Open Access Journal

Journal of Power Technologies 96 (3) (2016) 170–177

journal homepage:papers.itc.pw.edu.pl

Generation of Cyber-security Reinforcement Strategies for Smart Grid Based on the Attribute-based Attack Graph

Bo Zhang[a, b], Qianmu Li[a,*], Yiying Zhang[c], Xuan Liu[d], Zhen Ni[a]

[a] *School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China;*
[b] *Global energy interconnection research institute, Nanjing 210003, China;*
[c] *School of Resources & Safety Engineering, China University of Mining & Technology, Beijing, 100083 ,China;*
[d] *Illinois Institute of Technology, 10 w 35th st, Chicago,IL, USA*

Abstract

A smart grid is a kind of energy cyber-physical system (ECPS) with the interdependency of information and physicality. A cyber-attack gravely threatens the safe and stable operation of a physical power grid. Cyber-security reinforcement of smart grid has become a research issue. However, the information network scale of a smart grid is massive, and the generation of security reinforcement strategies has become a problem. Therefore, a generation method of security reinforcement strategies based on an attribute-based attack graph was proposed in this study. The method defined a smart grid based on premise and consequence attributes to form an attribute-based attack graph. With this graph, the method for the generation of security reinforcement strategies was transferred to the minimum dominating set of the attribute-based attack graph and solved to realize space reduction in the security reinforcement strategies. An algorithm for the generation of security reinforcement strategies was designed based on the greedy algorithm, and strategies for large-scale cyber security reinforcement of the smart grid were determined to eliminate the complexity and difficulty of this problem effectively. Through a simulation analysis of a large-scale node network, the efficiency of the generation method of reinforcement strategies based on the attribute-based attack graph and minimum dominating set was verified. Results show that the proposed method can be used for security reinforcement of large-scale complicated networks of a smart grid.

Keywords: Attribute-based attack graph, Reinforcement strategies, Cyber security, Dominating set, Smart grid

1. Introduction

With the development of modern information and communication technology, the smart grid, with the help of advanced information and communication technology, has realized online digital collection on relevant grid equipment and line status. It closely integrates information and physical power grid systems, perceives the real-time status of different links in the grid, and performs real-time decision control. Hence, it realizes networking, informationization, and intellectualization of power generation, transmission, provision, and consumption. The smart grid has become a kind of energy cyber-physical system (ECPS). However, the transmission probability of successive or cascading failure between information and physical power networks caused by the failure of the information system increases accordingly and may thus result in the collapse of the entire coupled system; it could even gravely threaten the safe operation of the power system. Multiple power security incidents caused by information security attacks have occurred in China and other countries. Examples of these incidents include the 2010 Stuxnet attack on an Iranian nuclear power station and the 2015 Ukrainian grid blackout caused by a “BlackEnergy” malware attack. Evidently, cyber-security attacks result in great harm to smart grid. Thus, studying the cyber security reinforcement technology of the smart grid is crucial. Cyber security evaluation based on an attack graph is an important method to reinforce cyber security. All possible attack paths from the perspective of the attacker are enumerated on the basis of a comprehensive analysis of node holes and vulnerability information, and security reinforcement strategies are generated. However, given that a smart grid has a large-scale network and complicated structure and possesses sophisticated and multiscale dynamic properties and complex network characteristics, security reinforcement strategies generated based on the entire-network attack graph are too massive to implement and are thus not feasible. How to generate a feasible

*Corresponding author
Email address: liqianmu@126.com (Qianmu Li)

security reinforcement strategy of a smart grid has become a research focus. This study shows how to establish a generation method of grid security reinforcement strategies based on the attribute-based attack graph.

2. Related Work

The attack graph model was first proposed by Swiler. In the original attack graph, each attack of the attacker is considered an edge, and each node represents a network status [2, 15]. The administrator can identify the key node of the network through the probability of successful attacks. The attack graph is a type of the status attack graph [8]. The advantage of the status attack graph is that it helps the administrator realize the entire process intuitively to implement security reinforcement, but it may generate an explosion with the enlargement of the network [14]. To solve this problem, Alhomidi et al. proposed the "monotone hypothesis" [5], which posits that the target of the attacker develops toward the increasing orientation of the attacker's capability, namely, they may not repeatedly require the required attacking capability [5, 7, 6]. Afterward, Noel et al. introduced the attribute-based attack graph model [11]. The attribute-based attack graph involves two types of nodes, namely, a cyber security element and specific vulnerability. Compressing the network scale through this abstract manner is effective. In recent years, many research results have been presented with regard to the mutation, construction, and application of the attack graph [1, 12, 13, 9, 10, 4]. For the network reinforcement method based on the attack graph, Reference [1] presented a cyber security measurement method based on the number of attack paths. Reference [12] presented another cyber security measurement method based on the average length of the attack paths. Reference [13] established a security measurement method, but this method is ineffective in cyber security evaluation, because it cannot effectively help the administrator make a decision. Reference [9] presented a cyber security reinforcement method based on the minimal critical set, but this method did not consider the complicated relation between the attack and the network configuration elements. References [10, 4, 3] proposed a series of network reinforcement methods by breaking the initial condition. However, all of these methods exhibit limitations as follows: (1) the solution space is of an exponential order, (2) disregard of the cost when selecting the initial condition to be broken, and (3) disregard of vulnerability repair as a desirable strategy of network reinforcement. In the case of a smart grid with a large-scale network, the attribute-based attack graph should be used for a vulnerability analysis instead of the status attack graph. Although the attribute-based attack graph has several flaws in intuitionistic apprehension of attack traces, it can effectively resolve the status explosion problem. The rest of this paper is organized as follows. The second section provides the definitions of the attribute-based attack graph and the dominating set and presents a modelling analysis of the information network and attack on a smart grid. The third section presents the proposed node decision method of cyber security reinforcement on the basis of calculating the minimum dominating set (MDS) of attack graph G to decide the method of security reinforcement. The fourth section introduces the security strategy generation algorithm based on the greedy algorithm. The fifth section presents the verification of the validity of the algorithm through a simulation. The last section provides the relevant results and the conclusion of the study.

3. Attribute-based Attack Graph and Dominating Set

Definition 1: The attribute-based attack graph is a digraph. Given the atomic attack node set A, attribute node set C, premise edge set $R_r \subseteq (C \times A)$, and consequence edge set $R_i \subseteq (A \times C)$, the attribute-based attack graph can be $G(A \cup C, R_r, \cup R_i)$, where $A \cup C$ is an attribute node set and $R_r \cup R_i$ is an edge set. The attribute-based attack graph contains two types of security attribute nodes. The first type of attribute nodes only exists as premise-attribute nodes of atomic attacks rather than consequence-attribute nodes of any atomic attacks. This type only lies in the initial location of the attribute-based attack graph. Nodes belonging to this type are important for network reinforcement, because they are at the entrance location of all kinds of attacks. The other type includes not only the premise-attribute nodes of atomic attacks but also the consequence-attribute nodes. This type of security-attribute nodes is not at the initial location of the attribute-based attack graph, representing the consequence of several successive atomic attacks.

Definition 2: $G = (V, E)$ is set as the directed bipartite graph constituted by node set V and directed edge set E. Then, $E \subseteq V \times V$. For the arbitrary edge $(u, v) \in E$, $(u, v) = u \rightarrow v$, indicates that this edge points to node v from node u; u is the precursor of V, and v is the successor of u. Supposing s_1 and s_2 constitute a division of set V, if and only if $u \in s_1 \wedge v \in s_2 \vee u \vee s_2 \wedge v \in s_1$, G is a bipartite graph. Given that the edges of the attribute-based attack graph can only point to the atomic attack nodes from the attribute nodes or point to the attribute nodes from the atomic attack nodes instead of pointing to the attribute nodes from the attribute nodes or to the atomic attack nodes from the atomic attack nodes, the attribute-based attack graph can be regarded as a directed bipartite graph. In this bipartite graph, the attribute nodes form one set, and the atomic attack nodes form another set.

Definition 3: The dominating set is represented by S. In the directed graph $G = (V, E)$, node set $S \subseteq V$ is a dominating set of G. If and only if in $\forall v \in (V - S)$, $u \in s$ making $(u, v) \in E$, v is covered by U, and the nodes in S are called dominating nodes.

Definition 4: The minimal dominating set presented by s_m. s_m is a minimal dominating set if and only if arbitrary $s \in s_m$ and s is no longer a dominating set.

Definition 5: The minimum dominating set is presented by s_M. It is a minimal dominating set with the smallest cardinal number. The relation between the initial attribute node

set and the atomic attack node set is M:N, because the status of a single initial attribute node can decide the success of multiple atomic attacks. Given an initial attribute node set $s = \{x, y, z\}$, if the initial attribute node x is a premise-attribute node of all atomic attack nodes but the nodes y and z are only the premises of several atomic attacks, then x predominates in this set. From Definition 1 we know that for atomic attack nodes, when the status of all premise nodes is "true," the atomic attack can execute. The relationships among all premise-attribute nodes are in conjunction; moving the predominating initial attribute node (e.g., x in this study) can prevent most atomic attacks. We are seeking such attribute nodes to decrease the number of initial attribute nodes to be removed, namely, to prevent the implementation of network attacks.

4. Solution of the Minimum Dominating Set of the Initial Attribute

The generation of optimal network reinforcement strategies is transferred to the solution of the minimum dominating set constituted by initial attribute nodes. The main idea is to regard the attribute-based attack graph as a directed bipartite graph through the calculation of the minimum dominating set constituted by the initial attribute node set of attack graph G to decide the method to be adopted in reinforcement of the network. The minimum dominating node obtained represents a series of key attributes that cover all the nodes of atomic attacks. If these attributes are invalid, cyber security defense can be effectively achieved. To solve this problem, the issue above is converted into a classic set cover problem (SCP). Given that each initial attribute node in attribute-based attack graph G can cover one or more atomic attack nodes, we assume that all (m) atomic attack nodes in attribute-based attack graph G can be divided into n sets. Each of the n sets has its given corresponding initial attribute node. The goal is to calculate the optimal coverage set of all the atomic attack nodes in attack graph G. Then, the set can cover all atomic attack nodes in the attribute-based attack graph, and the number of initial attribute nodes is guaranteed to be the smallest. For a more accurate expression, we let set ε, $|\varepsilon| = m$ be a complete set of atomic attack nodes, and C is the subset of power set ε, namely, $C \subseteq 2^{\varepsilon}$. Set X covers all atomic attack nodes when $X \in C \wedge \varepsilon = U_{x \in C} C$. We used the attribute-based attack graph without rings. This graph has no edges such as (u, u) and no similar and repetitive (u, v) edges. To the arbitrary nodes in attribute-based attack graph G, insets and outsets exist. The in-degree and out-degree of these nodes are as follows:

1. Attribute node set (initial condition): We let $Pre \subset V$ be the limited initial attribute node set that the attacker can touch in attribute-based attack graph G and let $u \in Pre$ be an initial attribute node. Then, $I(u) = \{w\colon (w, u) \in E\}$ is the inset of initial attribute node u. $\forall u \in Pre$, $(w\colon (w, u \in E))$ and $I(u) = \varnothing$, $\forall u \in Pre$. In-degree $id(u) = 0$, $u \in Pre$. The outset of the initial attribute nodes is $O(u) = \{v\colon (u, v) \in E\}$. Once an initial attribute node meets the condition, one or more vulnerabilities could be taken advantage of. In other words, arbitrary initial attribute node $u \in Pre$ is the attribute node of one or more atomic attack nodes. Therefore, the out-degree of initial attribute node $od(u) \geq 1$, $\forall u \in Pre$.
2. Attack node set (exploits): Based on Definition 1, we let $A \subset V$ be the limited set constituted by atomic attack nodes in attribute-based attack graph G, where $A = \{a_1, a_2, a_3, \ldots, a_m\}$. The inset of atomic attack a_i is $I(a_1) = \{w\colon (w, a_i) \in E\}$; w is a premise edge. If arbitrary atomic attack a_i is to be implemented successfully, one or more premise-attribute nodes must exist, and all the premises must be satisfied. Therefore, in-degree $id(a_1) \geq 1$, $\forall a_1 \in A$. A successful atomic attack will produce a consequence-attribute node; therefore, the out-degree of atomic attack $od(a_1) = 1 \forall a_1 \in A$.
3. Consequence-attribute node set (post condition): We let $Pst \subset V$ be the consequence-attribute node set produced by $|A|$- time successful atomic attacks in attribute-based attack graph G and let $u \in Pst$ be a consequence node. Then, $I(u) = \{w\colon (w, u) \in E\}$ is the consequence-attribute node $u \in Pst$. Each successful atomic attack will produce a consequence-attribute node. However, implementing different atomic attacks to the target host may produce similar consequence-attribute nodes. In consequence, the in-degree of the consequence-attribute node meets $id(u) \geq 1$, $\forall u \in Pst$. The newly produced consequence-attribute node can become the premise-attribute node of other atomic attacks. Therefore, apart from the final target consequence-attribute node, the out-degree of all consequence-attribute nodes is $od \geq 1$, $\forall u \in Pst$. Table 1 shows the conditions that the in-degree and out-degree of different kinds of nodes in the attribute-based attack graph should meet.

Table 1: In-degree and out-degree conditions of nodes

Node u	In-degree (u)	Out-degree (u)
Initial attribute node	0	>=1
Atomic attack	>=1	1
Consequence-attribute node	>=1	>=1/0

With an imaginary target network as an example, we regard its corresponding attribute-based attack graph as a bipartite network. As shown in Fig. 1a, compared with finding the dominating set of the same kind of node set from a common directed graph, finding the minimum dominating set in the attribute-based attack graph is more difficult. Notably, no polynomial time algorithm exists at present to calculate the dominating set of graphs. To eliminate the complexity and difficulty of this problem, we used a conservative method.

The atomic attack nodes and the initial attribute nodes

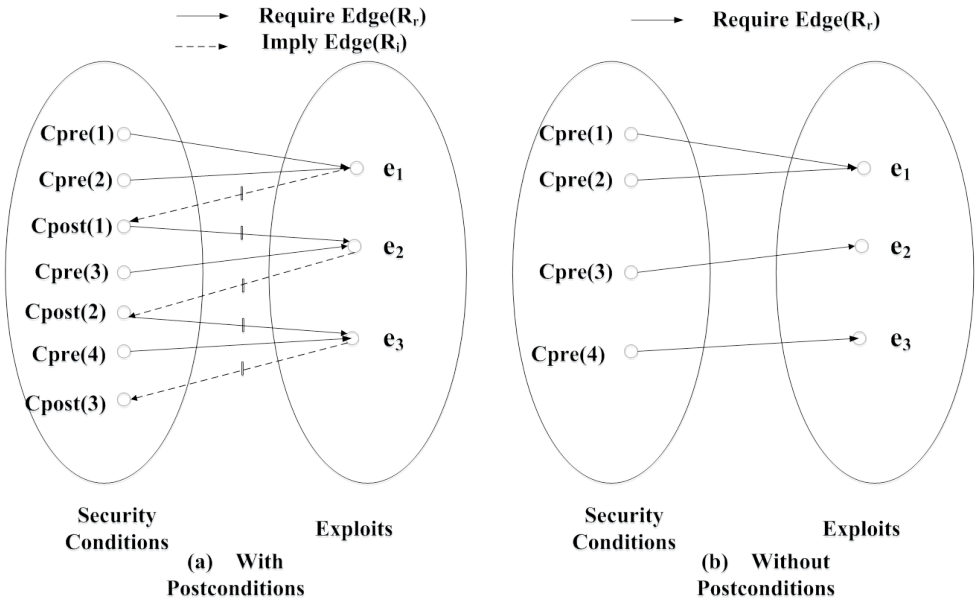

Figure 1: Corresponding bipartite graph of the attribute-based attack graph

are the most important nodes of the attack graph; however, a consequence-attribute node is only the consequence of a successful atomic attack. The target of this study is to calculate the MDS that can cover all atomic attacks in the initial attribute set so that we can remove all the consequence-attribute nodes in the bipartite graph. The bipartite graph of the operations is shown in Fig. 1b. However, the figure only contains initial attribute nodes, the atomic attack node, and directed edges pointing to the latter from the former. The MDS calculated from the directed edge bipartite graph provides the initial attribute node set covering all atomic attacks in the attribute-based attack graph.

5. Reinforcement Strategies Generation Algorithm based on the Greedy Algorithm

The process to calculate MDS is shown in Table 2. Primarily, all nodes in graph G are recognized and classified into a corresponding node set (2 to 11 lines) according to the in-degree and out-degree obtained from Table 1, namely, the initial attribute node set, atomic attack node set, and consequence-attribute node set caused by an atomic attack. Given that we only considered the initial attribute node set, the algorithm calculates the number (12 to 14 lines) of atomic attacks covered by each initial attribute node. The atomic attack covered by each initial attribute node represents the subset of its corresponding atomic attack in attack graph G. In set cluster C (15 lines), each subset covers at least a subset constituted by an atomic attack in attack graph G. The target is to find a set to cover all atomic attack nodes in attack graph G. The greedy set-cover algorithm (Algorithm 2) was used to achieve this goal. The minimal set cluster covering all atomic attacks generated through this algorithm is the MDS we ultimately seek. The set constituted by this kind of attribute nodes covers all atom attacks in G. Then, it becomes the corresponding dominating set of the initial attribute node set.

For attribute-based attack graph G having “m” atomic attack nodes and “n” initial attribute nodes, the time complexity of the greedy set-cover algorithm used in this study is O(mn). To sum up, the coverage problem of sets is an optimization problem.

6. Experiment and Analysis

We conducted an analysis with the network topology presented in Reference [6], as shown in Fig. 2. Host3 is the target host of the attacker, and the MySQL database service operated on it is our key resource. The attack is a malignant entity, and its target is to acquire the root authority on Host3. The firewall separates the target network from the internet. The firewall configuration in the network topology is shown in Table 4.

Table 5 shows the specific condition of the vulnerabilities in the host nodes of the network using relevant information. The information on vulnerabilities was obtained from the NVD database. The outer-network firewall in the network only allows the hosts in the outside net to access the Host0 services. Access to any other hosts is prevented. The intranet hosts are only allowed to communicate according to the access control regulation in Table 5. “ALL” indicates that the source host can access all services on the destination host. “NONE” indicates that any access to the source host to any destination host service is prevented [6].

The access control regulation is shown in Table 5, the network topology is shown in Fig. 2, and the generation-based attribute-based attack graph is shown in Fig. 3. The atomic attack nodes are denoted by an ellipse. The initial attribute

Table 2: In-degree and out-degree conditions of nodes

ALGORITHM 1: find MDS to calculate MDS in attack graph G based on the initial attribute nodes covering all attribute nodes of all atomic attack nodes
Input: $G = \langle V, E \rangle$**Target-network attribute-based attack graph** **Output: MDS**$\mathbf{MDS} \subseteq \mathbf{Initial}Condn \rightarrow$**minimum dominating set covering all atomic attacks in attack graph G**
1: $Start$
2: $\langle V, E \rangle \leftarrow MST(G)$
// to recognize all nodes and edges in G with minimum spanning tree algorithm
3: $For\ all\ u \in V$ do
4: $if\ (id(u) = 0 \wedge od(u) \geq 1)$
5: $InitialCondan \leftarrow u$
6: $Else\ If\ (id(u) \geq 1 \wedge od(u) = 1)$
7: $Exploit \leftarrow u$
8: $Else$
9: $PostCondan$
10: $End\ If$
11: $End\ For$
12: $For\ all\ u \in InitialCondan$ do
13: $c_i \leftarrow o(u)$
14: $End\ For$
15: $Compute\ set\ of\ sets\ C = U_{i=1}^{n} c_i^e;\ where\ n = \lvert InitialCondan \rvert$
16: $MDS\ (G)\ GREEDY - SET - COVER\ (Exploit, C)$
17: End

Table 3: Greedy set-cover algorithm

ALGORITHM 2: GREEDY-SET-COVER$(\varepsilon, \mathbf{S})$**to calculate the covering set**
Input: set cluster $\mathbf{S(i) = S_i\ (1 \leq i \leq n)}$ **is the subset of atomic attack node set**ε **Output: covering set D**
1: $Start$
2: $U \leftarrow \varepsilon$
3: $D \leftarrow \varnothing$
4: $While\ U \neq \varnothing$ do
5: $Select\ S\ (j) \in S\ that\ maximizes\ \lvert S\ (j) \cap U \rvert\ where\ j \leq n$
6: $U - S\ (j)$
7: $D = D \cup S\ (j)$
8: $S\ (i) = S\ (i) - S\ (j),\ 1 \leq i \leq n$
9: $End\ While$
10: $Return\ D$
11: End

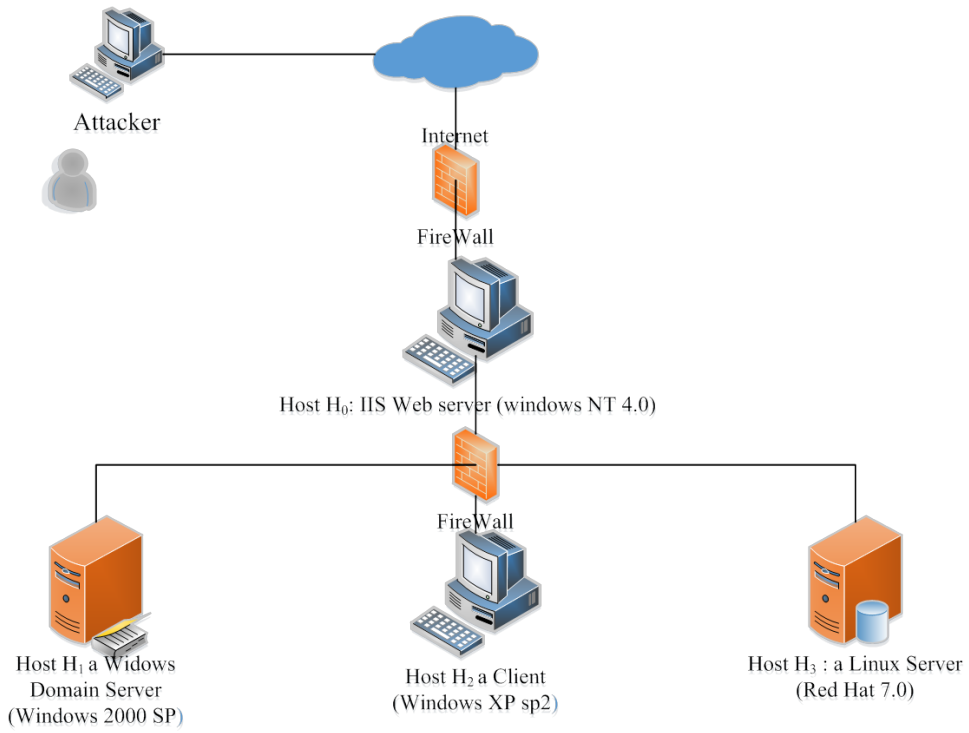

Figure 2: Corresponding bipartite graph of the attribute-based attack graph

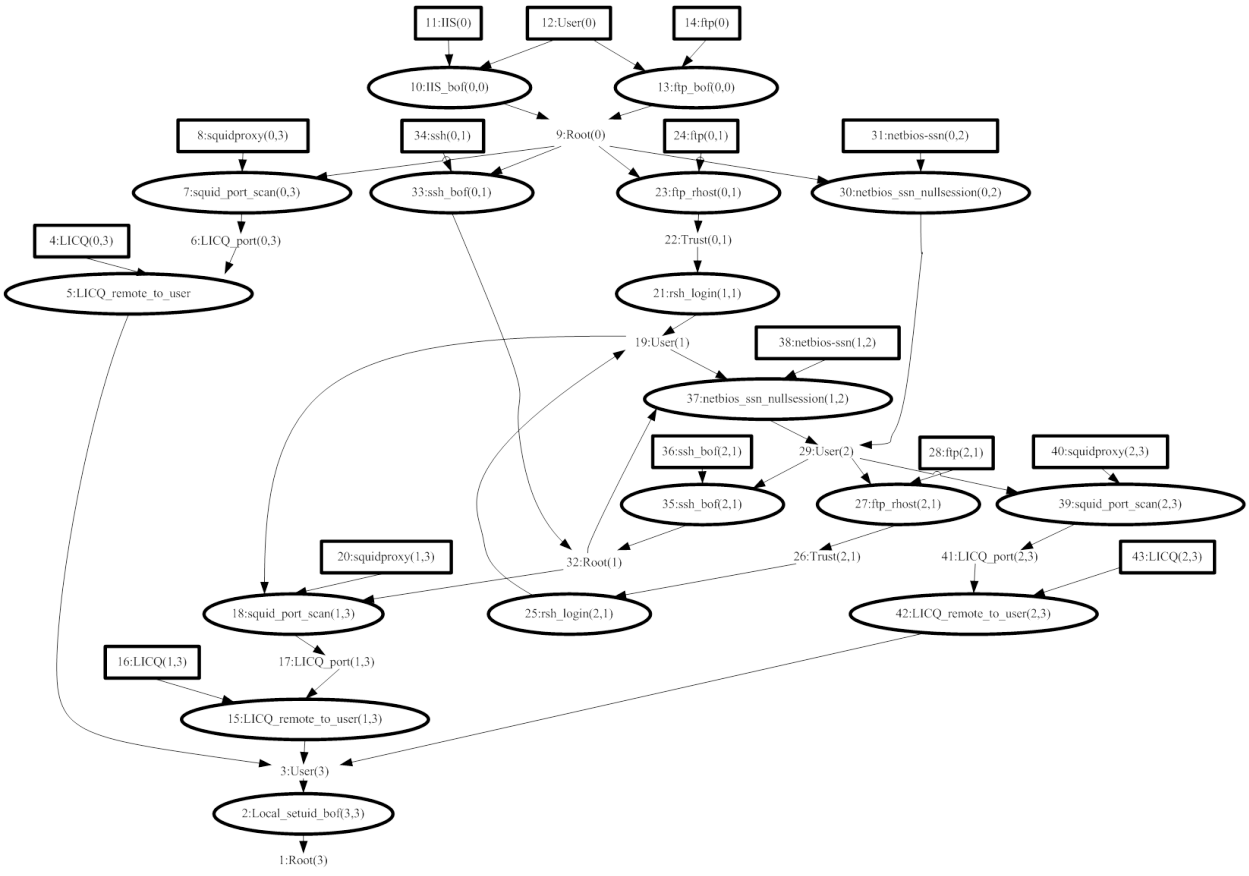

Figure 3: Generated attribute-based attack graph

Table 4: Network firewall configuration

Host	Attacker	Host0	Host1	Host2	Host3
Attacker	Localhost	All	NONE	NONE	NONE
Host0	ALL	Localhost	ALL	ALL	Squid LICQ
Host1	ALL	IIS	Localhost	ALL	Squid LICQ
Host2	ALL	IIS	ALL	Localhost	Squid LICQ
Host3	ALL	IIS	ALL	ALL	Localhost

Table 5: Information on vulnerabilities

Host	Services	Ports	Vulnerabilities	CVE IDs
Host0	IIS web service	80	IIS buffer overflow	CVE-2010-2370
	ftp	21	ftp buffer overflow	CVE-2009-3023
	ftp	21	ftp rhost overwrite	CVE-2008-1396
Host1	ssh	22	ssh buffer overflow	CVE-2002-1359
	rsh	514	rsh login	CVE-1999-0180
Host2	netbios-ssn	139	netbios-ssn nullsession	CVE-2003-0661
	rsh	514	rsh login	CVE-1999-0180
	LICQ	5190	LICQ-remote-to-user	CVE-2001-0439
Host3	Squid proxy	80	squid-port-scan	CVE-2001-1030
	MySQL DB	3306	local-setuid-bof	CVE-2006-3368

nodes are represented by a rectangle, and the consequence-attribute nodes are shown in plain text. Between the two atomic attacks, the ellipse connects the premise-attribute node and the consequence-attribute node. Fig. 3 includes 17 atomic attack nodes. If an atomic attack is to be implemented successfully, all of its premise-attribute nodes must be satisfied. The consequence-attribute node cannot be removed unless practical reasons require it (for example, vulnerabilities, unnecessary services/open ports) to be removed. Otherwise, the initial attribute node can be independently removed when reinforcing the network. By using the FindMDS algorithm, the minimal dominating set of the above attribute-based attack graph is *MDS = {user(0), ftp(0, 1), squid - proxy (1, 3), LICQ(0, 3), squid - proxy(0, 3), LICQ(0, 3), ftp(2, 1), ssh (2, 1), net - bios - ssn (0, 2), squid - proxy(2, 3), ssh(0, 1), netbios - ssn(1, 2), LICQ(2, 3)}*. Preferentially breaking one or more initial attribute nodes can prevent the network attacks needing them to be the prerequisite. The security administrator must consider the cost of these initial conditions when they make a decision.

7. Conclusion

To realize cyber security reinforcement in the context of a smart grid, a generation method of cyber-security reinforcement strategies for the smart grid was proposed in this study. The following conclusions were obtained.

1. Based on the attribute-based attack graph, a generation method of cyber-security reinforcement strategies for the smart grid was proposed. This method determines the minimum network reinforcement set by establishing the corresponding attribute-based attack graph of the target network and solving the MDS of the initial attribute node set.
2. The proposed method can realize entire-network reinforcement based on minimum-scale node reinforcement and analyze the minimum and optimum security reinforcement target while reducing the status space of the security reinforcement strategies.
3. Simulation verification showed that in a relatively large-scale network, the proposed generation algorithm of cyber-security reinforcement strategies of the smart grid based on the attribute-based attack graph can analyze the attack path and calculate the optimum defense object with the attacking profit to stop the attack. It provides guidance for security administrators to evaluate and control the cyber security risk and implement effective defensive measures. With this method, to realize efficient reinforcement to the network, network administrators only need to pay attention to a small part of the initial attribute node set. The method effectively avoids the explosion problem and can be used in security reinforcement strategy calculation of large-scale networks in a smart grid.

References

[1] Chen F., Liu D., Zhang Y., and Su J. A scalable approach to analyzing network security using compact attack graphs. *Journal of Networks*, 5 (5):543–550, 2010.

[2] Spanos G. and Angelis L. Impact metrics of security vulnerabilities: Analysis and weighing. *Information Security Journal: A Global Perspective*, pages 1–15, 2015.

[3] Wang L., Yao C., Singhal A., and Jajodia S. Implementing interactive analysis of attack graphs using relational database. *Journal of Computer Security*, 16(4):419–437, 2008.

[4] Xu L., Li Y.P., Li Q.M., Yang Y.W., Tang Z.M., and Zhang X.F. Proportional fair resource allocation based on hybrid ant colony optimization for slow adaptive ofdma system. *Information Science*, 293:1–10, 2015.

[5] Alhomidi M. and Reed M. Risk assessment and analysis through population–based attack graph modelling. *World Congress in Internet Security (WorldCIS)*, pages 19–24, 2013.

[6] Idika N. and Bhargava B. Extending attack graph-based security metrics and aggregating their application. *IEEE Transactions on Dependable & Secure Computing*, 9(1):75–85, 2012.

[7] Poolsappasit N., Dewri R., and Ray I. Dynamic security risk management using bayesian attack graphs. *IEEE Transactions on Dependable and Secure Computing*, 9(1):61–74, 2012.

[8] Li Q. Multiple qos constraints finding paths algorithm in tmn. *Information*, 14(3):731–737, 2011.

[9] Li Q.M. and Zhang. H. Information security risk assessment technology of cyberspace: a review. *International Journal on Information*, 15 (11):4677–4683, 2012.

[10] Xia R., Xu F., Zong C.Q., Li Q., Qi Y., and Li T. Dual sentiment analysis: Considering two sides of one review. *IEEE Transactions on Knowledge and Data Engineering*, 27(8):2120–2133, 2015.

[11] Noel S. and Jajodia S. Metrics suite for network attack graph analytics. *Proceedings of the 9th Annual Cyber and Information Security Research Conference ACM*, pages 5–8, 2014.

[12] Roschke S., Cheng F., and Meinel C. High-quality attack graph-based ids correlation. *Logic Journal of IGPL*, 21(4):571–591, 2013.

[13] Saurabh S. and Sairam A.S. A more accurate completion condition for attack-graph reconstruction in probabilistic packet marketing algorithm. *National Conference on Communications (NCC) IEEE*, pages 1–5, 2013.
[14] Chen X.J., Fang B.X., and Zhang H.L. Inferring attack intent of malicious insider based on probabilistic attack graph model. *Chinese Journal of Computers*, 37(1):62–72, 2014.
[15] Yun Y., Xishan X., Yan J., and Chang Q. Z. An attack graph-based probabilistic computing approach of network security. *Chinese Journal of Computers*, 33(10):1987–1996, 2010.