4. Pevny T. Merging Markov and DCT features for multiclass JPEG steganalysis/ T. Pevny, J. Fridrich// in Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX, pp. 301– 304, 2007.

5. Bestagini P. Local tampering detection in video sequences/ P. Bestagini, S. Milani, M. Tagliasacchi, S. Tubaro// IEEE 15th International Workshop on Multimedia Signal Processing (MMSP), Pula, Italy, 2013

6. Qadir G. Surrey University Library for Forensic Analysis (SULFA) of video content/ G. Qadir, S. Yahahya, A.T.S. Ho// IET Conference on Image Processing (IPR 2012), July 2012.

7. REWIND Forged Videos Data Set [Электронный ресурс]. – URL: https://sites.google.com/site/rewindpolimi/downloads/datasets/video-copy-move-forgeries-dataset (дата обращения: 14.05.2019).

8. GRIP Forged Videos Data Set [Электронный ресурс]. – URL: http://www.grip.unina.it/download/prog/ForgedVideosDataset/Copymove (дата обращения: 14.05.2019).

Ю.М. Злобин, В.П. Пряхин

ОЦЕНКА ЭФФЕКТИВНОСТИ МАСКИРОВАНИЯ ФУНКЦИОНАЛЬНО-ЛОГИЧЕСКОЙ СТРУКТУРЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ

(Самарский университет)

Провести оценку эффективности функционирования ранее разработанного средства масштабирования («маскирования») распределенной информационной системы (ИС) представляется возможным путем сравнения вероятностно-временных характеристик (ВВХ) полученной функционально-логической структуры с исходными характеристиками ИС [1]. Очевидно, что исходная ИС обладает рядом параметров, которые подвергнутся изменениям во время работы средства «маскирования» и, более того, появятся новые параметры, коренным образом влияющие на ВВХ ИС. С точки зрения дезинформации злоумышленника важно, чтобы разница между исходной и масштабируемой ИС была минимальна, то есть она должна стремиться к 0. Оценка этой разницы позволит говорить об эффективности «маскирования» ИС.

Предполагается, что сравнение ВВХ ИС возможно с помощью расстояния Кульбака-Лейблера. Для оценки информационного выигрыша (демонстрации его минимума) на $t \to \infty$ необходимо оперировать абсолютно непрерывными распределениями P и Q и иметь в распоряжении плотности этих распределений p(x) и q(x) соответственно. На данном этапе исследования получение плотности распределения случайных величин для маскированной структуры q(x) остается актуальной задачей. Другой вариант оценки расстояния Кульбака-Лейблера – аппроксимация для дискретных значений случайных величин.

Дискретные значения случайных величин для построения распределений P и Q могут быть получены путем синтеза марковских моделей функционирования ИС и их последующим решением.

Для моделирования функционирования ИКС, как правило, используются эргодические непрерывные марковские цепи. В этом случае состояния цепи соответствуют состояниям системы, различающихся составом исправного и отказавшего оборудования. Переходы между состояниями связаны с отказами и восстановлением устройств и реконфигурацией связей между ними, выполняемой для сохранения работоспособности системы [2]. Оценки характеристик эргодической цепи дают представление о надежности поведения системы в целом.

Основной характеристикой непрерывной марковской цепи является стационарное (финальное) распределение вероятностей состояний $p(t) = (p_1(t) \dots p_n(t))$, где $p_1(t) \dots p_n(t)$ - вероятности пребывания в состояниях $S_1 \dots S_n$ соответственно [3]. Вероятности $p_1(t) \dots p_n(t)$ и есть искомые ВВХ ИС, необходимые для оценки эффективности средства «маскирования».

Для построения распределения Q опишем состояния ИС, не использующей средство «маскирования» и проводящей противодействие сетевой разведке (СР) собственными ресурсами:

S_1 – ИКС работоспособна, функционирует в обычном режиме обнаружения СР;

S_2 – выработка стратегии противодействия СР;

S_3 – противодействие СР;

S_4 – отключение связи вследствие воздействия СР;

S_5 – отключения связи вследствие воздействия единой сети электросвязи (ЕСЭ).

Перечисленные дискретные состояния позволяют построить граф состояний исследуемой ИС, где λ_{ij} – интенсивности информационного обмена, характеризующие потоки событий (рис. 1):

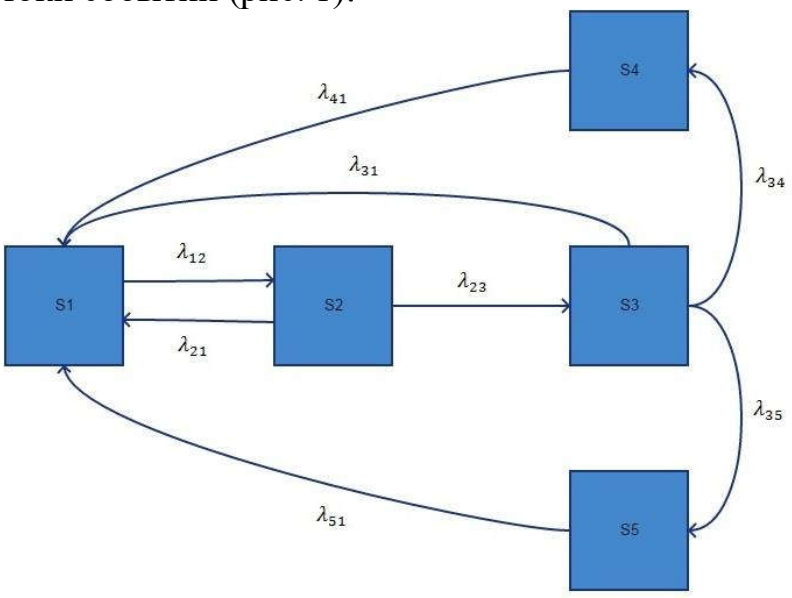

Рис. 1. Граф состояний ИС

Синтезируем систему дифференциальных уравнений (СДУ) Колмогорова-Чепмена [4]:

$$D(t,p)=\begin{cases}\dfrac{dp_1(t)}{dt}=\lambda_{51}p_5(t)+\lambda_{21}p_2(t)+\lambda_{31}p_3(t)+\lambda_{41}p_4(t)-\lambda_{12}p_1(t)\\ \dfrac{dp_2(t)}{dt}=\lambda_{12}p_1(t)-(\lambda_{21}+\lambda_{23})p_2(t)\\ \dfrac{dp_3(t)}{dt}=\lambda_{23}p_2(t)-(\lambda_{31}+\lambda_{34}+\lambda_{35})p_3(t)\\ \dfrac{dp_4(t)}{dt}=\lambda_{34}p_3(t)-\lambda_{41}p_4(t)\\ \dfrac{dp_5(t)}{dt}=\lambda_{35}p_3(t)-\lambda_{51}p_5(t)\end{cases} \quad (1)$$

Для построения распределения P опишем состояния ИС, использующей средство «маскирования» для противодействия СР:
S_1 – оценка значения корреляции между структурами СС;
S_2 – формирование ложной ФЛС ИКС и ее реализация;
S_3 – масштабирование структуры по требованию СУ;
S_4 – отключение связи вследствие воздействия СР;
S_5 – отключения связи вследствие воздействия ЕСЭ.

Перечисленные дискретные состояния позволяют построить граф состояний исследуемой и «маскируемой» ИС, где λ_{ij} – интенсивности информационного обмена, характеризующие потоки событий (рис. 2).

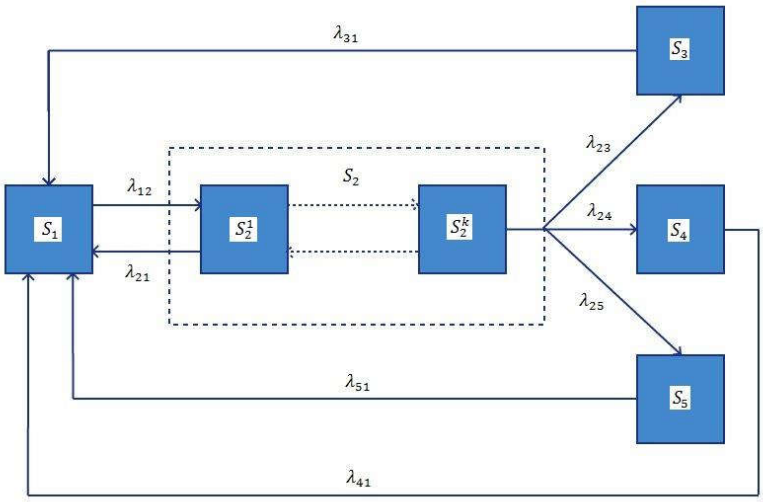

Рис. 2. Граф состояний системы принятия решения на управление (СПРУ)

Синтезируем математическую модель процесса перехода состояний СПРУ в виде СДУ Колмогорова-Чемпена и приведем ее к векторному представлению:

$$D(t,p)=\begin{cases}\frac{dp_1(t)}{dt}=\lambda_{21}p_2(t)+\lambda_{31}p_3(t)+\lambda_{41}p_{43}(t)+\lambda_{51}p_5(t)-\lambda_{12}p_1(t)\\ \frac{dp_2(t)}{dt}=\lambda_{12}p_1(t)-(\lambda_{21}+\lambda_{23}+\lambda_{24}+\lambda_{25})p_2(t)\\ \frac{dp_3(t)}{dt}=\lambda_{23}p_2(t)-\lambda_{31}p_3(t)\\ \frac{dp_4(t)}{dt}=\lambda_{24}p_2(t)-\lambda_{41}p_4(t)\\ \frac{dp_5(t)}{dt}=\lambda_{25}p_2(t)-\lambda_{51}p_5(t)\end{cases} \quad (2)$$

Для решения систем 1 и 2 и получения ВВХ ИС задаются начальные условия, $p_i(0)=(1,0,0,0,0)$, интервал интегрирования t_0=0, t_1=*10,* число этапов интегрирования n=10000. Применяя порядок решения СДУ методом Рунге-Кутты четвертого-пятого порядка, производится расчет для заданных значений интенсивностей событий λ_{ij}= *const* (марковский однородный процесс) [5].

Путем подстановки теоретических значений λ_{ij} были получены следующие значения предельных вероятностей для распределения Q и P соответственно:

$$q_1=0{,}299, q_2=0{,}206, q_3=0{,}124, q_4=0{,}165, q_5=0{,}206$$
$$p_1=0{,}269, p_2=0{,}141, p_3=0{,}169, p_4=0{,}188, p_5=0{,}234$$

Применяя формулу для оценки расстояния Кульбака-Лейблера между дискретными распределениями случайных величин [6]

$$D_{KL}(P||Q)=\sum_{i=1}^{n}p_i\log\frac{p_i}{q_i}$$

получим:

$$D_{KL}(P||Q)=0.0359$$

Полученный результат измеряется в битах, то есть, очевидно, что он является хорошим – различающая информация величиной менее одного бита не дает возможности предположить о преднамеренном вмешательстве в работу ИС и подталкивает злоумышленника к предположениям о влиянии случайных помех, например, от ЕСЭ.

Таким образом, расчет расстояния Кульбака-Лейблера позволяет говорить об эффективности использования средства «маскирования» ИС, так как информационный выигрыш минимален и при удачном выборе стратегии будет стремиться к 0.

Литература

1. Давыдов А.Е., Максимов Р.В., Савицкий О.К. Защита и безопасность ведомственных интегрированных инфокоммуникационных систем / А.Е.Давыдов, Р.В. Максимов, О.К. Савицкий. - Москва: ОАО «Воентелеком», 2015. - 520 с.

2. Марковские модели [Электронный ресурс] – Режим доступа: https://life-prog.ru/view_modelirovanie.php?id=19, свободный. Загл. с экрана. - Яз. русский. (дата обращения: 17.04.2019)

3. Вентцель Е.С. Теория вероятностей: Учеб. для вузов. [Текст]/Е.С. Вентцель - М.: Высш. шк., 1999. - 537 с.

4. Вентцель Е.С. Исследование операций. [Текст]/ Е.С. Вентцель –М.: Советское радио, 1972 - 210 с.

5. Бахвалов Н.С., Жидков Н.П., Кобельков Г.М. Численные методы. [Текст]/Н.С. Бахвалов, Н.П. Жидков, Г.М. Кобельков - М.: Наука, 1987. – 636 с.

6. S. Kullback, R.A. Leibler. On Information and Sufficiency [Текст]/ S. Kullback, R.A. Leibler - Ann. Math. Statist №1, 1951 - p. 79-86.

А.Н. Ивкин, М.Е. Бурлаков

РЕАЛИЗАЦИЯ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ С ВНЕДРЕННЫМИ ПРАВИЛАМИ МАШИННОГО ОБУЧЕНИЯ

(Самарский университет)

Аннотация

Система обнаружения вторжений является одним из важнейших устройств для защиты вычислительных систем, она способна выявлять и исследовать пакеты сетевого трафика. СОВ Snort - это бесплатное программное обеспечение с открытым исходным кодом, используемое в качестве средства защиты сети. Инструмент Snort обнаруживает только подтвержденные атаки, используя заранее определенные сигнатуры. В целях обнаружения новых, ранее не известных сетевых атак в данной работе разработаны расширенные правила для Snort, полученные с помощью инструмента машинного обучения WEKA и алгоритма j48. В статье, для экспериментального исследования, используется набор данных KDDCUP99. Основная цель данного исследования – реализация СОВ с внедренными правилами инструмента машинного обучения. Основными этапами исследований являются подготовка данных, применение алгоритма машинного обучения, извлечение экспертных правил, реализация правил Snort, обнаружение атак. Предлагаемая система обеспечивает эффективные показатели обнаружения и успешно выявляет новые, не представленные в сигнатурах атаки.

Введение

Система обнаружения вторжений (СОВ), специализированное программно-аппаратное средство, предназначенное для выявления несанкционированного доступа к ресурсам системы. Snort это СОВ с открытым исходным кодом [1]. Как правило snort разворачивают на маршрутизаторе как сетевую СОВ. Snort обнаруживает атаки на основе правил, написанных в заданном формате и синтаксисе. Snort - это многовариантный инструмент исследования пакетов, работающий в нескольких режимах.