УДК 004.891.3

ДЕТЕКТИРОВАНИЕ ПОВЕДЕНИЯ ОБЪЕКТОВ НА ОСНОВЕ ПОСЛЕДОВАТЕЛЬНЫХ ПАТТЕРНОВ

Молдавская А.В, Холовчук А.О.
к.т.н., доцент каф. СПО Рувинская В.М.
Одесский Национальный Политехнический Университет, УКРАИНА

АННОТАЦИЯ. В работе апробирована применимость последовательных паттернов для задачи детектирования поведения объектов. Проведены эксперименты на поведении вредоносных программ.

Введение. Во многих областях требуется анализ поведения объектов, изучаются типовые для предметной области последовательности взаимосвязанных действий. Ранее предложено [1] использовать одноуровневые и многоуровневые последовательные паттерны для добычи знаний о последовательностях действий, совершаемых изучаемыми классами объектов. В данной работе экспериментально опробован способ детектировать принадлежность объекта к заданному классу. В качестве предметной области выбрано поведение вредоносных программ.

Цель работы. Целью работы является уменьшение показателя среднего процента ошибок при детектировании образцов вредоносных программ, не включенных в обучающую выборку.

Основная часть работы. Будем сравнивать полученные результаты с работой [2], так как в ней, аналогично нашей работе, программы не просто детектируются как вредоносные по их поведению, но и распределяются по известным классам. Средняя ошибка в [2] составила 24%.

Эксперимент состоял из двух этапов: обучения и детектирования. В качестве исходных данных были использованы данные о поведении вредоносных программ, собранные в [3]. Исходные данные были разбиты на пять непересекающихся классов, соответствующих пяти классам изучаемых программ: Backdoor, Trojan, P2P-Worm, Worm, Virus. Для каждого класса C_k (k=1, 2, … , 5) были выделены непересекающиеся выборки: обучающая и тестовая. Объёмы выборок для каждого класса приведены в табл.1.

Табл.1 Количество образцов в выборках для каждого класса

Выб./Класс	Backdoor	Trojan	P2PWorm	Worm	Virus
Обучающая	412	211	154	124	114
Тестовая	179	80	56	49	33

После разделения обучающая выборка каждого класса была обработана алгоритмом секвенциального анализа. Применялся алгоритм нахождения максимальных паттернов VMSP [4] со следующими настройками: минимальная поддержка 70%, минимальная длина паттерна – 3 элемента. В результате для каждого класса были выделены одноуровневые паттерны.

В качестве способа детектирования была выбрана классификация тестовых образцов по пяти классам вредоносных программ («Backdoor», «Trojan», «Worm», «P2P-Worm», «Virus»). В качестве инструмента классификации был выбран наивный байесовский классификатор, основанный на формуле Байеса, представленной на формуле 1 [5][6]:

$$P(C \mid X) = \frac{P(C)P(X \mid C)}{P(X)} \qquad (1)$$

где $X=(x_1, \ldots, x_n)$ – набор длины n признаков классифицируемого объекта X.

Формула 2 показывает функцию правдоподобия применимо к задаче классификации по паттернам. Для каждого класса C_k:

$$P(C_k \mid p_1, p_2, \ldots, p_n) = \frac{P(C_k)\prod_{i=1}^{n} P(p_i \mid C_k)}{P(p_1)P(p_2)\ldots P(p_n)} \qquad (2)$$

где $p_1, p_2, \ldots p_n$ – паттерны, принадлежащие классифицируемой последовательности длины n,

$P(p_i|C_k)$ – величина поддержки паттерна p_i в классе C_k.

Нахождение априорной вероятности $P(C_k)$ производится по формуле 3:

$$P(C_k) = \frac{V^{C_k}}{V} \qquad (3)$$

где V^{C_k} – объём обучающей выборки для проверяемого класса C_k,

V – объём всей обучающей выборки.

Для решаемой задачи характерна следующая ситуация: один или несколько паттернов, принадлежащих тестируемой вредоносной программе, имеют поддержку $P(p_i|C_k)=0$ во всех классах, кроме того, в котором были обнаружены. Чтобы избежать нулевых значений функции правдоподобия, рекомендуется [6] применять аддитивное сглаживание, показанное в формуле 4:

$$P`(p_i \mid C_k) = \frac{P(p_i \mid C_k)+1}{V^{C_k}+V^{p}} \qquad (4)$$

Тогда функция правдоподобия для нашей задачи будет иметь вид, приведенный в формуле 5:

$$P(C_k \mid p_1, p_2, ..., p_n) = \frac{P(C_k)\prod_{i=1}^{n} P`(p_i \mid C_k)}{P(p_1)P(p_2)...P(p_n)} \qquad (5)$$

Для классификации по 5 классам были заданы следующие величины параметров: V=1068, V^{p}=451, V^{C_1}=412, V^{C_2}= 211, V^{C_3}= 154, V^{C_4}= 124, V^{C_5}= 114. Количественные результаты эксперимента для пяти классов представлены в табл.2. Процент ошибок по классам составил: Backdoor – 13%, Trojan – 25%, P2P-Worm – 11%, Worm – 22,4%, Virus – 42%.

Табл.2 Количество образцов в выборках для каждого класса

Тест/Класс	Backdoor	Trojan	P2PWorm	Worm	Virus
Test-Backdoor	156	5	0	18	0
Test-Trojan	2	60	4	14	0
Test-P2PWorm	0	4	50	2	0
Test-Worm	0	10	1	38	0
Test-Virus	0	7	2	5	19

Выводы. Получена оценка эффективности применения последовательных паттернов в задаче детектирования вредоносных программ по их поведению. Средняя ошибка составила 22%, что на 2% меньше, чем в [2].

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Moldavskaya A. V. Method of Learning Malware Behavior Scripts by Sequential Pattern Mining / A. V. Moldavskaya, V. M. Ruvinskaya, E. L. Berkovich //Symposium on Conformal and Probabilistic Prediction with Applications. – Springer International Publishing, 2016. – С. 196-207.

2. Zamboni D. Detection of Intrusions and Malware, and Vulnerability Assessment. / D. Zamboni. // Proceedings of 5th International Conference, DIMVA. – Springer International Publishing, 2008. - С. 10-11.

3. Ghiasi M. Dynamic VSA: a framework for malware detection based on register contents. / M. Ghiasi, A.Sami, Z. Saleri. // Engineering Applications of Artificial Intelligence, vol. 44. – Elsevier, 2015 - С. 111–122.

4. Fournier-Viger P. et al. VMSP: Efficient vertical mining of maximal sequential patterns. / P. Fournier-Viger, C.-W. Wu, A.Gomariz, V.S.Tseng //Canadian Conference on Artificial Intelligence. – Springer International Publishing, 2014. – С. 83-94.

5. Флах П. Машинное обучение. Наука и искусство построения алгоритмов, которые извлекают знания из данных. – Litres, 2017. – 402 с.

6. Yuan Q., Cong G., Thalmann N. M. Enhancing naive bayes with various smoothing methods for short text classification //Proceedings of the 21st International Conference on World Wide Web. – ACM, 2012. – С. 645-646.