Cyber-Attack for BGP Systems Using Stochastic Game Nets Model

Abdelali EL BOUCHTI
Computer, Networks, Mobility and Modeling laboratory
FST, Hassan 1st University, Settat, Morocco
a.elbouchti@gmail.com

ABSTRACT: *With the rise of cyber-attack activities in the recent years, research in this area has gained immense emphasis. One of such research efforts is modeling of cyber-attacks. In this context, several modeling approaches have been developed, such as approaches based on attack trees (AT). In this paper, we propose a novel modeling, Stochastic Game Nets (SGN) and use it to model and analyze the attack action in Border Gateway Protocol (BGP) networks. Firstly, the definition and modeling algorithm of SGN are given. And then we apply the SGN method to describe the attack and defense course in BGP networks. Finally, we analyze the attack time and attack probability in the BGP quantificationally based on the method successfully. The method can also be applied to other areas with respect to a game.*

Keywords: Vulnerability, Cyber-Attack, SGN, Attack action, Attack Modeling, BGP

Received: 8 November 2016, Revised 12 December 2016, Accepted 4 January 2017

1. Introduction

A secure computer system provides guarantees regarding the confidentiality, integrity and availability of its objects (such as data, processes or services). However, systems generally contain design and implementation flaws that result in security ulnerabilities. An intrusion takes place when an attacker or group of attackers exploit security vulnerabilities and thus violate the confidentiality, integrity, or availability guarantees of a system or a network. Intrusion Detection Systems (IDSs) [15] detect some set of intrusions and execute some predetermined action when an intrusion is detected.

Some literatures show a comprehensive taxonomy of internet attack [4, 6]. Other common intrusion database such as [5] also creates a common namespace for all vulnerabilities and exploits. Taxonomy of attacks fails to formally express their dynamic properties. Some graph-based attack models also provide means for modeling intrusion [7]. Other research [6] uses the software fault tree approach to analyze the design and implementation of intrusion detection system. Schneier [2] was the first one to associate the term "*attack tree*" with the use of fault tree for attack modeling which made this approach more widely known.

This modeling tool has proved to be simple, easy to use and easy to analyze results, and yet powerful in its modeling capability. Besides modeling attacker behavior ATs are found to be useful for modeling system vulnerabilities and points of access.

However, the capabilities of ATs are limited, because of their limited construct set and static nature. Our effort uses Petri Net constructs to augment and extend existing principles that are already proven useful in ATs. Although some Petri Net and CoPNet based models have existed, they are only used to model the intrusion detection system itself [8].

Our choice of a CoPNet formalism to address the design of security policies is motivated by the following reasons: Petri Nets are well known for their graphical and analytical capabilities for the specification and verification of concurrent, asynchronous, distributed, parallel, and nondeterministic systems. Various features contributing to such a success include graphical nature, the simplicity of the model, and the firm mathematical foundation. It also provides modularity in design. Hence, a Petri-net-based policy is more flexible when it is embedded into a system.

The purpose of our proposed approach, called Colored Petri Net Attack Modeling approach (CoPNet) [22] is to provide intuitive modeling approach for modeling attacker behavior in vulnerable systems from security perspective, based on the concepts of ATs and modeling abilities of Petri Nets. Some cost elements are added to CoPNet based attack modeling to evaluate the risk of intrusion. We choose Border Gateway Protocol (BGP) [23] networks as a case study that illustrates the CoPNet approach.

The remainder of this paper is organized as follows. An overview of AG and AT is presented in Section 2. In Section 3, we present and define Petri Nets and CoPNet. In Section 4, we show how to build CoPNet attack model from AT. We show the extended CoPNet model in Section 5. CoPNet based attack model of BGP systems is described in Section 6. Finally, we conclude the paper and give an overview of future work in Section 7.

2. Stochastic Petri Nets and Stochastic Gamenets

2.1 Stochastic Petri Nets

Stochastic Petri Nets are Petri nets augmented with the set of average transition rates for the exponentially distributed transition firing times. A transition represents a class of possible changes of markings. Such a change, also called transition firing, consists of removing tokens from the input places of the transition and adding tokens to the output places of the transition according to the expressions labeled on the arcs. A transition may be associated with an enabling predicate which can be expressed in terms of the place marking expressions.

If the predicate of a transition evaluates to be false, the transition is disabled.

In SPN models, transitions can be categorized into two classes: transitions of Class One are used to represent logical relations or determine if some conditions are satisfied [13].This class of transitions is called immediate transition with zero firing time. Transitions of Class Two are used to represent the operations on the tasks or information processing. This class of transitions is called timed transition with exponential distributed firing time. A marking in a SPN model represents a distribution of tokens in the model. The state space of a model consists of the set of all markings reachable from the initial marking through the occurrence of transition firing. A SPN is homomorphism to a continuous time Markov Chain (MC), and there is a one-to-one relationship between markings of the SPN and states of the MC [13] and [14].

Definition 1. (Stochastic Petri Nets) Stochastic Petri Net is a quadruple $(P\ T, F, \lambda)$, where

- P is a finite set of places;
- T is a finite set of transitions $(P \cap T \neq 0)$;
- $F \subseteq (P \times T) \cup (T \times P)$ is a set of arcs;
- $\lambda = (\lambda_1, \lambda_2, ..., \lambda_n)$ is a set of firing rates of transitions in transition set.

As an extension of Stochastic Petri Nets (SPN), Stochastic Reward Net (SRN) is a powerful graphical and mathematical tool, which not only is able to model concurrent, asynchronous, stochastic and nondeterministic events, but also provide transition

enabling function and firing probability that can be used to model various algorithms and strategies. The SRN differ from the SPN in several key aspects. From a structural point of view, both formalisms are equivalent to Turing machines. But the SRN provide enabling functions, marking dependent arc cardinalities, a more general approach to the specification of prioritie, and the ability to decide in a marking-dependent fashion whether the firing time of a transition is exponentially distributed or null, often resulting in more compact nets. Perhaps more important, though, are the differences from a stochastic modeling point of view. The SRN formalism considers the measure specification as an integral part of the model. Underlying an SRN is an independent semi-Markov reward process with reward rates associated to the states and reward impulses associated to the transitions between states [15].

2.2 Stochastic Game Nets

The aim of this section is introduce the Stochastic Game Nets (SGN). The SGN structure will represent all possible strategies existing within the game.

Definition 2. (Stochastic Game Nets)

A Stochastic Net is the 9-tuple $SGN = (N, P, T, \pi, F, R, \lambda, U, M_0)$, where

- $N = 1, 2, ..., n$ denotes a finite set of players;
- P is a finite set of places;
- $T = T^1 \cup T^2 \cup ... \cup T^n$ is a finite set of transitions,where T^k is the set of transitions with respect to player $k \in N$;
- $\pi : T \rightarrow [0,1]$ is a routing policy representing probability of choosing a particular transition;
- $F \subseteq I \cup O$ is a set of arcs where $I \subseteq (P \times T)$ and $O \subseteq (T \times P)$, such that $P \cap T \neq 0$ and $P \cup T \neq 0$;
- $R : T \rightarrow (IR^{(1)}, IR^{(2)}, ..., IR^{(n)})$ is a reward function for the player taking each action;
- $\lambda = (\lambda_1, \lambda_2, ..., \lambda_k)$ is a set of firing rates of transitions in transition set, where k is the number of transitions;
- $U(p_i^k)$ is the utility function, when player k in the condition p_i. Accordingly, the player can choose the best transition;
- M_0 is the initial marking.

Firing Rule: The firing rule of a $SGN = (N, P, T, \pi, F, R, \lambda, U, M_0)$ is given as follows. A marking m represents a distribution of the tokens in SGN. Each token s is related with a reward vector $h(s) = (h_1(s), h_2(s), ..., h_n(s))$ as its properties. Each element of T represents a class of possible changes of markings. Such a change of t, also called transition firing, consists of removing tokens from a subset of places and adding them to other subsets according to the expressions labeling the arcs. A transition t is enabled under a marking M whenever, for all $p \in P$ and $(p, t) \in F$, $M(p) \neq \phi$ Each player gets the reward $R(t)$ through the transition, and the reward is recorded in the reward vector h of each token.

Now, we present some notations with respect to a 9-tuple Stochastic Game Net $SGN = (N, P, T, \pi, F, R, \lambda, U, M_0)$.

Definition 6. An action $t \in T$ with respect a $SGN = (N, P, T, \pi, F, R, \lambda, U, M_0)$ is a optimum decision, while it is optimum ccording to the utility function for player k.

Definition 7. A strategy with respect to a $SGN = (N, P, T, \pi, F, R, \lambda, U, M_0)$ is identified by δ and consists of the transition sequence represented in the SGN graph model.

Definition 8. An optimum strategy with respect to a $SGN = (N, P, T, \pi, F, R, \lambda, U, M_0)$ is identified by δ, and consists of the transition sequence represented in the SGN graph model where a Nash equilibrium is reached for all the players.

Theorem 1. If a $SGN = (N, P, T, \pi, F, R, \lambda, U, M_0)$ has a finite set of places and transitions, there always exits a Nash equilibrium.

Proof.

Theorem 2. A $SGN = (N, P, T, \pi, F, R, \lambda, U, M_0)$ is sufficient to describe a game problem.

Proof.

Theorem 1 presents the feasibility of the SGN tool.

Theorem 2 proposes the maturity of the SGN tool. Moreover, we could determine the scope of this approach in a given area, such as the problems with respect to network security.

Now, we present the two steps to solve the SGN to find the Nash equilibrium. The Nash equilibrium corresponds to the optimized strategy of each player. We first construct the reachability tree according to the SGN, and then find out the Nash equilibrium.

Algorithm- 1: Construct the Reachability Tree from SGN
A reachability is consist of nodes, which are denoted by all the reachable markings of the SGN, and the arcs among the nodes. From a SGN with a starting marking M_0, we can construct a reachability tree. The algorithm has three steps.

• Make M_0 the root r of the tree.

• *Node x* marked by *M* is a leaf if and only if there isn't a transition $t \in T$ which is enabling under *M*, or there is a node $y \neq x$ along the road from *r* to *x*, which has a similar mark *M'* as *M*. We define two marks M_1 and M_2 similar as follows: $M_1 = \phi$ if and only if $M_2 = \phi$ for all $p \in P$.

• If a node *x* marked by *M* is not a leaf, fire a transition *t*; $(p, t) \in F$ to construct a new node in the reachability tree marked as *M'*.

Following the above three steps, we can construct the reachability tree from the SGN. The algorithm is similar with that in Stochastic Petri Nets.

Algorithm-2: Find out the Nash Equilibrium
The algorithm is to find the Nash Equilibrium of an action sequence with for all the players.

For every leaf node x_i marked by M_i in the reachability tree and a token *s* such that there is a state *p*, $M_i(p) = s_i, 1 \leq i \leq n$ the reachability tree.

Generally, there are multiple paths from the initial state to a leaf node. Assume *xi* is a leaf node, and there are *wi* separate paths from the root to x_i. Let $t_1^{(i,w)}, t_2^{(i,w)}, ..., t_{k(i,w)}^{(i,w)}$ be the *w*th path from root node to leaf node x_i. We define a leaf probability for the leaf node x_i of the w^{th} path as

$$(f^{(w)}(x_i) = \pi(t_1^{(i,w)}) . \pi(t_2^{(i,w)}) . \ldots . \pi\, t_{k(i,w)}^{(i,w)} \tag{3}$$

Then the final utility vector for the system is

$$(U_1, U_2, ..., U_n) = \sum \left[\sum (f^{(a)}(x_i) * (h^{(a)}(s_i)) \right] \tag{4}$$

where *m* is the number of leaves in the reachability tree. Note that $h^{(a)}(S_i)$ of size n × 1 is the reward vector of the token in leaf node x_i on the a^{th} path, and *n* is the number of players as in the definition of SGN.

According to the state of Nash equilibrium, every player has achieved his best when others don't change their strategies. Thus, the problem is to find such π that $(U_1, U_2, ..., U_n)$ is Nash equilibrium for each player, which could be given as:

$$\max_{\pi} U = (U_1, U_2, ..., U_n) \tag{5}$$

Note that, the above equation is a multi-objective optimization, which can be solved using the mathematical programming methods.

Remark 1. The algorithm can be implement based on that of Stochastic Petri Nets, where the Nash equilibrium equation can be automatically achieved.

3. BGP Networks

In this section, we will apply the Stochastic Game Nets to model the attack and defense actions, and investigate the security properties based on the Nash equilibrium, and propose the optimum strategy for the computers at each stage to minimum the loss during computer attacks. We apply the SGN to three typical cases including the basic attack-defend case, the multi-round case and the multi- player attack case. Three cases demonstrates the three fundamental structures, basic attack-defend case shows the sequence structure, multiround case shows the structure of loop and, the multi-player attack case presents the modeling of the multiple tokes.

First, we conclude the steps to apply the Stochastic Game Nets doing the security analysis, as the following six steps.

Step 1: Determine the players in the game N;

Step 2: Present the targets of each player k, and construct each player's action set T^k ;

Step 3: Define the reward function R for each transition;

Step 4: Construct the SGN model;

Step 5: Find the Nash equilibrium with respect to the SGN model, and propose optimum strategy accordingly;

Step 6: Simplify the SGN model and, compute the stationary probability distribution and security and performance measures according to the transition firing rate λ.

In this section, we describe the attack selection process for a case study process control network for a power grid, and we use this case study to illustrate the usages of CoPNet based attack modeling approach. We have chosen Border Gateway Protocol (BGP) networks as our case study.

An example scenario for a BGP attack is shown in Figure 1. An attacker prevents two peers from exchanging routing information by repeatedly causing a BGP session in Established state to reset. The BGP session can be reset by injecting a spoofed TCP

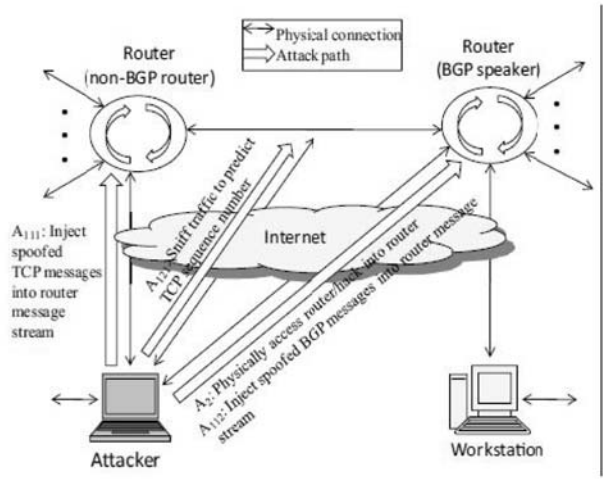

Figure 1. Example of attack for resetting a BGP session

(Transmission Control Protocol) or BGP message into the router message stream. Building a valid TCP/BGP packet requires a valid TCP sequence number (obtained by TCP sequence number prediction). During the initial stages of a TCP sequence number attack, a spoofed packet from an attacker is usually followed by the original packet from the authentic source.

Spoofed TCP message with RST flag set will cause a connection to reset. Spoofed BGP messages (OPEN, NOTIFICATION or KEEPALIVE messages) received by the BGP speaker in the Connect or Active states will cause the router to reset resulting in a denial of service. The BGP speaker can also be compromised by gaining physical or logical (hijacking a router management session) access to the router.

4. Conclusion and Future Work

In this paper, we have presented SGN based attack modeling approach to model the attacks. The objective of our modeling approach is to provide more precise quantitative parameterization and advanced modeling capabilities compared to ATs. After other features are added to this model, it can be used to model the intrusion detection and response. Another important feature of this model is that intrusion can be quantified, so the most effective controlling actions can be determined. But the practical experiment shows the SGN based attack model has a more complicated form than the graph-like model, especially AT. So it is necessary to condense the SGN based attack model. We have provided BGP systems as a case study that illustrates the SGN approach. Simulation approach of CoPNet based attack model is our future work.

References

[1] Jensen, K. (1992). Coloured Petri Nets: Basic Concepts, Analysis Methods and Practical Use. Springer-Verlag, Berlin, Germany/ Heidelberg, Germany/ London, UK/ ect., 1

[2] Schneier, B. (1999). Attack Trees, *Dr. Dobb's Journal of Software Tools*, 24 (12) 21-29.

[3] Cunningham, W. (2002). The WikiWikiWeb [DB/OL]. http:// c2.com/cgibin/wiki

[4] Ruiu, D. Cautionary tales: stealth coordinated attack how to [DB/OL]. http:// www.nswc.navy.mil/ISSEC/CID/Stealth_coordinated_Attack.html, July 1999.

[5] Bugtraq Vulnerability Database (2003). [DB/OL]. http://www.securityfocus.com

[6] Helmer, G., Wong, J., Slagell, M. A (2001). Software Fault Tree Approach to Requirements Analysis of an Intrusion Detection System, *In:* Proceeding of symposium on requirements engineering for information security. Center for education and research in information assurance and security, Perdue University, March 2001.

[7] Phillips, C., Swiler, L P. (1998). A Graph-based System for Network-Vulnerability Analysis, *In*: Proceeding of new security paradigms workshop, Charlottesville, VA, USA, 71-79.

[8] Helmer, G., Wong, J., Slagell, M. (2007). Software Fault Tree and Colored Petri Net based specification and implementation of agent- based intrusion detection systems, *Int. J. Information and Computer Security*, 1 (1/2).

[9] Jensen, K. (1998). A brief introduction to Colored Petri Nets, Workshop on the Applicability of Formal Models, 2 June Aarhus, Denmark, p. 55-58.

[10] Jensen. K. (1998). An introduction to the Theoretical Aspects of Colored Petri Nets, Workshop on the Applicability of Formal Models, Aarhus, Denmark.

[11] The center for SCADA security, The Center for SCADA Security, Sandia National laboratory. [online]. Available http://www.sandia.gov/scada/home.htm.

[12] Supervisory Control and Data Acquisition (SCADA) Systems, Technical Information Bulletin 04-1, National Communication System, October 2004. [online]. Available: http://www.ncs.gov/library/tech_bulletins/2004/tib_04- 1.pdf

[13] Understanding SCADA system security vulnerabilities, Symantec White Paper, 2005.

[14] Brown, T. (2005). Security in SCADA systems: How to handle the growing menace to process automation, *IEEE Comp. and Control Eng*., 16 (3), June/July. 42-47.

[15] Rehman, R. (2003). Intrusion Detection Systems with Snort. Prentice-Hall.

[16] Lippmann, R. Ingols, K. (2005). An annotated review of past papers on attack graphs. Technical report, MIT Lincoln Laboratory, March.

[17] Mauw, S., Oostdijk, M. (2005). Foundations of attack trees, *In:* Proceedingd 8th Annu. Int. Conf. Inf. Security Cryptol. (ICISC), Seoul, Korea, December, 186–198.

[18] Khand, P. (2009). System level security modeling using attack trees, *In*: Proceedings 2nd Int. Conf. Comput., Control, Commun. (ICA), Karachi, Pakistan, Feb. 1–6.

[19] Schneider, K., Liu, C. -C., Paul, J.-P. (2006). Assessment of interactions between power and telecommunications infrastructures, *IEEE Trans. Power Sys.*, 21, 1123–1130, Aug.

[20] Ten, C.-W., Liu, C.-C., Govindarasu, M. (2007). Vulnerability assessment of cybersecurity for scada systems using attack trees, *In: IEEE Power Eng. Soc. Gen. Meet., Tampa*, FL, June. 1–6.

[21] McLaughlin, S., Podkuiko, D., McDaniel, P. (2009). Energy theft in the advanced metering infrastructure, *In:* Proceedings 4th Int.Workshop Crit. Inf. Infrastruct. Security (CRITIS 2009), Bonn, Germany, September. *p* 176–187.

[22] El Bouchti, Abdelali., Haqiq, Abdelkrim (2012). Performance Modeling of Attack Countermeasure Using Colored Petri Nets, International Symposium on Security and Safety of Complex Systems, Agadir, Morocco, May 25 - 26, 2012.

[23] Convery, S., Cook, D., Franz, M. (2002). An Attack Tree for the Border Gateway Protocol, Cisco Internet draft.