Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 15 (2011) 3433 – 3438

Procedia Engineering

www.elsevier.com/locate/procedia

Advanced in Control Engineering and Information Science

Intrusion Intention Identification Methods Based on Dynamic Bayesian Networks

Qingtao Wu*, Ruijuan Zheng, Guanfeng Li, Juwei Zhang

Electronic & Information Engineering College, Henan University of Science & Technology, Luoyang 471003, China

Abstract

It is difficult to detect the intention of an intruder, identify semantics of attacks and predict further attacks effectively using intrusion detection methods in the construction of high-level attack scene and disposal of sophisticated attack. An intrusion intention identification method based on dynamic Bayesian network is proposed for indeterminate problems that occur during sophisticated network attacks. This method applies dynamic Bayesian directed acyclic graphs to give real-time formulation of incidence among attack behaviors, intentions and attacks. It also applies probabilistic reasoning method to predict further attacks by an intruder. The result reflects varying histories of the intention of an intruder and demonstrates the effectiveness of the method.

Keywords: dynamic Bayesian network; intrusion intention; directed acyclic graph; probabilistic reasoning

1. Introduction

Various intrusion detection systems (IDS) can provide in-depth defense for networks. However, for the flexibility, accuracy and efficiency of current IDS technology detection, there are still some problems, such as massive repeating alarms, serious false positives and false negatives, flooding alarms, and other issues. One main cause behind such problems is the failure of IDS to effectively use the logical relationship between attack events. This is crucial because the effective identification of such a relationship and associated relative steps consisting of a composite attack helps in identifying intrusion intention, obtaining more information, and identifying the real intention of the intrusion.

A previous study [1] has utilized the method called Colored and Time-Based Petri Net (CTPN) to predict sophisticated attacks. It improves and expands the traditional attack detection methods from the perspective of attack intention and has good real-time performance. However, the method needs to analyze more attack examples to further complete the categories based on the given information. Another study [2] has utilized the alarm message based on intrusion intention. It modifies the alarm message linking method based on intrusion strategies and increases the generalization of the intrusion strategy model.

* Corresponding author. Tel.: +86-379-64231963; fax: +86-379-64231910.
E-mail address: wqt8921@126.com

1877-7058 © 2011 Published by Elsevier Ltd.
doi:10.1016/j.proeng.2011.08.643

However, based on the bottom-up alarm information and intrusion strategy model, the precision and efficiency depends on the reliability and precision and relative intrusion strategy model.

The Dynamic Bayesian network (DBN), based on probabilistic network, combines static Bayesian network and timestamp to form a new probabilistic model with disposal of sequence data. The introduction of time factors allows data to form from conditions in different hours and reflect the developmental and varying history of the variables they represent.

This paper proposes an intrusion intention identification method based on dynamic Bayesian network to address indeterminate problems during sophisticated network attacks. The method utilizes the dynamic Bayesian network model to identify intrusion intention and link all steps during the intrusion.

2. DBN-based intrusion intention identification methods

2.1. Definitions

Definition 1 (Attack behavior [3]) Attack actions observed by the attacker. Assuming that X_i and X_j are two attack behaviors at time i and time j, where $i<j$, there is causality between X_i and X_j if and only if X_i is prerequisite for X_j.

Definition 2 (Attack plan) is a series of attack behaviors performed by the attacker to realize some intention. This can be expressed as an attack behavior aggregation $\pi=< X_1, X_2, \ldots, X_k>$, $k>0$, and π is considered an effective attack plan if the sequence corresponding to π satisfies its corresponding causality.

Definition 3 (Intrusion intention [4]) is an attack goal or attack intention realized by network attack through effective attack plans.

2.2. DBN model derivation based on intrusion intention

Considering the sequence of intrusion intention identification process, this study utilizes the DBN directed acyclic graph to describe intrusion intention. Assuming that the random variable aggregation $X=\{X_1, X_2, \ldots, X_n\}$ represents a series of sophisticated attacks conducted by the intruder to realize some attack goal, X_i is the corresponding attack node in the aggregation, and $Pa(X_i)$ is the father node aggregation of node X_i ;X_i at time t is expressed as $X_i[t]$, and each attack node X_i, given its father node, is independent of its non-descendant node. Random variable aggregation X is joint probability distribution. These include the following:

(a) the assumption that the varying process of aggregation within a limited period is stable for all t ;

(b) the assumption that the dynamic probability process is Markovian[5], which satisfies formula (1).

$$P(X[t+1] \mid X[1], X[2], \ldots, X[t]) = P(X[t+1] \mid X[t]) \quad (1)$$

(c) the assumption that the conditional probability process between neighboring time points is stable, that is, $P(X[t+1]|X[t])$ has nothing to do with time point t , then $P(X[t+1]|X[t])$ represents conditional branching probability in different time point.

Based on the above assumptions, DBN of joint probability distribution based on random time points is composed of two parts: prior network B_0, $X[1]$ joint probability distribution defined in primary attack condition; and transfer network $B_{\rightarrow}$, transfer probability $P(X[t+1]|X[t])$(holds for all t) defined in node variables $X[1]$ and $X[2]$; within the time period (1, 2, …, t), DBN composed of (B_0, $B_{\rightarrow}$) describes intrusion intention. At time point 1, the father node of $X[1]$ is the node in prior network B_0, and the father nodes at time point t+1, X[t+1]are those in transfer network $B_{\rightarrow}$ with time dynamic characteristics (Fig. 1). The joint probability distribution of the DBN models describing intrusion intention can be expressed as:

$$P(X[1], X[2], \ldots, X[t]) = P_{B_0}(X[1]) \prod_{t=1}^{T} P_{B_{\rightarrow}}(X[t+1] \mid X[t]) \quad (2)$$