ATLANTIS PRESS

Advances in Computer Science Research, volume 62

2nd Joint International Information Technology, Mechanical and Electronic Engineering Conference (JIMEC 2017)

Quantitative Assessment Of General Cyber-Attack And Optimal Strategy-Selection Modelling In CPPS

LI Baojie*, LU Yuxin, ZENG Xiaoming, CHEN Yufei, ZENG Xiangfeng, HE Weisheng

State Key Laboratory of Electrical Insulation for Power Equipment,
Xi'an Jiaotong University, Xi'an,
Shaanxi Province, China, 710049
** libaojie@stu.xjtu.edu.cn*

Keywords: Cyber-attack; Quantitative assessment; Strategy-selection; Cyber-Physical Power System; ADG;

Abstract

Recent years, an explosion of cyber-attack accidents once more sound the alarm on the significance of cyber-security issue. For the sake of establishing robust panoramic defense architecture in modern Cyber-Physical Power System (CPPS), an effective and quantitative vulnerability assessment of CPPS is in desperate demand. Consequently, based on the detailed induction and analysis of general framework of cyber-attack, a quantitative assessment method is proposed in the paper from the aspects of both attackers and defenders. In the first place, the probability of selecting access point from the attacker's view is quantized through the scoring of the three properties of information security, the penetration difficulty and the impact of vulnerability. Then, the impact assessment of defender and attacker strategies is discussed via the analysis of both positive and negative aspects. Afterwards, by means of the solving the linear programming issue, the optimal determination of strategy-selection is realized via Nash Equilibrium of Mixed Strategy(NEMS) algorithm. The reasonability of the proposed assessment framework together with future research work are demonstrated at the end of paper.

1 Introduction

The cyber-security issue has attracted increasing attention from researchers and system managers as the occurrence of severe cyber-attack accidents towards the Cyber-Physical Power System (CPPS) has experienced explosive growth in recent years. In 2010, the Supervisory Control And Data Acquisition (SCADA) system of Iranian nuclear facility was invaded and heavily destroyed by the "Stuxnet" virus [1]. On December 23, 2015, due to the attack of malicious code "Black Energy", the Ukrainian power grid suffered serious power outages, which was considered as the first cyber-attack accident against grid infrastructures [2]; Besides, on 25 January, 2016, the Israel electricity administration was also attacked by Ransomware blackmail software [3], fortunately the virus was detected and eliminated thanks to the timely and efficient defense strategies.

On encountering severe challenges, the CPPS longs for efficient methods for the assessment of vulnerability and the modelling of attack procedure so as to optimize the defense strategy as far as possible. According to the attack and defense context, both sides make individual decisions of strategies while questing for maximum payoff, the procedure of which could therefore be considered as the interaction of two players in non-cooperative strategic game [3]. Various research have been dedicated to the vulnerability assessment, like [4-5] proposed a common vulnerability scoring system (CVSS), [6] presents a unified formalism for CPS modelling, however most of these research require high computational power in networks which is beyond the capacity of realistic application, besides, the interaction between the attacker and defender is ignored, hence authentic assessment fails to be fully achieved.

This paper therefore proposes an improved quantitative technique of cyber-attack assessment on fully considering the integrity, availability and confidentiality property of information security at first, then adopts the non-cooperative attack-defense game (ADG) model to establish the impact matrix of different strategies, afterwards employs the Nash Equilibrium [7] algorithm to solve the linear programming issue and obtain the optimal selection results of strategies from both attacker and defender aspects.

The rest of the paper is organized as follows. Section Ⅱ presents the general cyber-attack framework. Section Ⅲ demonstrates the methodology of quantitative assessment. Section Ⅳ states the optimal modelling of strategy-selection. Section Ⅴ concludes the performance of proposed methods and highlights several key points in further study.

2 General cyber-attack framework

This section briefly introduces the classification, general modes and common influence of cyber-attack.

2.1 Classification of Cyber Attack

According to the coverage of influence, the attack generally can be classified into three types: Wide-area Attack (WAA), Neighbourhood-area Attack (NAA) and Individual-Customer Attack (ICA), with detailed relative attributes shown in Tab.1.

2.2 Modes of Cyber Attack

General cyber kill-chain can be divided into two stages-the invasion stage and the attack stage (Fig.1). For launching a high level of attack, attackers have to follow the steps of the two stages in the mode. Meanwhile, the attack traces of hackers can also be identified by the target defense system according to the steps.

	WAA	***NAA***	***ICA***
Coverage	100 km	10km	100m
Data transmission	10M-1G bit/s	0.1M-10M bit/s	up to 100K bit/s
Common Targets	Power and control device	Substation, Centre of distribution	Smart meter, Electric car
Communication	Fiber optic, WiMAX, satellite	ZigBee, PLC, DSL, cable	Wi-Fi, Bluetooth, Internet

Table 1: Classification of attack from influence coverage

Stage 1: First, attackers obtain the organizational structure and vulnerability information of the target system by means of prior field or network investigations, and then select the malware type and carrier to make the attack weapon, which will be delivered into the target system randomly or deliberately through social engineering means based on the locating information of the target system. Once the user is trapped, the malware will be released and implanted immediately, which then expand and permeate horizontally based on the infected workstations, in the meantime build up secluded communication channel with the attacker through the vulnerabilities or back doors. During the whole process, the malware collect certificates constantly and establish persistent connection of access, all of which are prepared for launching the attack of Stage 2.

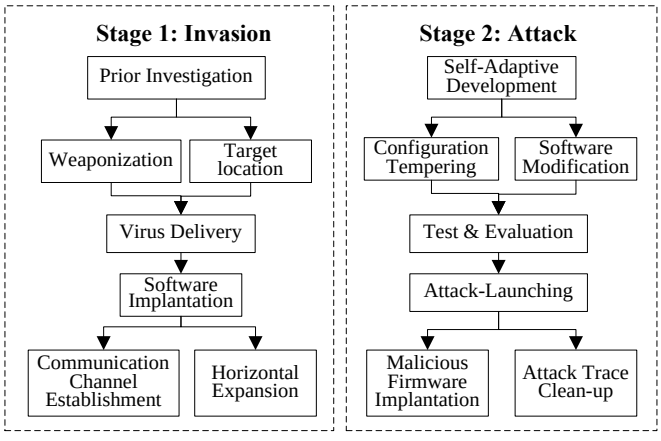

Figure 1: Common modes of cyber-attack

Stage 2: Based on the highly self-adaptability, the implanted malware develops rapidly via local connections and certificates obtained in the previous stage in the whole system environment. Attackers tamper the configuration setting of existing components as to achieve the interaction with the power distribution management system; on the other side, aiming at serial interfaces, develop specific destructive firmware. Prior to the final whistle, professional hacker team will commission careful tests and evaluation of the system controlled. During all-out offensive, the attackers employ the local software to obtain the direct control rights of the target infrastructure, and then modify the operating parameters or directly destroy the system in order to cause outages of facilities. Afterwards, the attackers implant the firmware specially developed in advance into specific command channels as to prevent the recovery of infrastructures, then clean up the system logs and overwrite the Master Boot Record (MBR), finally erase critical files or force shutdown of the target system.

2.3 Impact of Cyber Attack

Generally, an accomplished cyber-attack will cause violation of three properties of information security, including integrity, availability and confidentiality. Loss of integrity renders attackers the ability to modify control commands or measurement data; Loss of availability results in the loss of control over data-collection of remote power devices; Loss of confidentiality results in the divulgement of critical information like password of administrator, private encryption keys etc.

For the sake of quantitative assessment of attack, the impact level of losing the property and the corresponding detailed description are shown in Tab.2.

Property	***Level***	***Description***
I_{int}	High	Complete loss of integrity or protection. Attackers could modify any files protected or use malicious modification to achieve serious consequence.
	Low	Modification of some data is possible, but the consequence or the amount of modification is constrained.
I_{avail}	High	Sustained or persistent loss of availability. Attackers could fully deny access to resources, or prohibit novel connections even when fail to disrupt existing ones.
	Low	Reduced interruptions in availability. Attackers are incapable to completely deny service to legitimate users.
I_{conf}	High	All resources are divulged to attackers or only some critical information is disclosed
	Low	Access to some restricted information is obtained, but attacker does not have control over kind or degree.

Table 2: Definition of impact level of three properties

3 Quantitative assessment of cyber-attack

In view of the general attack framework discussed above, this section proposes a quantitative effectiveness assessment of the cyber-attack, including the selection of penetration point

from the attacker's view and the comprehensive assessment of impact of both defending and attack strategies.

3.1 Selection of penetration point

Generally speaking, the selection of penetration point of Advanced Persistent Threat (APT) attack always carefully takes the feature of target and the complexity of attack into consideration, including the following issues as shown in Tab.3 with corresponding quantitative description.

Aspects	*Factor*
Feature of target	Impact of target when penetrated successfully
	Pervasiveness of target system or configuration
Complexity of attack	Estimated attack time
	Cost of attack

Table 3: Factors considered in selecting penetration point

The levels of penetration difficulty D_{attack} is scored in Fig.2, in which lower value denotes more difficult attack, higher value denotes easier attack. The level *easy* means that attackers can always exploit the vulnerability at any time, *difficult* implies that successful attack depends on condition beyond the attacker's control. Detailed definition of D_{attack} level mainly relies on several factors, including physical protection, attack-time and distance of attack as demonstrated in Tab.2.

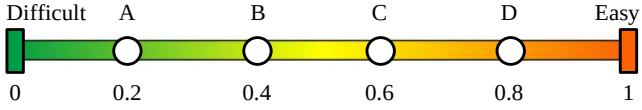

Figure 2: Levels and scoring of penetration difficulty D_{attack}

Levels	*A*	*B*		*C*		*D*
Perfect physical protection	Y	Y	Y	N	N	N
Long-term attack time	Y	Y	N	Y	N	N
Only local access	Y	N	Y	N	Y	N

Table 4: Definition of penetration difficulty

The impact of vulnerability i (V_i) in device n after being successfully penetrated denoted as $I_{\text{vul,i}}$ depends on various factors with the form as (1).

$$I_{vul,i} = \boldsymbol{\beta}_i \times \boldsymbol{I}_n^{\mathrm{T}} \tag{1}$$

$$\boldsymbol{\beta}_i = [\beta_{\text{int},i}, \beta_{\text{avail},i}, \beta_{\text{conf},i}] \tag{2}$$

$$\boldsymbol{I}_n = [I_{\text{int},n}, I_{\text{avail},n}, I_{\text{conf},n}] \tag{3}$$

where, $\boldsymbol{\beta}_i$ represents a vector of three Boolean variables with the value 1 or 0, which denotes whether the exploitation of V_i introduce the loss of integrity, availability or confidentiality; Vector $\boldsymbol{I}_n$ indicates the impact on target system n after the damage of the three properties aforementioned, the actual value of which depends on the topological structure in CPPS.

Based on the quantitative analysis of $I_{\text{vul},i}$, the probability of selection of V_i from the view of attacker could consequently be calculated as (4), in which the ϕ_{v} denotes the assembly of vulnerabilities in target system.

$$P_{\text{vul},i} = \frac{I_{\text{vul},i} * D_{\text{attack},i}}{\sum_{j \in \phi_{\text{v}}} (I_{\text{vul},j} * D_{\text{attack},j})} \times 100\% \tag{4}$$

3.2 Assessment of defending strategy

When the penetration of system is achieved, the attackers consider next-step exploitation on collecting constantly certificates and privileges of legitimate users. In the meantime, the defenders consider proper strategies to improve the reliability of the CPPS, the whole procedure of which exactly conforms to the principle of double-person ADG model. Nevertheless, due to the increasingly higher requirement of real-time data-transmission and dynamic analysis, the defence strategy will inevitably introduce more or less opposite forces in the performance of power system.

The positive impact of defense strategy is conducted to improve the security properties of target system, such as, the employment of user interaction with password authentication could enhance the data integrity, the installation of vulnerability patch contributes to the data confidentiality etc., all of which could be concluded as follows:

$$U_{\text{pos},j}^{\text{d}}(S_k^{\text{d}}) = (\boldsymbol{\beta}_j \wedge \boldsymbol{\gamma}_{k,j}) \times \boldsymbol{I}_{\text{vul},j}^{\text{T}} * D_{\text{attack},j} \tag{5}$$

$$\boldsymbol{\gamma}_{k,j} = [\gamma_{k,j}^{\text{int}}, \gamma_{k,j}^{\text{conf}}] \tag{6}$$

$$\boldsymbol{I}_{\text{vul},j}^{\text{T}} = [I_{\text{int},j}, I_{\text{conf},j}] \tag{7}$$

where, $U_{\text{pos},j}^{\text{d}}(S_k^{\text{d}})$ denotes the positive impact using strategy S_k^{d} against the attack of vulnerability j (V_j), $\boldsymbol{\gamma}_{k,j}$ represents a vector with two influence factors for reducing the impact of losing the integrity and confidentiality, respectively, as shown in (6).

For the sake of improving the reliability of CPPS, it is unavoidable for the defence strategy to employ encryption techniques, which will certainly bring in negative effect on real-time monitoring and response due to lack of computational capability in most of remote terminal units, consequently the property of data availability is damaged, described as follows:

$$U_{\text{neg},j}^{\text{d}}(S_k^{\text{d}}) = \sum_{i \in \phi_k} I_{\text{avail},j} \times \gamma_{\text{k},i}^{\text{avail}} \tag{8}$$

In (8), the $U_{\text{neg},j}^{\text{d}}(S_k^{\text{d}})$ represents the negative impact using S_k^{d}, $\gamma_{\text{k},i}^{\text{avail}}$ denotes the adverse influence on any device i which belongs to the assembly ϕ_k of all effected devices by strategy k.

Additionally, the complexity of defence strategy will as well augment the difficulty and cost of employment, which is relatively another negative impact on the CPPS. Considering all aspects, the total impact of defence strategy can be therefore denoted as:

$$U_j^{\mathrm{d}}(S_k^{\mathrm{d}})=(U_{\mathrm{pos},j}^{\mathrm{d}}(S_k^{\mathrm{d}})-U_{\mathrm{neg},j}^{\mathrm{d}}(S_k^{\mathrm{d}})*\theta_{\mathrm{impact}})*\theta_{\mathrm{act}} \quad (9)$$

$$\theta_{\mathrm{impact}}=\frac{I_{\mathrm{vul},j}}{\sum_{i\in\phi_{\mathrm{v}}} I_{\mathrm{vul},i}} \quad (10)$$

where, θ_{impact} refers to the impact ratio of V_j in the assembly of vulnerabilities ϕ_{v}, θ_{act} represents the actionability of S_k^{d}.

3.3 Assessment of attack strategy

On the basis of quantitative assessment of defence strategy, the utility $U_{\mathrm{attack,j}}$ of prochain attack strategy S_j^{a} aimed at vulnerability j when the S_k^{d} is adopted could therefore be demonstrated as follows:

$$U_{\mathrm{attack}}(S_j^a,\ S_k^{\mathrm{d}})=(I_{\mathrm{vul},j}-U_j^{\mathrm{d}}(S_k^{\mathrm{d}}))*D_{\mathrm{attack},j} \quad (11)$$

which is based on the impact difference between status of successful penetration and improvement of protection by the defenders, besides the attribute of attack difficulty is as well considered to assess the impact of attack strategy.

4 Optimal modelling of strategy-selection

Based on the quantitative assessment of attack and defense strategy analysis above, this section presents a non-cooperative ADG model and the corresponding linear programming algorithm to achievement optimal selection of strategy.

4.1 Non-cooperative ADG model

The non-cooperative attack-defense game model (NCADG) comprises three elements, player(N), strategy(S) and utility(U), defined as follows:

$$ADG_{NC}=(\boldsymbol{N},\boldsymbol{S},\boldsymbol{U}) \quad (12)$$

where the non-cooperative means the opposability of the relationship between the two sides; $\boldsymbol{N}$= (P_1, P_2, …, P_n) denotes the set of players; $\boldsymbol{S}$ = (S_1, S_2, …, S_n) represents the set of strategies adopted by $\boldsymbol{N}$, and meets the requirement in (13); $\boldsymbol{U}$ = (U_1, U_2, …, U_n) refers to the set of utility as a function of $\boldsymbol{S}$.

$$\forall i\in n, S_i\neq\varnothing;\ S_i=(\mathrm{S}_1^i,\mathrm{S}_2^i,...,\mathrm{S}_m^i),\mathrm{m}\geq 2 \quad (13)$$

For the sake of simplifying the analysis, the number of players is assigned 2, the ADG model therefore takes the form as:

$$ADG_{NC}=((P_{\mathrm{a}},P_{\mathrm{d}}),(\mathrm{S}_{\mathrm{a}},\mathrm{S}_{\mathrm{d}}),(U_{\mathrm{a}},U_{\mathrm{d}})) \quad (14)$$

where the subscript **a** and **d** denote the attacker and defender, respectively. Besides, the set of all utility could be described as a matrix $\boldsymbol{U}_{\mathrm{ADG}}$ as shown in Fig.3, horizontal rows of which represent the defense strategies, while the vertical columns refer to the attack strategies. The value of each element in $\boldsymbol{U}_{\mathrm{ADG}}$ denotes the payoff of different combination of strategies, and the both sides of players target to obtain maximum benefits.

$$\begin{array}{c} \\ S_1^{\mathrm{d}} \\ S_2^{\mathrm{d}} \\ S_3^{\mathrm{d}} \end{array}\begin{array}{c} \begin{array}{cccccc} S_1^a & & S_2^a & & S_3^a & \end{array} \\ \begin{pmatrix} U_{\mathrm{a}11} & U_{d11} & U_{\mathrm{a}21} & U_{d21} & U_{\mathrm{a}31} & U_{d31} \\ U_{\mathrm{a}12} & U_{d12} & U_{\mathrm{a}22} & U_{d22} & U_{\mathrm{a}32} & U_{d32} \\ U_{\mathrm{a}13} & U_{d13} & U_{\mathrm{a}23} & U_{d23} & U_{\mathrm{a}33} & U_{d33} \end{pmatrix} \end{array}$$

Figure 3: Utility matrix of non-cooperative ADG model

4.2 Nash Equilibrium of Mixed Strategy

Based on the utility matrix of NCADG model defined in the previous part, the selection of prochain strategy of both players could therefore be estimated through solving the Nash Equilibrium of Mixed Strategy(NEMS). Due to the uncertainty of attack and defence action, the probability distribution $\boldsymbol{p}_{\mathrm{a}}$ and $\boldsymbol{p}_{\mathrm{d}}$ of strategy-determination from attacks and defenders in model (12) is denoted as follows:

$$\boldsymbol{p}_{\mathrm{a}}=(p_{\mathrm{a}1},p_{\mathrm{a}2},...,p_{\mathrm{a}n}) \quad (15)$$

$$\boldsymbol{p}_{\mathrm{d}}=(p_{\mathrm{d}1},p_{\mathrm{d}2},...,p_{\mathrm{d}n}) \quad (16)$$

In consequence, the estimated utility of both players U_{aE} and U_{dE} under NEMS could be described as:

$$U_{\mathrm{aE}}(\boldsymbol{p}_{\mathrm{a}},\boldsymbol{p}_{\mathrm{d}})=\sum_i^m\sum_j^n p_{\mathrm{a}i}*p_{\mathrm{d}j}*U_{\mathrm{a}}(\mathrm{S}_i^{\mathrm{a}},\mathrm{S}_j^{\mathrm{d}}) \quad (17)$$

$$U_{\mathrm{dE}}(\boldsymbol{p}_{\mathrm{a}},\boldsymbol{p}_{\mathrm{d}})=\sum_j^n\sum_i^m p_{\mathrm{d}j}*p_{\mathrm{a}i}*U_d(\mathrm{S}_i^{\mathrm{a}},\mathrm{S}_j^{\mathrm{d}}) \quad (18)$$

4.3 Optimal linear programing algorithm

In order to solve the NEMS issue, the optimal linear programing algorithm is adopted and shown as follows:

Input : ADG_{NC}
Output : *Nash Equilibrium*
Maximize: $z=\boldsymbol{p}_a\boldsymbol{U}_{ADG}^a\boldsymbol{p}_d^T-U_{aE}+\boldsymbol{p}_a\boldsymbol{U}_{ADG}^d\boldsymbol{p}_d^T-U_{dE}$
Subject to: $\boldsymbol{U}_{ADG}^a\boldsymbol{p}_d^T\leq U_{aE}\boldsymbol{E}_m$
$(\boldsymbol{p}_a\boldsymbol{U}_{ADG}^d)^T\leq U_{dE}\boldsymbol{E}_n$
$\boldsymbol{p}_a\boldsymbol{E}_m=\boldsymbol{p}_d\boldsymbol{E}_n=1$

where, $\boldsymbol{E}_m$= $(1,1,1)_{m\times 1}$ and $\boldsymbol{E}_n$= $(1,1\ldots 1)_{n\times 1}$; $\boldsymbol{U}_{ADG}^a$ and $\boldsymbol{U}_{ADG}^d$ represents the attacker and defender's part in utility matrix defined in Fig.3. Through the maximization of value z, the optimal strategy-selection of both players in CPPS could therefore be well determined.

5 Conclusion

This paper develops a quantitative assessment technique of general cyber-attack in CPPS, then employs a non-cooperative ADG model to establish the impact matrix of different strategies, afterwards adopts NEMS algorithm to

solve the linear programming issue and finally obtains the optimal selection results of strategies from the perspectives of both attacker and defender. Compared to other approaches reported in literature, the proposed framework fully takes the interaction between attacker and defender into consideration. Additionally, the adaptability of method is as well improved as most of the efficient protection measures adopted in computer networks are unfit to the real application in establishing robust defense system of CPPS. Future research work will be dedicated to more simulation and field tests to evaluate the performance of strategy-selection in general cyber-attack.

Acknowledgements

This research work was supported by YANG Jingyi and FAN Jing from the school of electronic and information engineering of Xi'an Jiaotong University. The authors would like to sincerely acknowledge their assistance.

References

[1] T. M. Chen and S. Abu-Nimeh. "Lessons from Stuxnet." *Computer*, vol. 44, no. 4, pp. 91-93, (2011).

[2] L. Guo, S. Xin, et al. " Comprehensive security assessment for a cyber physical energy system: a lesson from Ukraine's blackout." *Automation of Electric Power Systems Press*, vol. 40, no. 5, pp. 145-147, (2016).

[3] Z. Li, W. Tong, X. Jin. "Construction of Cyber Security Defense Hierarchy and Cyber Security Testing System of Smart Grid: Thinking and Enlightenment for Network Attack Events to National Power Grid of Ukraine and Israel. " *Automation of Electric Power Systems Press*, vol. 40, no. 8, pp. 147-151, (2016).

[4] W. Jiang, B. Fang, et al. "Optimal Network Security Strengthening Using Attack-Defense Game Model." *International Conference on Information Technology: New Generations, Itng*, Las Vegas, pp. 475-480, (2009)

[5] P. Mell, K. Scarfone and S. Romanosky. "Common Vulnerability Scoring System," *IEEE Security & Privacy*, vol. 4, no. 6, pp. 85-89, (2006).

[6] X. Ye, J. Zhao, Y. Zhang, F. Wen. "Quantitative Vulnerability Assessment of Cyber Security for Distribution Automation Systems." *Energies*, vol. 8, no. 6, pp. 5266-5286, (2015).

[7] S. Zonouz, C. M. Davis, K. R. Davis, et al. "A security-oriented cyber-physical contingency analysis in power infrastructures. " *IEEE Transactions on Smart Grid*, vol 5, pp. 3–13, (2014).

[8] C. A. O. Soares, L. S. Batista, F. Campelo and F. G. Guimarães. "Computation of Mixed Strategy Non-dominated Nash Equilibria in Game Theory." *BRICS Congress on Computational Intelligence and 11th Brazilian Congress on Computational Intelligence*, Ipojuca, pp. 242-247, (2013).