A Bayesian Attack Tree Based Approach to Assess Cyber-Physical Security of Power System

Rounak Meyur
Department of Electrical and Computer Engineering
Virginia Polytechnic Institute and State University
Blacksburg, USA
rounakm8@vt.edu

***Abstract*—The advantage of adding modern day information and communication technology (ICT) in the supervisory control and data acquisition (SCADA) system associated with the power network comes at the cost of an increased risk due to cyber intrusion. A well planned malicious attack on the SCADA system can not only compromise the communication network, but also cause catastrophic effects on the power grid in form of a widespread blackout. In this context, a lot of prior work deals with the comprehensive modeling of the cyber-physical system (CPS) and evaluating the possible vulnerabilities. In the present work, a Bayesian attack tree based approach is used to model cyber attacks in the SCADA network and the associated risk is evaluated as the combined effect on the communication and power system. This avoids the detailed modeling of every component in the CPS and considers only the critical vulnerabilities required to be exploited to perform the attack. Furthermore, the model takes into account the skill level of the adversary and the difficulty in intruding through each type of vulnerability. The proposed cyber attack model is applied on the IEEE-39 bus system with an associated SCADA network. The risk of a cyber attack on the critical vulnerabilities is evaluated for the power system.**

***Index Terms*—cyber-physical security, Bayesian attack tree, mean time to compromise, vulnerability assessment**

I. Introduction

The modern day power grid is an important societal infrastructure; its failure can have a significant impact on national and economic security of a country [1]–[3]. The inclusion of ICT in the SCADA network has increased the resiliency and facilitated self healing capabilities of the power grid [4]. This has been made possible through the large connected communication network with several remote access points enabling coordinated monitoring and control functions on the power grid [5]. However, this has exposed the system to numerous possibilities of cyber threat increasing the risk of a combined catastrophic failure of the power grid along with the communication network [6]. Therefore, the smart power grid consisting of the traditional power system with the intertwined ICT elements is identified as a critical interdependent infrastructure where a failure in either network can result in severe impact on the combined system [7].

The usage of standardized communication protocol in the SCADA system has opened up several vulnerabilities in the commonly used protocols like distributed network protocol (DNP) and IEC 61850 [8]. These may be known and zero-day type which can be exploited by an adversary to gain unauthorized access to control assets in the SCADA system [9]. For example in the cyber physical system depicted in Fig. 1 the lower part represents the physical power system with substation buses, generators, loads, transformers and transmission lines. The upper part denotes the hierarchical cyber system or the SCADA network associated with the power grid. The substations communicate with the regional control centers through Ethernet communication protocol, the control centers interchange information using the inter control center protocol (ICCP) and also communicate with the transmission operator (TO) through Ethernet routers. In such a setup, an intruder can exploit the vulnerabilities of the control center or substation LAN to gain root or administrator privilege in one of the human machine interfaces (HMIs) [10]. By obtaining access, the control commands might be manipulated to operate the circuit breakers in the physical power system resulting in instability in the grid from load-generation imbalance [11]. Often such attack can cause cascading events in the system leading to widespread blackout as in the case of Stuxnet malware attack in Ukraine in 2015 [12], [13]. This is due to the fact that the power system is operated with security analysis performed for at most 2 contingencies. A planned cyber attack can lead to multiple contingencies at the same time exacerbating the disturbance in the grid. In addition to that an adversary can gain access to the intelligent electronic devices (IEDs) connected to the substation LAN and create a man-in-the-middle attack by injecting false data or modifying information coming from the IEDs to the substation servers [14].

Several models have been proposed for identifying vulnerabilities in the CPS by evaluating the impact resulted from a cyber attack [7], [14]–[20]. A very simple statistical model based on graph theory results has been proposed in [7] where neither the SCADA nor the power network is accurately modeled. A Petri Net based cyber model consisting of firewalls and passwords has been proposed in [15]. Though the model was capable of replicating the operation of firewalls precisely, the probability of intrusion through a firewall was randomly selected irrespective of the hierarchy at which it is present. An improved usage of hierarchical Petri Nets is seen in [16] where the vulnerabilities of smart meters are modeled. However, the model was not developed to be applicable in the hierarchy

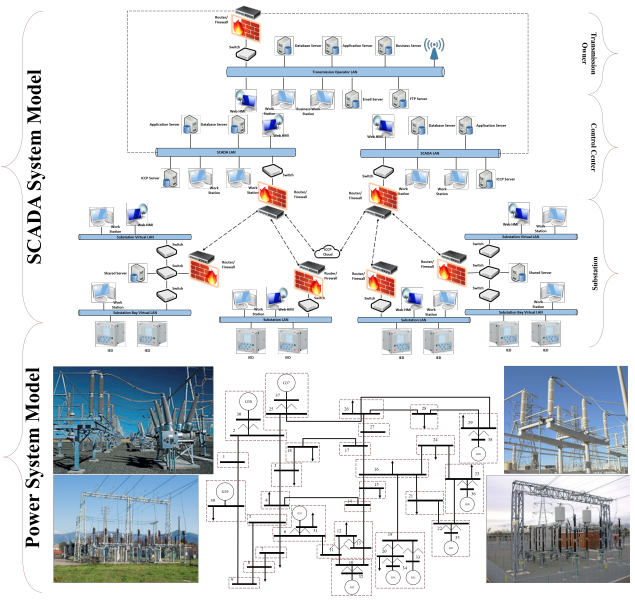

Fig. 1. Cyber-physical model of a typical power system.

of the SCADA system for the power grid. In [17], a similar Petri Net model for password and firewall has been considered to study the impact of coordinated intelligent cyber attack on the power system. However, only a simple model of firewall and password is used for every HMI in the cyber system. A comprehensive CPS model has been used in [18]–[20] where every element of the communication system is modeled using queues. The attack efficiency of a possible cyber threat is evaluated as the time required to send a packet of data from the source vulnerability to the target. However, the time of arrival of the data packet is selected randomly based on the processing rate. Therefore, the relative difficulty in exploiting a particular vulnerability is not considered; nor the skill level of the intruder is used to determine the time to compromise a target vulnerability. In this context, a statistical model is proposed in [21] where the skill level of the intruder and the difficulty of exploiting a vulnerability is considered to determine the time to compromise a given vulnerability.

Contribution. In this work, a Bayesian attack tree based CPS model would be considered. The important source vulnerabilities in the SCADA network would be first identified and then the attack path to a target goal would be evaluated. The probability of successfully exploiting a vulnerability would be calculated based on its type (relative difficulty to exploit) and the time to compromise it would be evaluated depending on the skill level of the intruder. The risk of the cyber vulnerabilities would be measured as the combined impact on both the cyber system and the power grid. Such a model would avoid comprehensive modeling of every element in the cyber system and would emphasize the modeling of the possible attack paths through the critical vulnerabilities.

The remainder of the proposal is organized as follows. Section II discusses about the necessary preliminaries for the technical approach outlined in the proposal. Section III discusses about the cyber system and the physical system models which has been used for performing the security analysis. Finally Section IV details the simulation results for the proposed methodology.

II. Preliminaries

A planned cyber attack on the SCADA system takes place through multiple steps in which the software protection elements are compromised. This entire process can be effectively modeled using attack trees. A cyber intrusion consists of vulnerabilities in the cyber system and the dependency among them to be exploited. Therefore, a cyber attack can be represented as a directed graph with vulnerabilities denoted by the nodes and edges symbolizing the dependencies. In this section, the attack tree representation of a cyber attack on the SCADA system and the method to evaluate probability of successful intrusion are detailed.

A. Attack Tree Representation of Vulnerabilities

In this paper, the attack graph $\mathcal{G}(\mathcal{V} \bigcup \mathcal{C})$ consists of two types of nodes: exploit to vulnerabilities denoted by $\mathcal{V}$ and conditions required for exploiting represented as $\mathcal{C}$. The preconditions needed to exploit a vulnerability are assumed to be either initial conditions of the attack or resulting output of some previously occurred exploit. In this case, three preconditions are required to be satisfied in order to exploit a vulnerability: (*i*)service which is denoted by *Service Name*(*Source Host ID*), (*ii*)connection represented by $\langle$*Source Host ID*,*Target Host ID*$\rangle$ and (*iii*)privilege which is denoted as *Privilege Name*(*Source Host ID*).

For example, a cyber intrusion scenario is considered for a control center SCADA system, where an adversary aims to gain unauthorized access to control assets in the power system. The cyber intruder has to access the application server for this purpose which is dedicated to send control commands to open/close circuit breakers in the power system. In order to do so, the adversary needs to gain access of the historian server through a firewall and thereafter reach the application server through a different firewall as shown in Fig. 2.

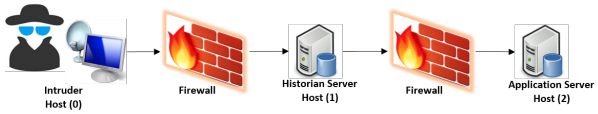

Fig. 2. Cyber intrusion scenario in control center application server.

Let there be two possible exploits to the vulnerabilities in the first firewall denoted by $\langle \text{Ser1}, 0, 1 \rangle$ and $\langle \text{Ser2}, 0, 1 \rangle$ as shown in Fig. 3. The first one is assumed to be a zero day exploit and the second one is considered as a known exploitation. A zero day exploit to a vulnerability is one which may not be publicly known but identified by an intruder. In order to exploit either of the vulnerabilities, the intruder needs the privilege *user*(*0*) (which denotes him being present) and is required to be connected to the historian server through $\langle 0,1 \rangle$. Additionally, the vulnerabilities require the services

Ser1(1) and *Ser2(1)* respectively to be available for them to be exploited. Once the vulnerability is successfully exploited, the intruder gains the user privilege *user(1)* of the historian server. This output of previously occurred exploit can be used as a precondition of the successive exploits. Let there be a single zero-day exploit to a vulnerability in the second firewall denoted by $\langle \text{Ser3}, 1, 2 \rangle$. This can be successfully exploited by an intruder having privilege *user(1)* to obtain access to the application server. Thereafter, the intruder can utilize the privilege *user(2)* of the application server to reach the goal privilege *root(2)*.

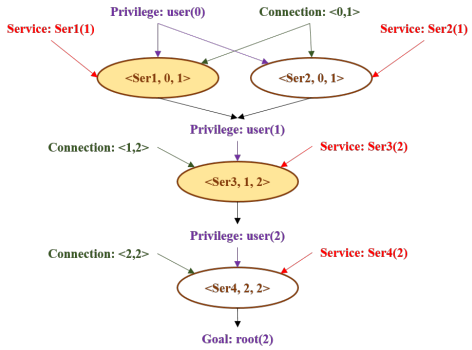

Fig. 3. Attack tree representation of cyber intrusion in control center application server.

B. Modeling Bayesian Attack Tree

Attack trees can be effectively modeled using Bayesian networks (BN) which are widely used to develop the probabilistic model for the same. BN is denoted by a pair $\langle \mathcal{G}, \mathcal{N} \rangle$ where $\mathcal{G}(\mathcal{V}, \mathcal{E})$ denotes a directed graph and $\mathcal{N}$ represents a set of parameters. In a BN, the probability of each node is dependent on the conditional probability of its parent nodes defined on the parameters in $\mathcal{N}$. The above attack tree is modeled as a Bayesian attack tree to evaluate the probability of a successful intrusion to the target condition. For this purpose, the individual probability of a successful exploitation of a vulnerability is required to be calculated. Every vulnerability can be scored based on its severity of being exploited by a standard Common Vulnerability Scoring System (CVSS) [22]. Since the scores are provided on a scale from 0 to 10, they can be normalized through division by 10. The probability of a successful exploit on a vulnerability (v_i) with preconditions satisfied is given by

$$\mathbb{P}(v_i|s_i, l_i) = \frac{\mathsf{CVSS}(v_i)}{10} \tag{1}$$

where s_i and l_i respectively denote that the service and connection required to exploit the vulnerability v_i are available. For known vulnerabilities, the CVSS scores can be evaluated from [23], [24] depending on the level of access complexity, authentication requirements and other factors. The CVSS score for the zero-day exploits are evaluated as 0.8 if the severity of access complexity and authentication requirements is considered to be the highest.

Thereafter, using the Bayes' theorem, the probability of a successful exploit on a vulnerability (v_i) is calculated as

$$\mathbb{P}(v_i) = \mathbb{P}(s_i) \cdot \mathbb{P}(l_i) \cdot \frac{\mathsf{CVSS}(v_i)}{10} \tag{2}$$

The probabilities of availability of service and connection given by $\mathbb{P}(s_i)$ and $\mathbb{P}(l_i)$ respectively can be randomly selected from 0.85 to 1.0. The initial probability of availability of user privilege $\mathbb{P}(c_i)$ is considered to be 1.0 since it is assumed that the intruder is present to perform the cyber attack. For evaluating the availability of privileges in the successive target vulnerabilities, the probability of a successful intrusion through the preceding vulnerability is calculated. Therefore, the attack tree follows the structure of a *Markov Chain* where the probability of occurrence of a state is only dependent on the probability of occurrence of preceding state(s).

Certain access privileges can be achieved by exploiting more than one vulnerability from multiple prior access privileges. The probability of successfully reaching the condition c_i from n privileges $(c_j, j = 1, 2, \cdots n)$ through the m_j vulnerabilities $v_k, k = 1, 2, \cdots m_j$ is given by

$$\mathbb{P}(c_i) = \sum_{j=1}^{n} \mathbb{P}\left(\bigcup_{k=1}^{m_j} v_k \right) \mathbb{P}(c_j) \tag{3}$$

Finally the probability of successfully exploiting a target vulnerability through a minimal attack sequence is considered. It is assumed that the adversary does not waste any time in attacking multiple vulnerabilities of the same system while targeting a given goal condition. In order to calculate this probability, a backward traversal is considered from the target condition (c_i) to each of the possible vulnerabilities v_j. The probability of successful intrusion through each v_j to reach target c_i is given by

$$\mathbb{P}(v_j \wedge c_i) = \begin{cases} \mathbb{P}(v_j) \cdot \mathbb{P}(c_i|v_j), & j = 1 \\ \mathbb{P}(v_j) \cdot \prod_{k \neq j} \mathbb{P}(v_k = False), & j > 1 \\ \quad \cdot \mathbb{P}(c_i|v_j = True, v_{k \neq j} = False) & \end{cases} \tag{4}$$

III. Technical Approach

The proposed security assessment of the power system consists of two parts: (*i*)vulnerability assessment of the SCADA system associated with the grid and (*ii*) evaluating vulnerabilities in the physical power system. The net impact of a cyber attack on the SCADA system is therefore evaluated as the combined impact on the cyber system and the physical power system. Each of the system model is discussed in this section.

A. Cyber system model

The cyber system model consists of the evaluation of probability of successfully exploiting the vulnerabilities which has been detailed in Section II and the calculation of time to compromise a vulnerability. For a known vulnerability, there can be two possibilities: (*i*) intruder has the required code to exploit it and (*ii*) the intruder does not have the code to

exploit the known vulnerability. The mean time to compromise a known vulnerability is evaluated in [21] as

$$T(v_i) = \frac{10}{\mathsf{CVSS}(v_i)}\left(1 + 4.8e^{-k}\right) \quad \text{days} \tag{5}$$

For a zero day vulnerability, the two possible cases are possible: (*i*) intruder knows about the existence of the vulnerability and (*ii*) the intruder does not know about any vulnerability. The mean time to compromise a zero day vulnerability [21] is given by

$$T(v_i) = \left(32 + \frac{10}{\mathsf{CVSS}(v_i)}\right) + \left(33 + 4.8\frac{10}{\mathsf{CVSS}(v_i)}\right)e^{-k} \quad \text{days} \tag{6}$$

where k represents the capability of the intruder in identifying a possible exploit to a vulnerability. In this paper, four possible skill levels are considered for the intruder with $k = 10, 2, 1, 0.01$. These intruders are identified as expert, professional, intermediate and amateur level adversaries respectively.

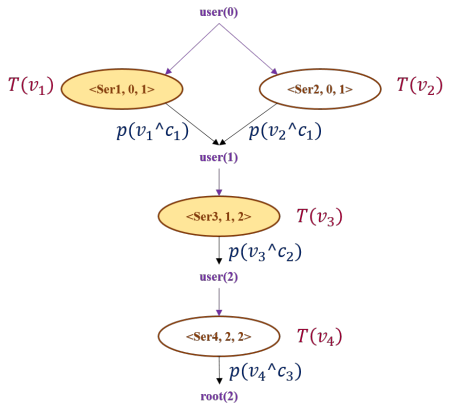

Fig. 4. Simplified attack tree targeting control center application server.

Fig. 4 shows a simplified Bayesian attack tree for the attack path in Fig. 2 where the time to compromise each vulnerability is shown beside each node and the probability of successfully reaching target condition c_i from vulnerability v_j denoted by $\mathbb{P}(v_j \wedge c_i)$ is shown beside each edge. The mean time to compromise (MTTC) and reach a target access level c_i from n possible prior access levels $c_j = 1, 2, \cdots, n$ is calculated. Let there be m_j vulnerabilities to reach from access level c_j to c_i given by $v_k, j = 1, 2, \cdots, m_j$.

$$\mathsf{MTTC}(c_i) = \frac{1}{\mathbb{P}(c_i)}\left[\sum_{j=1}^{n}\mathsf{MTTC}(c_j) + \sum_{k=1}^{m_j}\mathbb{P}(v_k \wedge c_i)\cdot T(v_k)\right] \tag{7}$$

The mean time to compromise a vulnerability with exploit code available is 1 day as evaluated in [21]. Therefore, the attack efficiency (ζ) for the target c can be calculated as

$$\zeta(c) = \frac{1}{\mathsf{MTTC}(c)} \tag{8}$$

In this paper, three substation LAN models and a SCADA model for control center are considered and the attack tree for the same are generated. In each substation model, the intruder aims to attack the human machine interface (HMI) to gain administrator access and thereafter send control signals to trip breakers in the physical power system. In the control center model, the goal of intruder is to access the application server.

Substation LAN Model A In this model, the HMI, workstations and the IEDs at a substation are connected to a common LAN network as shown in Fig. 5. A single firewall with an ethernet switch controls the passage of information to and from the network. In this case, the intruder can exploit a vulnerability in the firewall to directly access the HMI which is connected to the LAN network.

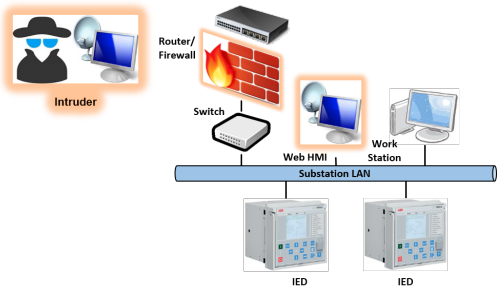

Fig. 5. Cyber intrusion scenario in Substation LAN Model A.

The attack graph is developed based on the above steps and is shown in Fig. 6. First, the intruder can exploit vulnerabilities to remotely access the HMI. Two most popularly used protocols for remote access are the file transfer protocol (FTP) and the secure shell (SSH). In this paper, vulnerabilities in these protocols have been considered for remote access of host systems. It is assumed that the FTP vulnerability is a known type and SSH vulnerability is a zero day type. Once the intruder accesses the HMI, a buffer overflow vulnerability (bof) can be exploited to gain administrator privilege on the HMI system.

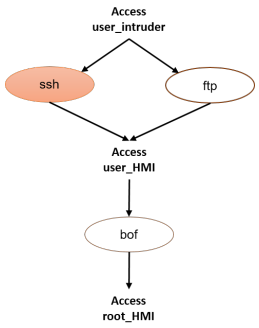

Fig. 6. Attack tree representation for Substation LAN Model A.

Substation LAN Model B In this model, the substation LAN is divided into two virtual LANs (VLANs). The substation VLAN connects the workstations, HMI and other control units and the bay VLAN connects the IEDs in the switchyard. These two VLANs communicate with a shared server which alternates between the networks through a pair of ethernet

switches as shown in Fig. 7. Such an architecture increases the level of security of the SCADA system. An intruder can exploit a vulnerability in the firewall to access the shared server. Thereafter, the HMI can be accessed by exploiting a vulnerability from the shared server. The intruder can also directly access the HMI by exploiting the vulnerabilities as in case of model A.

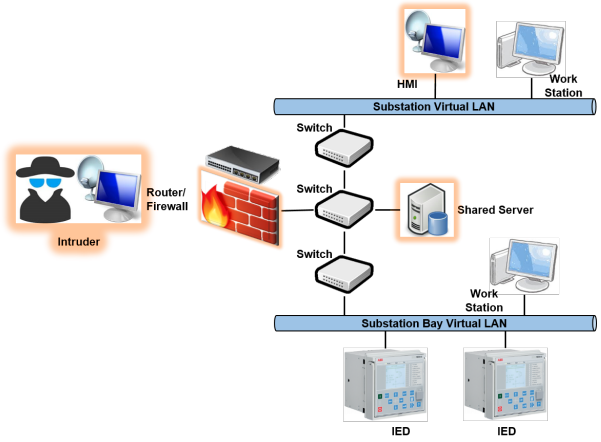

Fig. 7. Cyber intrusion scenario in Substation LAN Model B.

Fig. 8 shows the attack graph based on the above architecture. The intruder can exploit vulnerabilities to gain access of the shared server. In this case a cross scripting vulnerability (XSS) is considered which allows remote attackers to arbitrarily inject web script to access the shared server [25]. The remote access of the HMI can be done from the shared server as well as from the intruder system through the two popularly used protocols FTP and SSH. It is assumed that the XSS and FTP vulnerabilities are known type and SSH vulnerability is zero day type. Once the intruder accesses the HMI, a buffer overflow vulnerability (bof) can be exploited to gain administrator privilege on the HMI system.

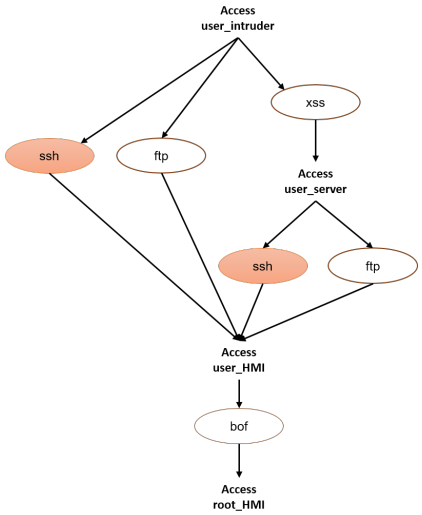

Fig. 8. Attack tree representation for Substation LAN Model B.

Substation LAN Model C Fig. 9 shows the architecture of this LAN model. In this case, a local SCADA system connects all components in the substation LAN. The HMI cannot be accessed remotely and all communication has to pass through the local SCADA system. An intruder can exploit a vulnerability in the firewall to access the local SCADA system. Thereafter, the HMI can be accessed by exploiting a vulnerability from the local SCADA. Finally, vulnerabilities within the HMI can be exploited to gain administrator privilege on the system.

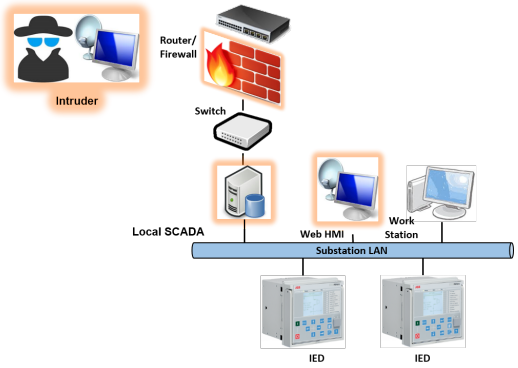

Fig. 9. Cyber intrusion scenario in Substation LAN Model C.

The attack graph for this LAN architecture is shown in Fig. 10. The intruder can exploit a HTTP vulnerability in the SCADA firewall to gain access of the local SCADA system. This vulnerability can cause denial of service (DoS) in the servers as discussed in [26]. The remote access of the HMI can be done from the SCADA through FTP and SSH. It is assumed that the HTTP and FTP vulnerabilities are known type and SSH vulnerability is zero day type. Once the intruder accesses the HMI, similar to the previous cases, a buffer overflow vulnerability (bof) can be exploited to gain administrator privilege on the HMI system.

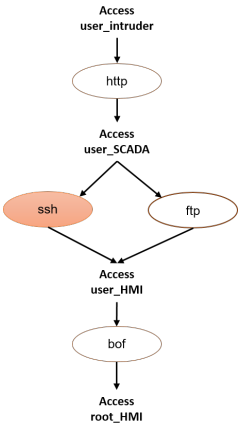

Fig. 10. Attack tree representation for Substation LAN Model C.

Control Center SCADA Model Fig. 11 shows the SCADA system for a control center. In this case, an intruder can

exploit a vulnerability in the firewall to access the database server. Thereafter, the application server can be accessed by exploiting a vulnerability from the database server. Finally, vulnerabilities within the application server can be exploited to gain administrator privilege on the system.

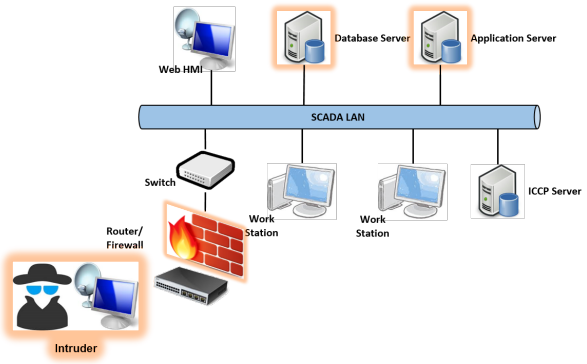

Fig. 11. Cyber intrusion scenario in control center SCADA system.

The attack graph for this control center architecture is shown in Fig. 12. The intruder can exploit two vulnerabilities (denial of service (DoS) and Exec Code Overflow (exe)) [27] in the SCADA firewall to gain access of the database server. The remote access of the HMI can be done from the SCADA through FTP and SSH. It is assumed that the HTTP and FTP vulnerabilities are known type and SSH vulnerability is zero day type. Once the intruder accesses the HMI, similar to the previous cases, a buffer overflow vulnerability (bof) can be exploited to gain administrator privilege on the HMI system.

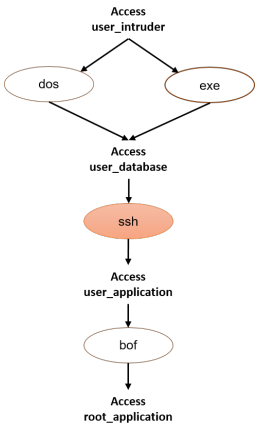

Fig. 12. Attack tree representation for control center SCADA system.

B. Physical system model

For modeling the physical system, the individual substations are required to be identified along with the associated IEDs. Thereafter, the possible combination of the IEDs are considered and contingencies are simulated based on these combinations. For example in Fig. 13 the substation with buses 2 and 30 has 6 IEDs controlling the circuit breakers

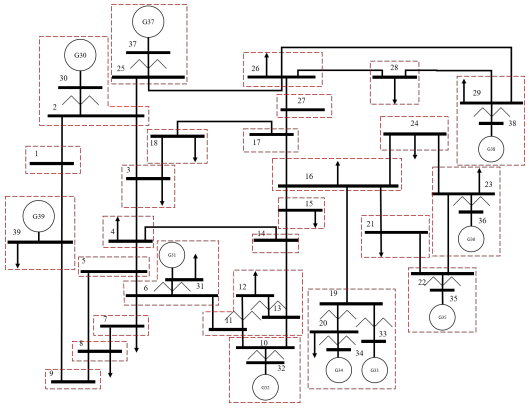

Fig. 13. IEEE 39 bus system with 27 substation.

for generator G39, transformer HV and LV sides, and three transmission lines. There can be 63 combinations of these IEDs and the list of contingencies are shown in Fig. 14.

Fig. 14. List of contingencies when HMI of substation 2 is compromised.

For each of these contingencies, a dynamic simulation is carried out for 10 seconds. Therefore, the impact when an HMI is compromised and target IED set S is attacked can be evaluated as

$$I(\mathsf{S}) = \beta_f \frac{\Delta f}{\Delta f_{\text{rated}}} + \beta_v \frac{1}{N} \sum_{i=1}^{N} \frac{\Delta V_i}{\Delta V_{\text{rated}}} \tag{9}$$

where Δf and ΔV represent the maximum frequency and voltage deviation respectively and they are normalized to the rated deviations of 1% and 5% respectively. β_f and β_v are the suitable weighting factor and N is the total number of buses in the system. Fig. 15 shows the impact of 63 possible contingencies when IEDs of substation 2 are targeted. The impact has been calculated with $\beta_f = \beta_v = 0.1$.

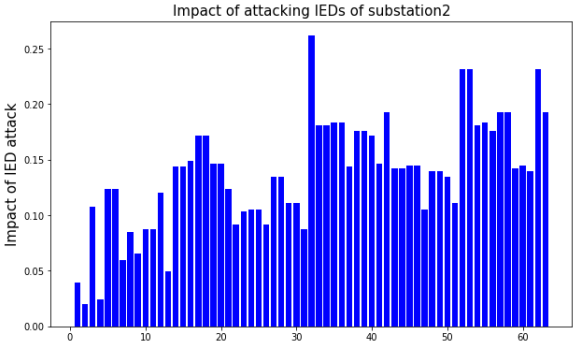

Fig. 15. Impact of attacks on the IEDs of substation 2.

Let $\mathcal{T}_c = \{\mathsf{S}_1, \mathsf{S}_2, \cdots, \mathsf{S}_\mathsf{M}\}$ be the list of possible contingencies which can be created when the target vulnerability (HMI at substation 2) is compromised. The resulting risk (R) associated with the cyber attack on the target vulnerability c is given by

$$R(c) = \zeta(c) \cdot \frac{1}{M} \sum_{i=1}^{M} \mathsf{S}_\mathsf{i} \tag{10}$$

The mean impact of all possible contingencies from a compromised HMI is considered as the measure of physical impact of the cyber attack. From Fig. 15 the physical impact of compromising the HMI at substation 2 is 0.138. This is the mean impact of all the 63 possible contingencies.

IV. Simulation and Results

A. Cyber system security evaluation:

The three substation cyber system models are designed as discussed in Section III. The SSH vulnerability is considered to be a zero day type and the CVSS score for it is 0.8. For the other vulnerabilities, the vulnerability database is used to determine the CVSS scores [23]–[27]. The CVSS scores for the vulnerabilities are listed in Table I.

TABLE I
CVSS SCORES OF VULNERABILITIES

Vulnerability	ssh	ftp	http	xss	bof	exe	dos
CVSS score	0.8	6.4	9.3	4.5	6.8	10.0	5.0

Fig. 16 shows the mean time to compromise a substation HMI when model A LAN architecture is used for all the substations. The red colored graph shows the mean time taken by an expert intruder to compromise the HMI. The yellow, green and blue graphs show the same for adversaries with professional, intermediate and amateur skill level respectively.

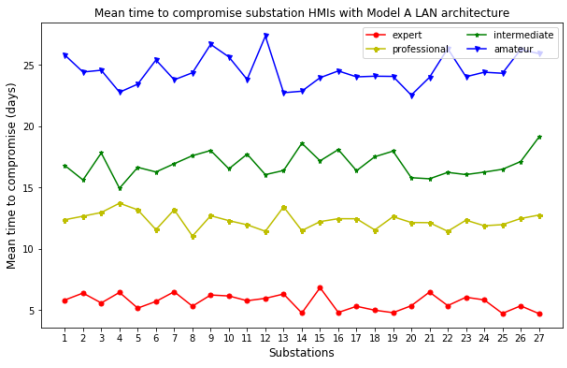

Fig. 16. Mean time to compromise substation HMIs with model A LAN architecture for different intruders.

It is evident that the time taken by an expert adversary to compromise an HMI is the least followed by a professionally skilled intruder and intermediate level. The amateur adversary takes the longest to compromise the HMIs in the substation. Similar results can be observed for other substation LAN architectures and control center model.

Fig. 17 compares the security of different substation LAN architectures. The red graph shows the mean time to compromise a HMI in LAN architecture A for an adversary with intermediate skill level. The same intruder requires more time to exploit vulnerabilities in architectures B and C. Therefore, LAN models B and C are more secure than model A. The yellow graph shows the mean time to compromise the application server in a control center overseeing the substation. It is observed that the control center cyber system has a higher security than the substation LAN models.

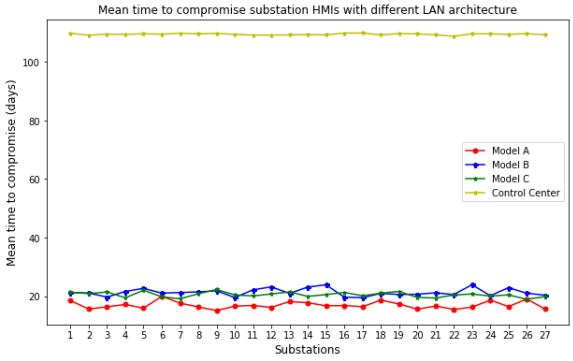

Fig. 17. Mean time to compromise SCADA systems in substations and control center.

B. Risk assessment of cyber-physical system:

Fig. 18 shows the impact of a cyber-physical attack on substation HMIs in the IEEE 39-bus power system. There are 27 substations as shown in Fig. 13. The LAN architecture for each substation is randomly selected from the three models (Model A, Model B and Model C). The physical impact of a cyber attack at a substation is the mean impact of all possible contingencies if the HMI of the substation is compromised. The green graph shows the physical impact for a compromised HMI at each substation. The blue graph shows the attack efficiency for each substation SCADA system. The red graph depicts the risk associated with a cyber-physical attack on the substation HMIs.

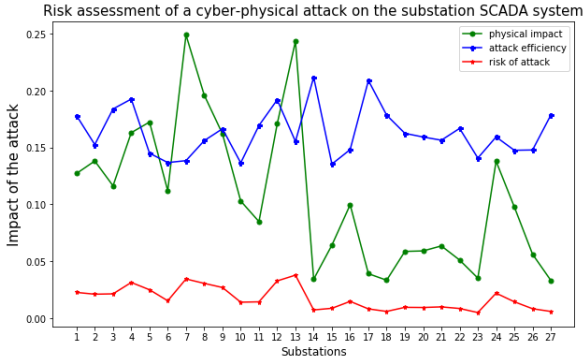

Fig. 18. Impact of a cyber-physical attack on the substation LAN.

Fig. 19 shows the impact of a cyber-physical attack on control center application server in the IEEE 39-bus power system. Comparing this type of attack with the attack on substation, it is observed that the LAN models of substations are more vulnerable than the control center SCADA system.

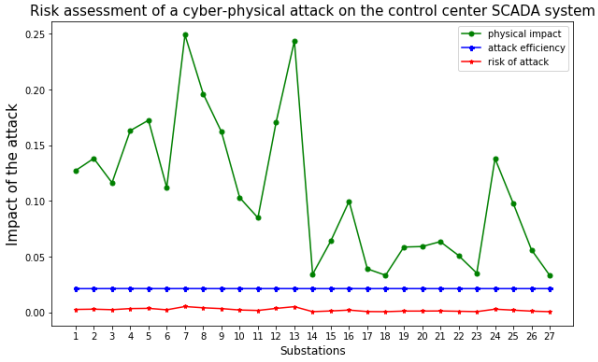

Fig. 19. Impact of a cyber-physical attack on the control center SCADA.

V. Conclusion

A Bayesian attack tree approach has been used to model cyber attacks in the SCADA networks of substations and control centers. The attack trees are identified based on the probable intrusion paths in each SCADA system with a goal to gain administrative access in control assets of the network. The vulnerabilities in each attack path and probability of their successful exploit are identified based on the latest vulnerability statistics in cyber systems. The time to compromise vulnerabilities is calculated for each of them and considered as a metric of intruder attack efficiency. The risk of a cyber attack is assessed from the attack efficiency as well as the impact on power grid.

In this work, each vulnerability is considered to be distinct from one another. In reality, some vulnerabilities are common in all systems. If the exploit code is available to the adversary, time to compromise a known vulnerability reduces significantly. This modification to the evaluation of time to compromise can be considered as a scope of future work. The present work is focused on cyber attacks to gain unauthorized access to control assets in the SCADA network. A similar approach can be used to model man-in-the-middle attacks using flooding of queues which can be another possible scope of future work.

References

[1] National Academies of Sciences, Engineering, and Medicine, "Analytic Research Foundations for the Next-Generation Electric Grid," The National Academies Press, Washington, DC, Tech. Rep., 2016.

[2] C. L. Barrett, S. Eubank, C. Y. Evrenosoglu, A. Marathe, M. V. Marathe, A. Phadke, J. Thorp, and A. Vullikanti, "Effects of Hypothetical Improvised Nuclear Detonation on the Electrical Infrastructure," in *International ETG-Congress 2013; Symposium 1: Security in Critical Infrastructures Today*, vol. 1, no. 1, Nov 2013, pp. 1–7.

[3] C. D. Brummitt, R. M. D'Souza, and E. A. Leicht, "Suppressing Cascades of Load in Interdependent Networks," *Proceedings of the National Academy of Sciences*, vol. 109, no. 12, pp. E680–E689, Mar 2012.

[4] C. Liu, A. Stefanov, J. Hong, and P. Panciatici, "Intruders in the Grid," *IEEE Power and Energy Magazine*, vol. 10, no. 1, pp. 58–66, Jan 2012.

[5] S. M. Amin and B. F. Wollenberg, "Toward a Smart Grid: Power Delivery for the 21st Century," *IEEE Power and Energy Magazine*, vol. 3, no. 5, pp. 34–41, Sept 2005.

[6] CIGRE, "Security for Information Systems and Intranets for Electric Power Systems," *ELECTRA Tech. Brochure*, vol. 231, no. 317, pp. 70–81, Apr 2007.

[7] W. Wang, S. Yang, F. Hu, H. E. Stanley, S. He, and M. Shi, "An Approach for Cascading Effects within Critical Infrastructure Systems," *Physica A: Statistical Mechanics and its Applications*, vol. 510, no. 1, pp. 164 – 177, Nov 2018.

[8] R. E. Mackiewicz, "Overview of IEC 61850 and Benefits," in *2006 IEEE PES Power Systems Conference and Exposition*, Oct 2006, pp. 623–630.

[9] L. Wang, S. Jajodia, A. Singhal, P. Cheng, and S. Noel, "k-Zero Day Safety: A Network Security Metric for Measuring the Risk of Unknown Vulnerabilities," *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 1, pp. 30–44, Jan 2014.

[10] Y. Zhang, L. Wang, Y. Xiang, and C. Ten, "Power System Reliability Evaluation With SCADA Cybersecurity Considerations," *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1707–1721, July 2015.

[11] J. Stamp, A. McIntyre, and B. Ricardson, "Reliability Impacts from Cyber Attack on Electric Power Systems," in *2009 IEEE/PES Power Systems Conference and Exposition*, March 2009, pp. 1–8.

[12] T. Pultarova, "Cyber Security - Ukraine Grid Hack is Wake-up Call for Network Operators [News Briefing]," *Engineering Technology*, vol. 11, no. 1, pp. 12–13, 2016.

[13] A. C. K. Gary and U. N. Prananto, "Cyber Security in the Energy World," in *2017 Asian Conference on Energy, Power and Transportation Electrification (ACEPT)*, Oct 2017, pp. 1–5.

[14] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava, "Analyzing the Cyber-Physical Impact of Cyber Events on the Power Grid," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2444–2453, Sept 2015.

[15] C. Ten, C. Liu, and G. Manimaran, "Vulnerability Assessment of Cybersecurity for SCADA Systems," *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1836–1846, Nov 2008.

[16] T. M. Chen, J. C. Sanchez-Aarnoutse, and J. Buford, "Petri Net Modeling of Cyber-Physical Attacks on Smart Grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 741–749, Dec 2011.

[17] S. Sridhar, M. Govindarasu, and C. Liu, "Risk Analysis of Coordinated Cyber Attacks on Power Grid," in *Control and Optimization Methods for Electric Smart Grids*, 1st ed., A. Chakrabortty and M. D. Ilić, Eds. New York, NY: Springer New York, 2012, pp. 275–294.

[18] J. Xie, A. Stefanov, and C. Liu, "Physical and Cyber Security in a Smart Grid Environment," *Wiley Interdisciplinary Reviews: Energy and Environment*, vol. 5, no. 5, pp. 519–542, Mar 2016.

[19] A. Stefanov, C. Liu, M. Govindarasu, and S. Wu, "SCADA Modeling for Performance and Vulnerability Assessment of Integrated Cyberphysical Systems," *International Transactions on Electrical Energy Systems*, vol. 25, no. 3, pp. 498–519, Dec 2013.

[20] A. Stefanov and C. Liu, "ICT Modeling for Integrated Simulation of Cyber-Physical Power Systems," in *2012 3rd IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe)*, Oct 2012, pp. 1–8.

[21] M. A. McQueen, W. F. Boyer, M. A. Flynn, and A. G. Beitel, "Time-to-Compromise Model for Cyber Risk Reduction Estimation," in *Quality of Protection: Advances in Information Security*, 1st ed., D. Gollmann, F. Massacci, and A. Yautsiukhin, Eds. Boston, MA: Springer US, 2006, pp. 49–64.

[22] P. Mell, K. Scarfone, and S. Romanosky, "Common Vulnerability Scoring System," *IEEE Security Privacy*, vol. 4, no. 6, pp. 85–89, Nov 2006.

[23] National Institute of Standards and Technology. National Software Reference Library. [Online]. Available: http://www.nsrl.nist.gov

[24] National Institute of Standards and Technology. National Vulnerability Database Version 2.2. [Online]. Available: https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator?name=CVE-2007-1001, 2007

[25] CVE Database of FTP Vulnerability. CVE Details. [Online]. Available: https://www.cvedetails.com/vendor/2/FTP.html

[26] CVE Database of HTTP Vulnerability. CVE Details of Apache HTTP Vulnerability. [Online]. Available: https://www.cvedetails.com/vendor/45/Apache.html

[27] CVE Database of SSH Vulnerability. CVE Details of SSH Vulnerability. [Online]. Available: https://www.cvedetails.com/vendor/120/SSH.html