Improving Attack Trees Analysis using Petri Net modeling of Cyber-Attacks

Shabnam Pasandideh
Universidade Nova de Lisboa – FCT – DEEC & UNINOVA – CTS
Portugal
shabnam.pasandide@uninova.pt

Luis Gomes
Universidade Nova de Lisboa – FCT – DEEC & UNINOVA – CTS
Portugal
lugo@fct.unl.pt

Pedro Maló
Universidade Nova de Lisboa – FCT – DEEC
Portugal
pmm@fct.unl.pt

Abstract— Cyber security is one general concern to all network-based organizations. In recent years, by significant increasing cyber-attacks in critical infrastructures (CIs) the need of smart prediction, awareness and protection systems is not deniable. The first step for security assessment is on recognizing and analyzing attacks. In this paper, one of the graphical security assessments named Attack Tree (AT) is used to illustrate one kind of cyber-attacks scenario in Industry 4.0 and the system's behavior is analyzed by Petri Nets.

Keywords— ***Petri nets, Attack Trees analysis, Industry 4.0, Cyberattacks***

I. Introduction

Cyber physical systems (CPS) can be characterized as an integration of physical subsystems with computing and networking capabilities [1]. CPS concept includes support for networking of several devices and integrates the control of them. CPS can be seen as an evolution of the old concept of "embedded systems", where networking is included. Networking techniques brings timing variability and stochastic behavior [2].

CPS has been increasingly recognized as a core function of a new paradigm in manufacturing which is called Industry 4.0 as fourth industry revolution [3]. Industry 4.0 is a German strategic initiative with cross multidisciplinary approach to aim creating intelligent factories included transformed CPSs, the Internet of Things (IoT), cloud computing and Big Data. In this era, physical processes are monitored by manufacturing systems, the so-called digital twins, supporting smart and real time decisions. This includes communication and collaboration among human, sensors and machines [4]. As a result, intelligent factories commonly integrate following characteristics: smart networking, mobility, flexibility, integration of customers, new innovation business models [5]. Industry 4.0 has cyber and physical vulnerability which provides some threats for the system. Apparently, reaching the goal point of Industry 4.0 requires high confidence of system security, specifically cyber security and provide efficient defense and countermeasure systems. In Table I, main cyber-attacks are categorized and briefly described [6]. As in the Table is shown, the aim of cyber-attack is disrupting of data or information integrity or authenticity [7]. An attacker's behavior is not deterministic and designing systems that be completely secured is not possible, some combination methodology is needed, included deterministic and stochastic to analysis the performance of systems under attacks.

Moreover, the classic solutions for cyber security in CPSs are not sufficient to cover analysis security of the system as a whole, not from network, communication or physical security viewpoints separately. For example, during the last years, some researches toward cyber security have been conducted to visualize the analysis. The proposed models include Attack tree/graphs (AT/AG), Attack Vector, Attack surface, Diamond model, OWASP's threat model and Kill Chain [8]. Due to find the path and potential attacks, attack tree/graph are widely used in different application domains from E-commerce, network monitoring systems, online game systems, cyber physical systems, to social systems [9].

In addition, stochastic characterization can properly evaluate and analyze the systems' performance in uncertain environment. In this regard, Petri nets are successfully used in security analysis [9] and they can contribute to fill the gaps in AT/AG models.

The motivation of this study arises from the important role of cyber security in industrial CPSs within I4.0, which needs to obtain a solution to analyze the performance of CPSs under attacks.

The aim of this work is to apply techniques to the analysis of attack-defense trees and evaluate performance of the system by focus on resilience. In this paper, the authors use a graphical security assessment tool namely Attack Tree (AT) to illustrate attacks process as a static part of security analysis intrusion detection for each attack. Following that, a new framework to translate attack countermeasure tree (here intrusion detection) to Petri nets is proposed based on some defined translation rules. Expected result will show the dynamic behavior of the system under attack and defense, therefore the accuracy and resilience of each intrusion detection systems under cyber-attacks.

Paper organization. Section II addresses literature review of ATs and PNs; Section III proposes a translation of common types of cyber-attacks into Petri nets; Section IV applies ATs and PNs for a given scenario; Finally, in section V the conclusion of the work is provided.

II. Literature Review

A. Attack Trees

To anticipate and prevent harms and damages caused by cyber-attacks it is of paramount importance to understand how to secure cyber physical systems. [9].

Attack trees are generating considerable interest in terms of system's security modelling. It is one type of logic trees which model sequential and multiple actions of an adversary(ies) to defeat a defensive system. AT was one of the process of security analysis in defense department of US. After all it is coined by Schneier and formulated basically by him and Mauw [10],[11] as an advanced work on that. Attack tree is built by mainly three graphical components, namely Nodes, Edges and combinators or logical gates. Initially, AT is for formulating independent events, which in security term are called attacks.

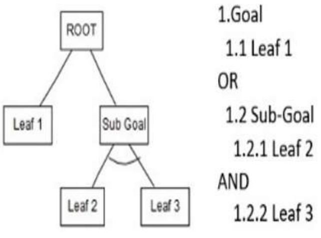
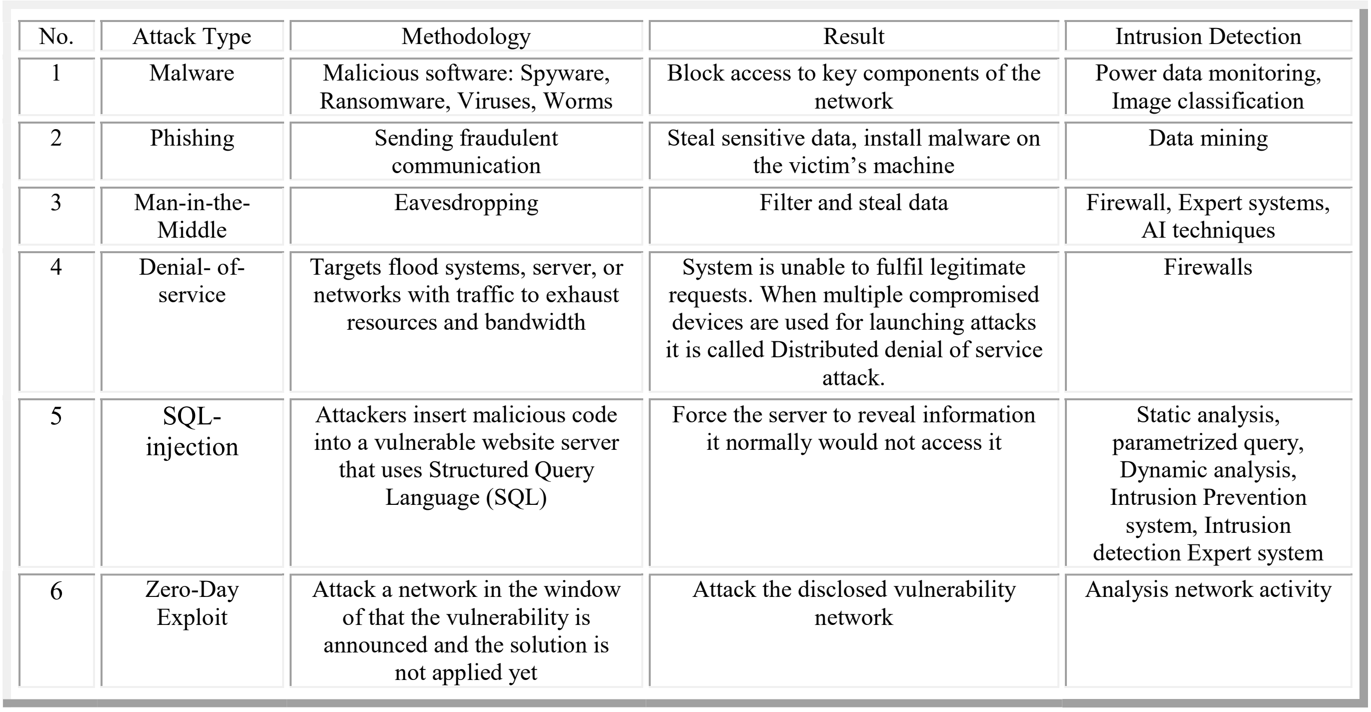


Fig. 1. Attack tree representations.

TABLE I. Cyber Attack Types



No.	Attack Type	Methodology	Result	Intrusion Detection
1	Malware	Malicious software: Spyware, Ransomware, Viruses, Worms	Block access to key components of the network	Power data monitoring, Image classification
2	Phishing	Sending fraudulent communication	Steal sensitive data, install malware on the victim's machine	Data mining
3	Man-in-the-Middle	Eavesdropping	Filter and steal data	Firewall, Expert systems, AI techniques
4	Denial- of-service	Targets flood systems, server, or networks with traffic to exhaust resources and bandwidth	System is unable to fulfil legitimate requests. When multiple compromised devices are used for launching attacks it is called Distributed denial of service attack.	Firewalls
5	SQL-injection	Attackers insert malicious code into a vulnerable website server that uses Structured Query Language (SQL)	Force the server to reveal information it normally would not access it	Static analysis, parametrized query, Dynamic analysis, Intrusion Prevention system, Intrusion detection Expert system
6	Zero-Day Exploit	Attack a network in the window of that the vulnerability is announced and the solution is not applied yet	Attack the disclosed vulnerability network	Analysis network activity

Nodes include root (goal) or parent, sub-goal or children and leaves. AT is top-down tree which is structured based on the goals. Children (sub-goals) or intermediate nodes show the ways to achieve the particular goal (In AT called root node means the goal of attackers, instead for Defense tree the root is defined as the goal of defenders). These nodes refine to basic level or atomic attacks called leaf nodes. A refinement can be conjunctive (aggregation) or disjunctive (choice) [11]. The former one is described and formulated by AND logic gates, which means that all the requirements should be met, and the latter one defined by OR, meaning that any of the requirements is enough to reach the upper node.Also, some values/attribution assigned to the leaf nodes can be Boolean e.g. Possible/Impossible, or numerical assessments such as cost, impact, severity of attack [10]. Text representation of ATs makes it easily readable, supporting its comparison and computing. Representing attack graphs was not enough to the analysis of performance and survivability of the system, and it was a need for adding countermeasures and defenses to the trees In this regard, attack defense tree (ADT) [12], and attack countermeasures (ACT) [13] have been proposed. Kordy [14] introduced a new concept called Attack Defense Tree (ADT), which decorated AT by Defense nodes not only in Leaf level but in any levels of the Tree and provide a tool to generate the ADTs named ADTools [15]. In another work by Edge in his Ph.D. dissertation, Protection Tree (PT) is introduced, which assigned protection (countermeasure) events to nodes. It means that instead of using attack or vulnerability analysis, the protections for each event will be analyzed. This process should be continued from the leaf nodes to cover root nodes by a protection [16]. Kumar et al. [17] proposed another extension of AT, which analysis both security and safety of the system named Attack Fault Tree (ATF). This model has an advantage that analyzers can consider two situations of the system in a single model.

Much work on the potential of ATs has been carried out [18] yet, because of their efficiency and simple structure. As the primary benefits of AT [19] are that it provides convenient representation for defenders to identify potential attacks and paths against their systems and empower decision makers to choose or define proper countermeasures or protections. Also, they have self-documenting nature. In addition, textually representation of the attacks makes it possible to automatic processing and generated by different languages as Java, Extensible Markup Language (XML) in complex systems [20]. Hong, Kim, and others [9] [18] have an accomplished survey about the usability and practical applications of Graphical Security Models (GrSMs), which they analyze in terms of networked system security analysis regarding efficiency, application of metrics, and availability of tools. The represented models are not considered from the point of view of probabilistic and stochastics of possible events.

Considering cyber-attacks, the most important focus is on outside activities and attackers' behaviors. It means that modeling attacks should be formalized as independent events by stochastic characteristics. In this sense, it is adequate to apply stochastic models for analysis of the behavior of the system.

In some extent, the nature of attacks that is based on human intention is commonly dependable which comparing the accidental nature of faults in the systems. Because of that we suggest modeling attacks and then define the proper defense for them by independent approach [21].

Model specification of attacker's behavior and system's intrusion needs the combination of the appropriate state-based models and attack tree's analysis. For this respect, authors apply Petri nets to analyze the system.

B. Petri Nets

A Petri Net is a mathematical and graphical formalism, first introduced by Carl Adam Petri, a German mathematician in the 1960s [22]. Petri nets were introduced for modelling of the system's behavior using the concepts of event and condition. Petri nets as a graphical model is a directed bipartite graph using Places, Transitions, and Arcs, which in order shows the components, elements, actions, and events, as well as connections between transitions and places. Current state of the systems is shown by tokens associated with places, and the dynamics depend on the transition firing rules. In Fig. 2 a simple Petri net is shown.

Petri nets contribute with more flexibility to describe systems' behavior, for instance the ability to represent concurrency which is one of the limitations of the traditional attack trees. There are some proposed techniques to overcome this problem using Petri nets [23].

The first proposal of applying Petri Nets for modelling attacks by attack tree was by McDermontt [24]. In this model transition and places correspond to nodes and attack actions in attack trees. In Petri Nets, transitions are enabled to fire if all the places connected to them are marked, which defines the AND semantic. Also, it is possible to define AND semantics by adding new places in the net [25].

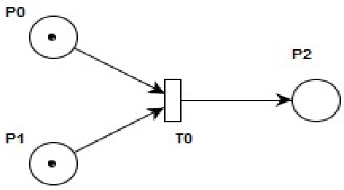


Fig. 2. Petri Net enabled transition

Generalized Stochastic Petri nets (GSPN) were proposed by Balbo and Conte to solve some limitations of other Petri nets classes, including:

- Complexity of their analysis: the possibility to have very large number of reachable marking [26].
- Model solution complexity: presence in one model of activities that take place on a much faster (or slower) time scale than the one relating to the events that play a critical role on the overall performance [27].

GSPN is an extension of Stochastic Petri nets (SPN) by allowing infinite transition firing rates, comprise two types of transitions: Timed transitions, which are associated with random, exponentially distributed firing delays, as in SPN, and Immediate transitions, which fire in zero time with firing probabilities.

C. Intrusion Detection Systems (IDS)

Intrusion detection is a common cyber security mechanism that reside on the network or host to detect suspicious or malicious activities and alarm the system [28]. The detection of malicious activities enables timely reaction, for example, stop or ongoing attack. Intrusion Detection Systems (IDS) for detecting cyber-attacks, mainly categorized into two groups: Anomaly-based and signature-based data. Based on techniques for monitor and analysis intrusion, there is a classification as presented in Fig. 3 [29]. A network-based intrusion (NIDS) monitors the traffic and activities on a network and look for signs of intrusion in that data, (using, for example, the well-known software Snort). A host-based intrusion (HIDS) monitors and analysis log files in a particular system (using, for example, the open source software OSSEC).

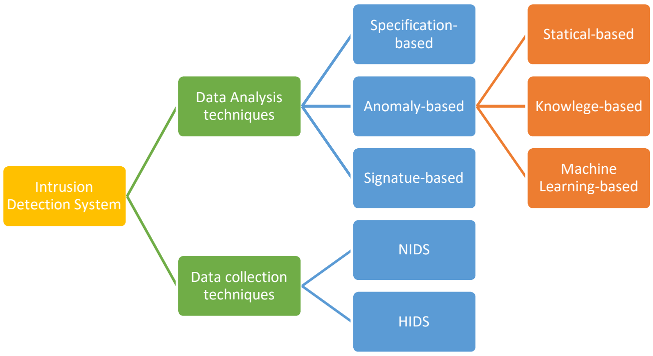


Fig. 3. Intrusion Detection Classification

There are common basic indicators to evaluate performance of IDS. In table II the basic metrics for evaluating the performance of IDS is provided. False positive and false negative rates are considering the noise of an IDS.

TABLE II. Security Metrics for IDS

Metrics for attack detection	Definition
True Positive (TP)	The number of malicious executables correctly detected as malicious
True Negative (TN)	The number of benign programs correctly detected as benign
False Positive (FP)	The number of benign programs falsely detected as malicious
False Negative (FN)	The number of malicious executables falsely detected as benign

To evaluate the performance of the IDS, the rates of accuracy, detection and false alarm are widely used as can be obtained by these equations [30]:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

$$False\ Alram = \frac{FP}{FP+T} \quad (2)$$

$$Detection\ rate = \frac{TP}{TP+FP} \quad (3)$$

III. Cyber Attack Analysis

A. *Translations ATs to Generalized Stochastic Petri nets*

Beside strengths of Attack Trees, they support the static part of attack scenarios and for describing and analysis dynamic part specially in system levels, another tool is needed. By modelling a system, it is possible to describe consisting of entities and relationship between them.

As described in section II.B, Petri nets are a promising candidate to this area. In this paper we translate Attack Tree and then Attack-Detection Trees to Generalized Stochastic Petri nets (GSPN). The main reason to select GSPN for modelling and analysis the security of the system is its ability to show the dynamic behavior and stochastic variables in the system under attack. It means that each attack scenario can be an option for the system [31]. In addition, as cyber-attacks can be stochastic and independent, it is important to analysis security of CPSs by considering these characteristics.

Fig. 4 graphically presents a simple example of an AT. The goal of attacker, is shown by root node and the sequence of activities to reach this node are shown by events (E). Here, D1 is used for intrusion detection as a defense technique.

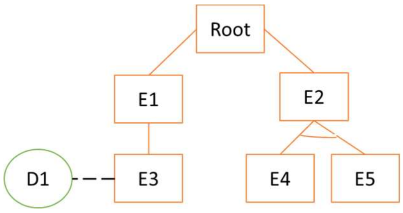


Fig.4. Attack Tree with Detection Intrusion

For translating ATs to GSPNs, the rules presented in Fig. 5 are proposed, defining translation to each node.

In this methodology, the translation of leaf nodes and sub-goals are represented by transitions in the generated PN model. Places in the PN model represent the arcs in AT. Gradually the attack can be executed to the ultimate goal that is represented by Root node in the AT that will be shown by a place in the PN model, representing the state of the system regarding the attack. For a successful attack, this place is marked with a token. Constructs considered in the translation mechanisms shown in Fig. 5:

- Sequence; in the AT, E1 a depended event by conducting E2, which in PNs is translated in a sequence.
- OR; in the AT, it defines the two possible events which is translated to concurrency in PNs. E2 and E3 are called concurrent if they are neither casually dependent nor in with conflict one another.
- AND; In the AT means two dependent events that in PN, E1 cannot be fire without firing E2 and E3.
- Finally, detection node in the AT is shown by a loop in Petri nets.

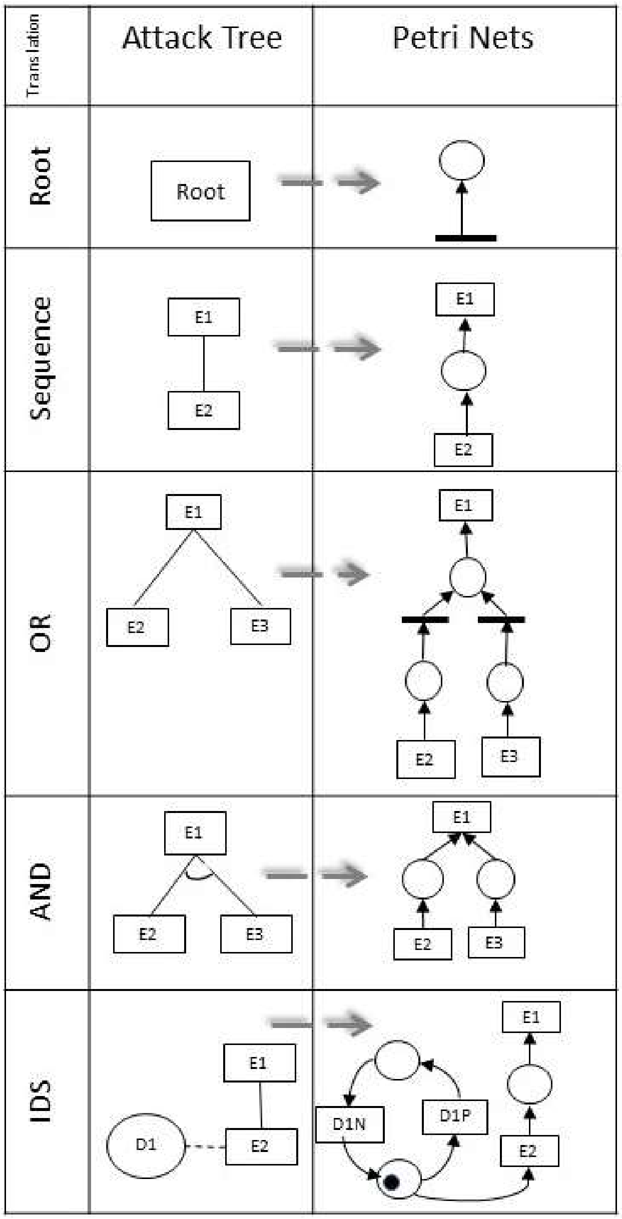


Fig. 5. Translation rule for AT structure to PNs

Applying the rules presented in Fig. 5 to the AT of Fig. 4, the PN model is obtained as Fig.6.

B. Attack detection tree analysis

Full automated process in the Industry 4.0 makes cyber and physical environment vulnerable to cyber-attacks. Here, we use the simulated cyber-attack in [32]. The five attack vectors that can get control and disturb normal procedure of the system is categorized as: Repackaging, Cross Site Request Forgery (CSRF), Shellshock, Race condition and SQL injection. In I4.0, customers can select their product and its features from a third-party online store. Repackaging attack happens when adversaries download an app and obtain the original code by reverse engineering and inject their malicious code to it and repackage and release it on the app market. Another vector called Cross Site Request Forgery (CSRF) which attacker can take over of end users' actions as POST or GET. For reaching this goal, attacker send a malicious link or website via the user's browser. Shellshock attack, which is also known as the bash bug, is an attack that effects most versions of the Linux and Unix operating systems. Successful attacker can gain control over a targeted computer. The last but not the least frequent attack is SQL injection, which is a code injection technique, used to attack data-driven applications. In this attack, Advisories by code injection technique tries to spoof identity in order to disclosure data and as a successful result act as a database server administrator. The common defense action is using Intrusion detection systems (IDS). Intrusion detection is the activity of detecting actions that intruders carry out against Information systems. The aim of these actions is to obtain unauthorized access to a computer system.

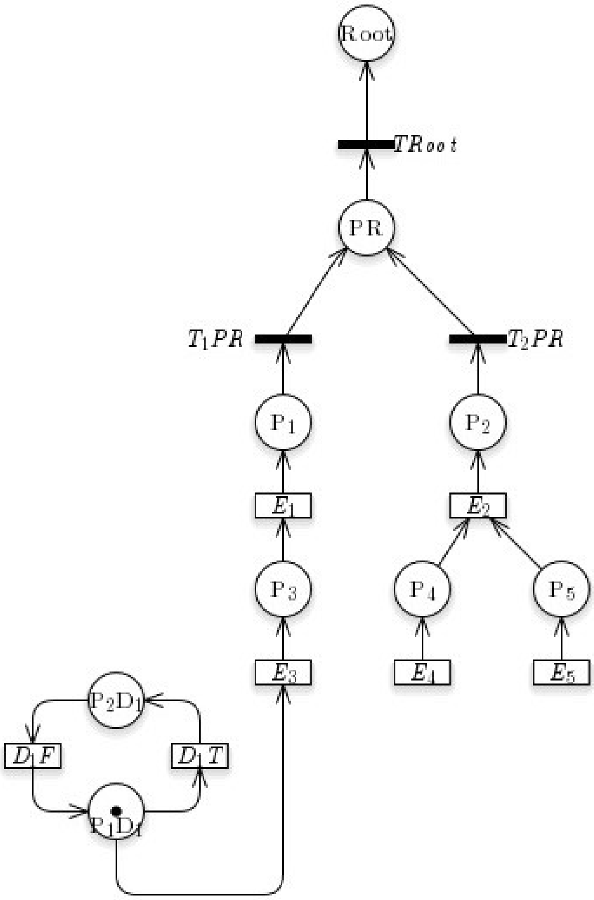


Fig. 6. GSPN model of the Attack tree with Detection Intrusion of Fig. 4.

The objectives of Intrusion detections are detecting and alarming true attacks, notify the network administration of the malicious activities. In Fig. 7 the attack tree for describing one scenario is illustrated. In this scenario, injecting malicious code to target spindle speed and by POST malicious form in the website are shown in the AT. The defense mechanism is shown by green circles. The goal of the attacker is access to the data base and authorized as the administrator to manipulate information. Obtaining this objective, there are some possible attempts by the attacker that shows the path of the attack. Utilizing AT, provide a the graphical document for security team to elaborate in their decision-making process for assigning intuitive defense strategy for the system. IDS are considered as one of the defense solutions that expected to detect attacks and block them

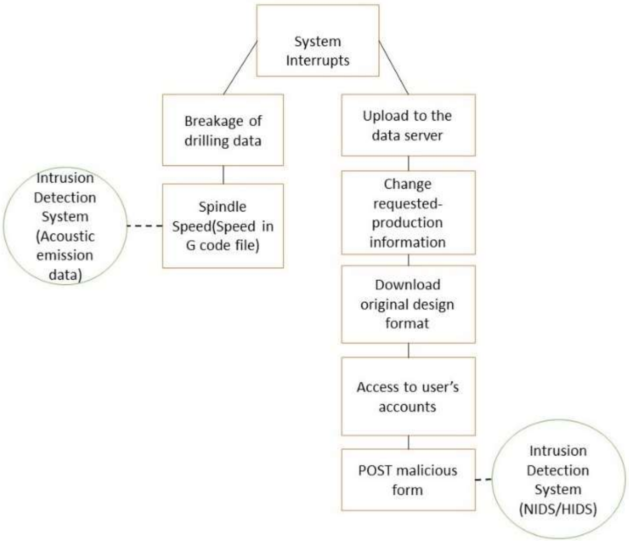

System Interrupts
Breakage of drilling data
Upload to the data server
Intrusion Detection System (Acoustic emission data)
Spindle Speed(Speed in G code file)
Change requested-production information
Download original design format
Access to user's accounts
POST malicious form
Intrusion Detection System (NIDS/HIDS)

Fig. 7 Attack Tree decorated by Intrusion Detection

IV. Application of security analysis in I4.0 by GSPN based on Attack Tree

In this work, it is proposed to translate each event as a transition in PNs considering Immediate transition for the kind of attacks which happen as a sequence result of certain attack. For independent and distributed attacks Exponential transitions are defined. General Transitions illustrate consequence of some actions which happens in an interval time. Estimated time and probabilistic to conduct an attack successfully depend on attacker's technical skill, social engineering skills, facilities, level of access to information resources, and so on. On the other hand, the maturity level of organization's security systems, their team education and knowledge, also resources and so on are other effected parameters which determines values of each leaves.

Translating ATs to GSPNs gives an opportunity to analysis probability, time for attacks and evaluate resilience of each intrusion detection systems for each attack. The idea of modelling system with PNs is showing the behavior of the system regarding possible reaction of the system to each attack.

In this paper, we chose one of the potential cyber-attacks in I4.0 that was mentioned in section III.A. In this work, the provided example is about a 3D printer. In this case, the attacker goal using cyber-attack vectors such as SQL injection is to increase feed speed that causes tool damages and as a result, a low finish quality product. As a result, the attacker may control spindle speed G-code file and concluded to the breakage of drilling bits. Each attack vectors related to Intrusion Detection systems are represented in Fig. 5 [32]. When attacker publish a malicious form in the website there are three possibilities: 1. User open and fulfil the form; 2. user informs the fraud and doesn't use it; 3. intrusion detection system is active and detects the fraud and abandon the attack and remove the form and block the access of attackers to the website.

The proper model to show the behavior of all the system by considering random behavior of attackers and not in the deterministic time, is General Stochastic Petri Nets (GSPNs) as presented in Fig 4 (GreatSPN tool was used for its edition).

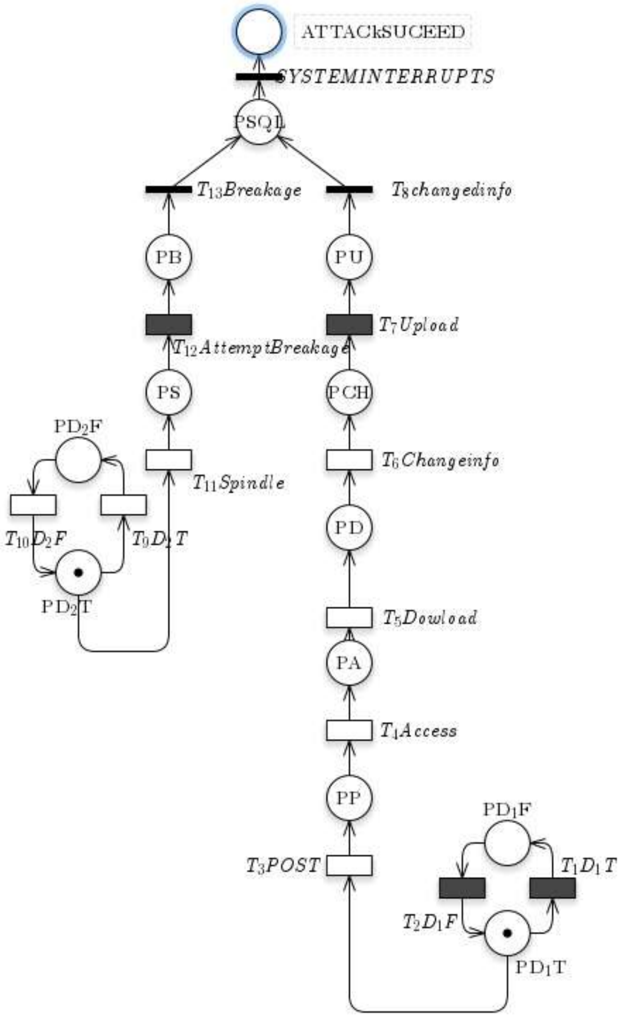


Fig. 8. GSPN modelling cyber-attack in 3D printer in I4.0

TABLE III. Transitions in SQL injection detection GSPN analysis

Transitions	*Description*	*Firing time*
T1	Intrusion Detection (NIDS/HIDS) Positive alarm	D
T2	Intrusion Detection (NIDES/HIDS) Negative alarm	S
T3	POST malicious form	S
T4	Access to user's account	S
T5	Download Original form and use's information	S
T6	Change the user's Information	S
T7	Upload information to the data server	D
T8	New information Submitted	I
T9	Intrusion Detection (Acoustic) Positive alarm	D
T10	Intrusion Detection (Acoustic) Negative alarm	D
T11	Spindle Speed Requested Production	S
T12	Attempt to Breakage of drilling bits	D
T13	Breakage of drilling bits	I
System Interrupts	System Interrupts	I

In Table III, all transitions for possible scenarios in Cyber-attack are provided. For T2, T3, T4, T5, T6 and T11. firing delay is stochastic and can be different for each attack. T7, T9, T10, and T11 firing delay are in an interval time that depends on the system. Cyber-attacks transition on Petri nets are combination of deterministic and random firing delay distribution. The objective of analysis the system is reducing an interval time to detect the attack and also, distinguishing between false and true attacks. In Table III, Immediate (I), Stochastic(s) and Deterministic(D) transitions are listed

V. Conclusion and Future works

In this study authors represented a new method for modelling one type of Cyber-attacks in I4.0 by using Attack trees assigned by Intrusion Detection Systems and then analysis behavior of the system (in this case 3D printer) by Generalized Stochastic Petri nets. This paper shows the application of GSPN as a promising tool for analysis and assessment security of Cyber Physical Systems. In the future work we plan to enhance the of IDS performance by training data using with learning algorithm and develop a methodology to automatic generating Attack Defense trees to Petri nets models. The idea of proposing the translation rules, opens an opportunity to automatically generate Petri Nets models from any different scenario using Attack Trees.

Acknowledgments

This work was partially financed by Portuguese Agency FCT – Fundação para a Ciência e a Tecnologia, in the framework of project UID/EEA/00066/2019.

References

[1] E. A. Lee and S. A. Seshia, *Intoruction to Embedded Systems A Cyber-Physical System approach*, Second. Massachusetts: MIT Press, 2017.

[2] E. A. Lee, “Cyber Physical Systems: Design Challenges,” in *11th IEEE Symposium on Object Oriented Real-Time Distributed Computing (ISORC) Cyber*, 2008, pp. 363–369.

[3] L. Da Xu, E. L. Xu, and L. Li, “Industry 4.0: state of the art and future trends,” *Int. J. Prod. Res.*, vol. 7543, pp. 1–22, 2018.

[4] R. Y. Zhong, X. Xu, E. Klotz, and S. T. Newman, “Intelligent Manufacturing in the Context of Industry 4.0: A Review,” *Engineering*, vol. 3, no. 5, pp. 616–630, 2017.

[5] N. Jazdi, “Cyber physical systems in the context of Industry 4.0,” *2014 IEEE Autom. Qual. Testing, Robot.*, pp. 2–4, 2014.

[6] “CISCO.” [Online]. Available: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html.

[7] M. Uma and G. Padmavathi, “A Survey on Various Cyber Attacks and Their Classification,” vol. 15, no. 5, pp. 390–396, 2013.

[8] H. Al-Mohannadi, Q. Mirza, A. Namanya, I. Awan, A. Cullen, and J. Disso, “Cyber-Attack Modeling Analysis Techniques : An Overview,” *2016 IEEE 4th Int. Conf. Futur. Internet Things Cloud Work.*, pp. 69–76, 2016.

[9] J. B. Hong, D. S. Kim, C. J. Chung, and D. Huang, “A survey on the usability and practical applications of Graphical Security Models,” *Comput. Sci. Rev.*, vol. 26, pp. 1–16, 2017.

[10] B. Schneier, “Attack Trees,” *Dr. Dobb’s J. Software Tools*, vol. 24, no. 12, p. 60, 1999.

[11] S. Mauw and M. Oostdijk, *LNCS 3935 - Foundations of Attack Trees*. Springer-Verlag Berlin Heidelberg, 2006.

[12] B. Kordy, S. Mauw, M. Melissen, and P. Schweitzer, “Attack-defense trees and two-player binary zero-sum extensive form games are equivalent,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6442 LNCS, pp. 245–256, 2010.

[13] A. Roy, D. S. Kim, and K. S. Trivedi, “Cyber security analysis using attack countermeasure trees,” *Proc. Sixth Annu. Work. Cyber Secur. Inf. Intell. Res. - CSIIRW ’10*, no. December 2013, p. 1, 2010.

[14] A. Bagnato, B. Kordy, P. H. Meland, and P. Schweitzer, “Attribute Decoration of Attack – Defense Trees,” *Int. J. Secur. Softw. Eng.*, vol. 3, no. 2, pp. 1–35, 2012.

[15] B. Kordy, P. Kordy, S. Mauw, and P. Schweitzer, “ADTool: Security Analysis with Attack- Defense Trees,” *Lect. Notes Comput. Sci.*, vol. 8054, no. 318003, pp. 173–176, 2013.

[16] Kenneth S. Edge, “A FRAMEWORK FOR ANALYZING AND MITIGATING THE VULNERABILITIES OF COMPLEX SYSTEMS VIA ATTACK AND PROTECTION TREES,” University Air, 2007.

[17] R. Kumar and M. Stoelinga, “Quantitative security and safety analysis with attack-fault trees,” in *Proceedings of IEEE International Symposium on High Assurance Systems Engineering*, 2017, pp. 25–32.

[18] J. B. Hong and D. S. Kim, “Towards scalable security analysis using multi-layered security models,” *J. Netw. Comput. Appl.*, vol. 75, pp. 156–168, 2016.

[19] N. Vidhyashree, F. Lance, T. Wandji, V. Nagaraju, L. Fiondella, and T. Wandji, “A survey of fault and attack tree modeling and analysis for cyber risk management,” *2017 IEEE Int. Symp. Technol. Homel. Secur. HST 2017*, 2017.

[20] K. S. Edge, G. C. Dalton, R. A. Raines, and R. F. Mills, “Using attack and protection trees to analyze threats and defenses to homeland security,” in *Proceedings - IEEE Military Communications Conference MILCOM*, 2007, pp. 1–7.

[21] D. M. Nicol, W. H. Sanders, and K. S. Trivedi, “Model-based evaluation: From dependability to security,” *IEEE Trans. Dependable Secur. Comput.*, vol. 1, no. 1, pp. 48–64, 2004.

[22] M. A. Marsan, G. Conte, and G. Balbo, “A Class of Generalized Stochastic Petri Nets for the Performance Evaluation of Multiprocessor Systems,” vol. 2, no. 2, pp. 93–122, 1984.

[23] T. M. Chen, J. C. Sanchez-Aarnoutse, and J. Buford, “Petri net modeling of cyber-physical attacks on smart grid,” *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 741–749, 2011.

[24] J. P. McDermott, “Attack net penetration testing,” *Proc. 2000 Work. New Secur. Paradig.*, pp. 15–21, 2001.

[25] J. Steffan and M. Schumacher, “Collaborative attack modeling,” *Proc. ACM Symp. Appl. Comput. (SAC ’02)*, p. 253, 2002.

[26] Louchka Popova-Zeugmann, *Time Petri Nets*. Springer-Verlag Berlin Heidelberg, 2013.

[27] M. A. Marsan and U. Milano, “Stochastic Petri nets: An elementary introduction,” in *European Workshop on Applications and Theory in Petri Net: European Workshop on Applications and Theory in Petri Net*, springer, 1988, pp. 1–29.

[28] F. S. Rietta and G. Way, “Application Layer Intrusion Detection for SQL Injection,” pp. 531–536.

[29] R. Nehemia, C. Lim, Z. Rustam, D. Zahras, M. Ahsan, and M. Mashuri, “A Survey on Anomaly Based Host Intrusion Detection System,” 2018.

[30] W. Lin, S. Ke, and C. Tsai, “Knowledge-Based Systems CANN : An intrusion detection system based on combining cluster centers and nearest neighbors,” *Knowledge-Based Syst.*, vol. 78, pp. 13–21, 2015.

[31] L. M. Almutairi and S. Shetty, “Generalized stochastic Petri Net model based security risk assessment of software defined networks,” in *MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)*, 2017, pp. 545–550.

[32] M. Wu *et al.*, “Establishment of intrusion detection testbed for CyberManufacturing systems,” in *Procedia Manufacturing 46th SME North American Manufacturing Research Conference, NAMRC 46*, 2018, vol. 26, pp. 1053–1064.

[33] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. De, “A survey of intrusion detection in Internet of Things,” *J. Netw. Comput. Appl.*, vol. 84, no. September 2016, pp. 25–37, 2017.