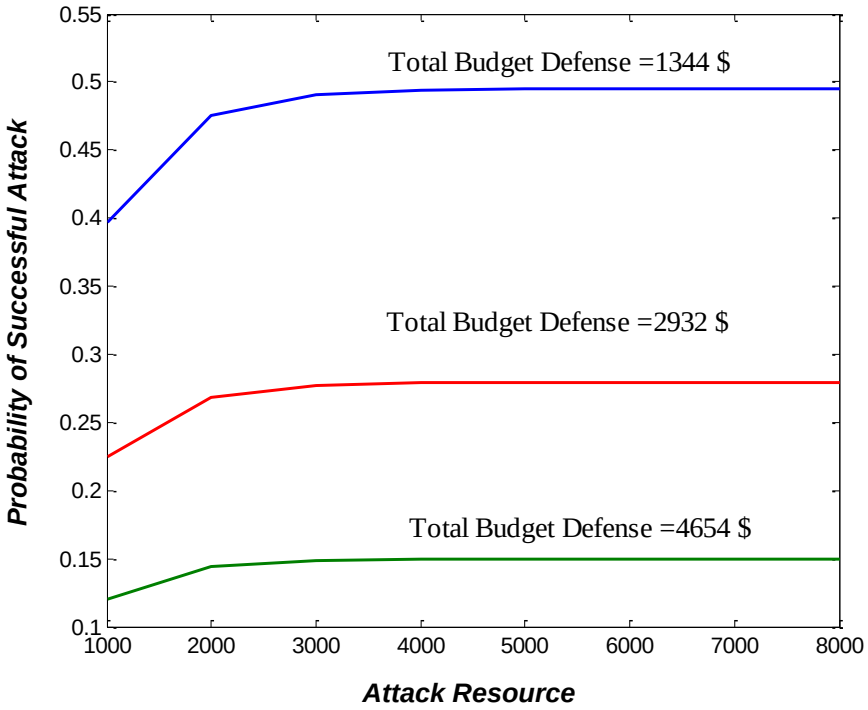


**Figure 12. Probability of Successful Attack with Attack and Defense Budget**

## 7. Conclusions

Type of cyber defense solutions, the arrangement in SCADA center, and HV substations of smart grid play the main role in secure operation and reliability index. In this paper, an efficient method including Fuzzy Analytic Hierarchy Process and mathematical relations based on knowledge and experience of experts result in the optimum defense budget for SCADA and HV substations. Calculation of optimal cyber budget for each part of the smart network is performed based on a permitted level of LOLE via proposed algorithm. With considering the optimal cyber defense solution, the success probability of attack will be minimized. Thanks to the proposed algorithm, cyber defense budgets could be systematically allocated to the smart grid according to the voltage level and substation topology.

# Appendix

Criteria weights

| | Geostrategic | Strategic Industries | SAS | Vulnerable |
|---|---|---|---|---|
| Geostrategic | (1,1,1) | (1,1,1) | (0.333,0.5,1) | (0.25,0.333,0.5) |
| Strategic Industries | (1,1,1) | (1,1,1) | (0.2,0.25,0.333) | (0.166,0.2,0.25) |
| SAS | (1,2,3) | (3,4,5) | (1,1,1) | (0.25,0.333,0.5) |
| Vulnerable | (2,3,4) | (4,5,6) | (2,3,4) | (1,1,1) |

Alternative weights relative to Geostrategic criteria

| Geostrategic | Shielding | Software | Hardware | Route Selection |
|---|---|---|---|---|
| Shielding | (1,1,1) | (3,4,5) | (1,1,1) | (0.333,0.5,1) |
| Software | (0.2,0.25,0.333) | (1,1,1) | (0.2,0.25,0.333) | (0.142,0.166,0.2) |
| Hardware | (1,1,1) | (3,4,5) | (1,1,1) | (0.333,0.5,1) |
| Route Selection | (1,2,3) | (5,6,7) | (1,23) | (1,1,1) |

Alternative weights relative to Strategic Industries criteria

| Strategic Industries | Shielding | Software | Hardware | Route Selection |
|---|---|---|---|---|
| Shielding | (1,1,1) | (1,1,1) | (1,1,1) | (0.333,0.5,1) |
| Software | (1,1,1) | (1,1,1) | (0.2,0.25,0.333) | (0.333,0.5,1) |
| Hardware | (2,3,4) | (3,4,5) | (1,1,1) | (1,2,3) |
| Route Selection | (1,2,3) | (1,2,3) | (0.333,0.5,1) | (1,1,1) |

Alternative weights relative to SAS criteria

| SAS | Shielding | Software | Hardware | Route Selection |
|---|---|---|---|---|
| Shielding | (1,1,1) | (1,2,3) | (0.333,0.5,1) | (0.333,0.5,1) |
| Software | (0.333,0.5,1) | (1,1,1) | (0.2,0.25,0.333) | (0.333,0.5,1) |
| Hardware | (2,3,4) | (3,4,5) | (1,1,1) | (1,2,3) |
| Route Selection | (1,2,3) | (1,2,3) | (0.333,0.5,1) | (1,1,1) |

Alternative weights relative to Vulnerable Substations criteria

| Vulnerable | Shielding | Software | Hardware | Route Selection |
|---|---|---|---|---|
| Shielding | (1,1,1) | (1,2,3) | (0.333,0.5,1) | (0.333,0.5,1) |
| Software | (0.333,0.5,1) | (1,1,1) | (0.25,0.333,0.5) | (0.166,0.2,0.25) |
| Hardware | (1,1,1) | (2,3,4) | (1,1,1) | (0.333,0.5,1) |
| Route Selection | (1,2,3) | (4,5,6) | (1,2,3) | (1,1,1) |

# References

[1] Y. Zhang, L. Wang, Y. Xiang and C. W. Ten, "Reliability Evaluation with SCADA Cybersecurity Considerations", IEEE Transactions on Smart Grid, vol. 6, no. 4, **(2015)**, pp. 1707-1721.
[2] H. Hosseini, S.M.T Bathaee, A. Abedini, M. Hosseina and A. Fereydunian, "Defending false data injection attack on smart grid network using neuro-fuzzy controller", Journal of Intelligent & Fuzzy Systems, vol. 27, no. 3, **(2014)**, pp. 1457-1467.
[3] Y. Chen, J. Hong and C. Ching Liu, "Modeling of Intrusion and Defense for Assessment of Cyber Security at Power Substations", IEEE Transactions on Smart Grid, vol. PP**, (2016)**, pp. 1-13.
[4] L. Wei, A.I. Sawart, W. Saad and S. Biswas, "Stochastic Games for Power Grid Protection against Coordinated Cyber-Physical Attacks", IEEE Transactions on Smart Grid, vol. PP, **(2016)**, pp. 1-11.
[5] Z. Li, M. Shahidehpour, A. Alabdulwahab and A. Abusorrah, "Bi-level Model for Analyzing Coordinated Cyber-Physical Attacks on Power Systems", IEEE Transactions on Smart Grid, vol. 7, no. 5**, (2016)**, pp. 2260-2272.
[6] C. Wang and Y. Hou, "Reliability-Based Updating Strategies of Cyber Infrastructures", Power & Energy Society General Meeting, Denver, USA, **(2015)**.
[7] S. S. Wu, C.C. Liu and A. Stefanov, "Distributed Specification-Based Firewalls for Power Grid Substations", Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), Istanbul, Turkey, **(2014)**.

 

[8] C.C. Liu, A. Stefanov, J. Hong and P. Panciatici, "Intruders in the Grid", IEEE Power and Energy Magazine, vol. 7, no. 1, **(2011)**, pp. 58-66.
[9] P. Jafary, S. Repo and H. Koivisto, "Secure Communication of Smart Metering Data in the Smart Grid Secondary Substation", Innovative Smart Grid Technologies - Asia (ISGT ASIA), Bangkok, Thailand, **(2015)**.
[10] K. Stouffer, J. Falco and K. Kent, "Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security-Recommendations of the National Institute of Standards and Technology", NIST Standard Special Publication 800-82, **(2006)**.
[11] Z. Ismail, J. Leneutre, D. Bateman and L. Chen, "A Game-Theoretical Model for Security Risk Management of Interdependent ICT and Electrical Infrastructures", IEEE 16th International Symposium on High Assurance Systems Engineering (HASE), Daytona Beach Shores, USA, **(2015)**.
[12] K. Farraj, M. Hammad, A. Daoud and D. Kundur, "A Game-Theoretic Control Approach to Mitigate Cyber Switching Attacks in Smart Grid Systems", IEEE International Conference on Smart Grid Communications (SmartGridComm), Venice, Italy, **(2014)**.
[13] Y. Zhang, L. Wang and W. Sun, "A Preliminary Study of Power System Reliability Evaluation Considering Cyber Attack Effects", Power and Energy Society General Meeting (PES), Vancouver, Canada, **(2013)**.
[14] N. Nezamoddinia, S. Mousavianb and M. E. Kantarci, "A risk optimization model for enhanced power grid resilience against physical attacks", Electric Power Systems Research, vol. 143, **(2017)**, pp. 329–338.
[15] J. Stamp, A. McIntyre and B. Richardson, "Reliability impacts from cyber-attack on electric power systems", Power Systems Conference and Exposition, Seattle, USA, **(2013)**.
[16] Z. Shahooei, M. Fotuhi-Firuzabad and A. Abbaspour, "Reliability improvement of power system utilizing BESS with wind farm", IEEE 15th International Conference on Environment and Electrical Engineering (EEEIC), Rome, Italy, (**2015)**.
[17] F. Farzan, M. A. Jafari, D. Wei and Y. Lu, "Cyber-related risk assessment and critical asset identification in power grids", Innovative Smart Grid Technologies Conference (ISGT), Washington, USA, (**2014)**.
[18] V. Abbasi, H. Heydari and F. Faghihi, "Heuristic mathematical formulations and comprehensive algorithm for optimal decision making for power system cabling", Scientia Iranica, vol. 19, no. 3, **(2012)**, pp. 707-720.
[19] "High-Impact, Low-Frequency Event Risk (HILF) to the North American Bulk Power System", Jointly-Commissioned Summary Report of the North American Electric Reliability Corporation and the U.S. Department of Energy, **(2009)**.
[20] S. Benedetto, E. Biglieri and V. Castellani, "Digital Transmission Theory", Englewood Cliffs, NJ: Prentice Hall, **(1987)**.
[21] S.K. Khaitan, J.D. MC calley and C.C. Liu, "Cyber Physical Systems Approach to Smart Electric Power Grid", Springer, **(2015)**.
[22] W. I. Al Mannai and T. G. Lewis, "A general defender-attacker risk model for networks", The Journal of Risk Finance, vol. 9, no. 3, **(2008)**, pp. 244–261.
[23] Y. Zhang, L. Wang and Y. Xiang, "Power System Reliability Analysis with Intrusion Tolerance in SCADA Systems", IEEE Transactions on Smart Grid, vol. 7, no. 2, **(2015)**, pp. 669-683.
[24] R. Billinton and W. Li, "Reliability Assessment of Electric Power Systems Using Monte Carlo Methods", Springer Science Business Media, **(1994)**.
[25] A. Almutairi, M.H. Ahmed and M.M.A. Salama, "Probabilistic generating capacity adequacy evaluation: Research roadmap", Electric Power System Research, vol. 129, **(2015)**, pp. 83-93.

## Authors

**Noorollah Fardad**, he obtained the B.Sc. degree in Electrical Engineering from Shahid Chamran University of Ahvaz, Iran, in 1995 and then an M.Sc in Electrical engineering from Tarbiat Moddaress University, Tehran, Iran, in 2000. PhD student at Science and Research Branch, Islamic Azad University. His research interests are Smart Grid, Renewable Energy, Digital Substation protection and control and cyber security.

 

**Soodabeh Soleymani**, she obtained the B.Sc. degree in Electronic Engineering, Sharif University of Technology, Tehran, Iran, in 2000, and then an M.Sc in Electrical Engineering, Sharif University of Technology, Tehran, Iran, in 2002. Ph.D. in Electrical Engineering, Sharif University of Technology, Tehran, Iran, in 2007 Faculty member of Science and Research Branch, Islamic Azad University. Her research interests are power system operation and planning, Smart Grid and cyber security.

**Faramarz Faghihi**, he obtained the B.Sc. degree in Electrical Engineering from university of Tehran, Iran, in 2000 and then an M.Sc in communication engineering from Imam Hossein University, Tehran, Iran, in 2002. A Ph.D. in current injection transformer optimization at IUST in 2008.Faculty member of Science and Research Branch, Islamic Azad University. His research interests are EMC, Transformers, Renewable Energy and Superconductors, Smart Grid and cyber security.