УДК 004.021

Р.В. Мещеряков, И.А. Ходашинский, Е.Н. Гусакова

ОЦЕНКА ИНФОРМАТИВНОГО ПРИЗНАКОВОГО ПРОСТРАНСТВА ДЛЯ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Целью работы является рассмотрение и оценка методов формирования информативного признакового пространства, применяемых при построении систем обнаружения вторжений. Предлагается использовать для выявления информативных признаков генетический алгоритм и алгоритм муравьиной колонии. В качестве набора данных для экспериментов выбран KDD '99. В качестве классификатора использован алгоритм k ближайших соседей. С помощью жадного алгоритма экспериментально определяется оптимальное число информативных признаков, а сами признаки выбираются генетическим алгоритмом и алгоритмом муравьиной колонии. Параметры алгоритма классификации выбираются на основе проведенных экспериментов. Параметры генетического алгоритма (метод скрещивания, метод селекции, способ вычисления фитнес-функции) менялись в ходе эксперимента. Было установлено, что параметры генетического алгоритма не влияют на его результативность, влияют лишь на время выполнения. Эксперименты с алгоритмом муравьиной колонии показали, что с помощью этого алгоритма можно выявить группы информативных признаков (те признаки, которые именно в группе серьезно влияют на ошибку классификации). Эксперименты с жадным алгоритмом показали достаточность 11 признаков для классификации объектов из указанного набора с ошибкой классификации, не превышающей 5 %. Это подтверждается результатами сравнения с работами других исследователей.

Информативный признак; оценка информативности; атака; система обнаружения вторжений; генетический алгоритм; жадный алгоритм; алгоритм муравьиной колонии.

R.V. Meshcheriakov, I.A. Hodashinsky, E.N. Gusakova

EVALUATION OF FEATURE SPACE FOR INTRUSION DETECTION SYSTEM

With the rapid growth of computer networks during the past decade, security has become a crucial issue for computer systems. The detection of attacks against computer networks is becoming a harder problem to solve in the field of network security. Intrusion detection is an essential mechanism to protect computer systems from many attacks. As the transmission of data over the Internet increases the need to protect connected system also increases. Therefore, unwanted intrusions take place when the actual software systems are running.

In this paper we consider different methods of relevant feature set creation, which applicable to intrusion detection system development. We suggest using genetic algorithm and ant colony algorithm for feature selection. We used the KDD '99 intrusion detection dataset for experiments. K-nearest neighbor algorithm (kNN) was used for classifying objects. Optimal amount of relevant features is determined with greedy algorithm. Relevant features are selected with genetic algorithm and ant colony algorithm. Classification algorithm parameters are chosen based on experimental results. Genetic algorithm parameters (crossing method, selection method, fitness-function) were manipulated during the experiment. It was found that genetic algorithm parameters do not make influence on its results, but do make influence on the working time. Ant colony algorithm experiments have shown that this algorithm can find groups of relevant features (i.e. those features, that make big influence on classification rate when grouped with other features). Empirical results show that eleven features is enough for classification with error less than 5%. Results of comparison with other researches confirm this.

Relevant feature; relevance evaluation; intrusion; intrusion detection system; greedy algorithm; genetic algorithm; ant colony algorithm.

Введение. Под вторжением понимаются действия, направленные на нарушение целостности, конфиденциальности и доступности информационного ресурса. Одним из подходов к построению систем обнаружения вторжений является анализ

данных аудита и построение моделей вторжений. Суть подхода заключается в анализе большого объема ретроспективных данных с использованием алгоритмов интеллектуального анализа и создание на их основе моделей в форме классификаторов, отличающих нормальное поведение от вторжения. Системой обнаружения вторжений (СОВ) называются программные или программно-аппаратные средства выявления фактов несанкционированного доступа в компьютерную систему или сеть [1]. Важной задачей при разработке СОВ является задача поиск информативных признаков.

Алгоритмы выделения информативных признаков. Решение задачи формирования информативного признакового пространства в данной работе проводится с помощью трех алгоритмов: жадного, генетического и алгоритма муравьиной колонии.

Работа *жадного алгоритма* заключается в принятии локально оптимальных решений на каждом этапе, предполагая, что конечное решение также окажется оптимальным [2]. Жадный алгоритм применялся в двух модификациях:

- из набора признаков убирался один, и вычислялась ошибка классификации; на следующей итерации выбрасывался тот признак, ошибка при исключении которого была минимальна;
- на каждом шаге добавляется признак, в результирующий набор попадает тот признак, при добавлении которого ошибка классификации становится меньше всех.

При этом признаки исключались из набора или добавлялись в набор по одному. Предполагается, что в данных условиях для конкретного набора данных может быть выявлено оптимальное количество признаков для классификации.

Генетический алгоритм [3]. При использовании генетического алгоритма каждая хромосома представляет собой набор признаков, где каждый ген характеризует признак: 0 – отсутствует, 1 – присутствует. Выбор признаков проводился при различных фитнес-функциях. Первый способ формирования фитнес-функции основан на алгоритме классификации k ближайших соседей. Фитнес-функция формируется в предположении, что после отбрасывания неинформативного признака набор ближайших соседей изменяется минимально. Другой способ задания фитнес-функции – вычисление ее как точности классификации.

Алгоритм муравьиной колонии представляет собой итеративный метод случайного поиска, основанный на моделировании поведения агентов (муравьев) в процессе решения ими оптимизационных задач [4]. В случае решения задачи выбора информативных признаков набор признаков представлен в виде графа, в котором каждый узел – это признак [5]. В начале алгоритма задается количество информативных признаков, которые необходимо найти. Муравей останавливается тогда, когда пройдено необходимое количество признаков. На каждом шаге происходит испарение феромона. На каждой итерации выбирается набор признаков (путь муравья) с минимальной ошибкой. Алгоритм завершается тогда, когда пройдено требуемое количество итераций, либо когда минимальная ошибка становится больше (или остается неизменной). Таким образом, количество феромона на каждой грани обратно пропорционально проценту ошибок, полученному при классификации объектов по этому признаку. В данном подходе предполагается, что существует какой-то оптимальный набор признаков, на котором классификаторы дают минимальный процент ошибок. Следовательно, существует полносвязный подграф, на гранях которого будет максимальное количество феромона. На гранях же, соединяющих неинформативные признаки феромона должно быть минимальное количество.

Эксперимент. Исходными данными для эксперимента послужили данные из набора KDDCup'99. Несмотря на то, что этот набор данных создан довольно давно, исследователи продолжают использовать его для проверки работы алгоритмов выбора признаков. Объясняется это следующими факторами: большой объем набора данных, около 5 млн. объектов; популярность KDDCup'99 позволяет сравнивать полученные результаты с результатами других исследователей и делать выводы относительно результативности предлагаемых методов. Каждая запись набора представляет собой полную информацию об одном соединении. Соединение – это последовательность TCP-пакетов, начинающихся и заканчивающихся в некоторые определенные моменты, между которыми данные переходят между исходным и целевым IP-адресами по определенному протоколу. Каждое соединение было помечено либо как нормальное, либо как атака, с точным указанием одного определенного типа атаки [6].

Основным критерием информативности признаков в задачах классификации является процент ошибок. Чем информативнее признак или группа признаков, тем выше процент ошибок при его отсутствии в итоговом наборе признаков. Однако вычисление процента ошибок классификации связано с большими затратами машинного времени. В связи с этим при поиске информативных признаков были учтены следующие условия: объекты классифицируются наиболее простым способом для того, чтобы вычисление процента ошибок для каждого из признаков происходило максимально быстро; алгоритм классификации и его параметры выбраны таким образом, чтобы на каждом этапе эксперимента процент ошибок зависел в первую очередь от изучаемого критерия информативности, а не от способа классификации.

Поэтому для всех методов выбора признаков использовался один и тот же классификатор: метод k ближайших соседей. Оптимальное количество соседей было выбрано равным 5 на основе предварительных экспериментов. Расстояние между объектами рассчитывалось как Евклидово. Все признаки были предварительно нормализованы. Кроме того, сведения по атакам, для которых имеется менее двух сотен записей, не могут являться репрезентативными и были исключены из эксперимента. Из оставшихся записей было сформировано 5 выборок: по 100 записей на каждое из 10 типов соединений. Выборки были составлены таким образом, что одна запись о соединении встречалась лишь в одной выборке. Из выборки были исключены признаки, которые измерялись по номинальной шкале. В результате получился набор данных 5000 записей по 10 соединениям, каждое из которых характеризовалось 38 признакам.

На вход генетического алгоритма сокращения размерности подавались 38 признаков, алгоритм последовательно сокращал их до 2. На рис. 1 и 2 показан график зависимости правильно классифицируемых записей от количества признаков на обучающей и тестовой выборке для элитарного метода селекции.

Для селекции методом колеса рулетки зависимости правильно классифицируемых объектов мало отличаются от элитарного метода. Характер зависимости процента правильно классифицируемых объектов при выборе признаков с использованием жадного алгоритма совпадает с приведенными выше зависимостями. Таким образом, был сделан вывод, что оптимальным является количество признаков, равное 11.

После 12 запусков генетического алгоритма в итоговый набор были отобраны 11 признаков, которые исключались из наборов как неинформативные два и менее раз: logged_in, dst_host_diff_srv_rate, dst_host_same_srv_rate, duration, src_bytes, dst_bytes, dst_host_same_src_port_rate, wrong_fragment, root_shell, count, srv_count.

Рис. 1. График зависимости правильно классифицируемых записей от количества признаков для элитарного метода селекции

Рис. 2. График зависимости правильно классифицируемых записей от количества признаков на тестовой выборке для элитарного метода селекции

Эксперименты с муравьиным алгоритмом отличались друг от друга длиной пути муравья: расчеты проводились для 20, 15, 11, 8 и 6 признаков, соответственно. Каждый эксперимент включал 10 итераций. Минимальный процент ошибок был получен на наборе из 11 признаков. По результатам экспериментов, основываясь на количестве наиболее удачных наборов, в которых присутствовал тот или иной признак, в итоговый набор были отобраны следующие признаки: src_bytes, hot, logged_in, su_attempted, is_guest_login, count, dst_host_same_srv_rate, dst_host_diff_srv_rate, dst_host_same_src_port_rate, dst_host_serror_rate, dst_host_srv_serror_rate.

Однако, стоит обратить внимание на особенности алгоритма. Так как набор признаков рассматривается в виде графа, а муравей каждый раз выбирает ребро, которое связывает два признака, то некоторые признаки попали в итоговые наборы только в паре. Так, например, признаки dst_host_diff_srv_rate и dst_host_same_src_port_rate всегда присутствуют вместе во всех самых успешных наборах признаков. Признак dst_host_same_srv_rate встречается в тех же наборах, но не встречается в самых удачных наборах из малого количества признаков (6–8). Признаки hot, logged_in и count так же часто встречаются вместе.

Сравнение с аналогами. Специалисты, изучавшие способы выбора признаков для обнаружения вторжений, по-разному решали поставленную задачу. Здесь можно выделить два подхода: поиск информативных признаков для каждого класса соединений [7, 8] в отдельности или же поиск универсальных информативных признаков[9–11].

Первый подход удобен тем, что сведения, полученные в результате подобного анализа, позволяют построить ансамбль классификаторов. Каждый классификатор при этом будет содержать информацию о соединении лишь по одному-двум признакам и будет различать соединения как принадлежащие к его классу атак или неизвестные ему. Итоговый класс соединения может быть получен, например, методом простого голосования. Таким образом, классификация может проводиться в реальном времени, что очень важно при построении СОВ. Однако, данная система будет требовать постоянного обновления и будет совершенно неустойчива к новым видам атак: аномальные значения признаков могут привести к тому, что соединение не будет идентифицировано ни одним из классификаторов и таким образом будет принято решение о его «нормальности».

Другие исследователи на основе результатов обучения моделей и классификаторов формируют способ вычисления количественного показателя информативности каждого признака [9, 10]. Недостаток данного подхода в том, что группа признаков, имеющих максимальное значение полученного показателя, может быть менее информативна, чем набор признаков с меньшим значением данного показателя. Два малоинформативных признака могут давать очень малый процент ошибок при использовании их не по отдельности, а в паре. Формирование новых информативных признаков – задача отдельного исследования (feature extraction).

Некоторые исследователи рассматривают задачу выбора признаков как задачу оптимизации [5, 12, 13], при этом максимизируется (или минимизируется) функция, зависящая от процента ошибок, получаемого при обучении модели на итоговом наборе признаков. Значения признаков при этом чаще всего нормализуются и приводятся к одной шкале, но могут быть оставлены в первоначальном виде. Решение задачи классификации в данном случае может решаться множеством способов, в частности: классическим генетическим, алгоритмом перемещения бактерий, алгоритмом муравьиной колонии и т.д. [14].

Сравним полученные результаты работы генетического алгоритма и алгоритма муравьиной колонии с результатами работы других исследователей. Для сравнения были выбраны работы [7–10] по следующим причинам:

- в качестве алгоритма классификации в них используется алгоритм *k* ближайших соседей, потому разницу в результативности алгоритмов выбора признаков нельзя будет отнести к алгоритму классификации;
- в данных работах классификация проводится по всем классам соединений, а не по двум или четырем классам, как делают другие исследователи;

Авторы работ [7–10] включают в набор информативных следующие признаки: src_bytes, service, count, dst_bytes, srv_count, logged_in, dst_host_same_src_port_rate, wrong_fragment, protocol_type, dst_host_srv_count.

Указанные признаки реже всего удалялись при работе генетического алгоритма, а также входили в наиболее успешные наборы в алгоритме муравьиной колонии, на основании чего можно сделать вывод о применимости данных методов для решения задачи селекции признаков.

Заключение и выводы. В результате проведенного исследования можно сделать нижеследующие выводы.

Для выявления оптимального количества информативных признаков удобно использовать жадный алгоритм: по форме зависимости несложно определить, при каком количестве признаков ошибка начинает резко падать либо возрастать.

Генетический алгоритм и алгоритм муравьиной колонии можно использовать для формирования информативного признакового пространства. Алгоритмы позволяют выявить как отдельные информативные признаки, так и группы признаков, совместное использование которых дает уменьшение ошибки классификации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Trost R.* Practical Intrusion Analysis. Prevention and Detection for the Twenty-First Century. – Addison-Wesley, 2010. – 455 p.
2. *Кормен Т., Лейзерсон Ч., Ривест Р., Штайн К.* Алгоритмы: построение и анализ, 2е изд. – М.: Изд. дом «Вильямс», 2005. – 1296 с.
3. *Емельянов В.В., Курейчик В.В., Курейчик В.М.* Теория и практика эволюционного моделирования. – М.: Физматлит, 2003. – 432 с.
4. *Dorigo M., Maniezzo V., Colorni A.* Ant System: Optimization by Colony of Cooperating Agents // IEEE Transaction Systems, Man and Cybernetics. – Part B. 1996. – Vol. 26. – P. 29-41.
5. *Олейник А.А., Субботин С.А.* Мультиагентный метод с непрямой связью между агентами для выделения информативных признаков // Штучний інтелект. – 2009. – № 4. – С. 75-82.
6. *KDD-CUP-99* [Электронный ресурс] – Режим доступа: http://kdd.ics.uci.edu/databases/kddcup99/task.html.
7. *Olusola A.A., Oladele A.S., Abosede D.O.* Analysis of KDD ’99 Intrusion Detection Dataset for Selection of Relevance Features // Proceedings of the World Congress on Engineering and Computer Science. Vol I. – San Francisco, 2010. – P. 162-168.
8. *Kayacık H.G., A. Zincir-Heywood N., Heywood M.I.* Selecting Features for Intrusion Detection: A Feature Relevance Analysis on KDD 99 Intrusion Detection Datasets [Электронный ресурс]. – Режим доступа: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.7574&rep=rep1&type=pdf.
9. *Singh S., Silakari S.* An ensemble approach for feature selection of Cyber Attack Dataset // International Journal of Computer Science and Information Security. – 2009. – Vol. 6, № 2. – P. 297-302.
10. *Tavallaee M., Bagheri E., Lu W., Ghorbani A.A.* A detailed analysis of the KDD CUP 99 data set // Proceedings IEEE international conference on computational intelligence for security. – Ottawa, 2009. – P. 53-58.
11. *Wang W., Knapskog S. J., Gombault S.* Attribute Normalization in Network Intrusion Detection // Proceedings 10th International Symposium on Pervasive Systems, Algorithms, and Networks. – Kaohsiung, 2009. – P. 448-453.
12. *Van Dijck G., Van Hulle M., Wevers M.* Genetic Algorithm for Feature Subset Selection with Exploitation of Feature Correlations from Continuous Wavelet Transform: a real-case Application // International Journal of Computational Intelligence. – 2004. – Vol. 1. – P. 1-12.
13. *Kim Y., Street W. Nick, Menczer F.* Feature Selection in Data Mining // Data mining. – 2003. – P. 80-105.
14. *Ходашинский И.А., Мещеряков Р.В., Горбунов И.В.* Методы нечеткого извлечения знаний в задачах обнаружения вторжений // Вопросы защиты информации. – 2012. – № 1. – С. 45-50.

Статью рекомендовал к опубликованию д.т.н., профессор Ю.П. Ехлаков.

Гусакова Екатерина Николаевна – Томский государственный университет систем управления и радиоэлектроники; e-mail: rouxrenard@list.ru; 634050, г. Томск, пр. Ленина, 40; тел./факс: 83822900111; аспирантка.

Мещеряков Роман Валерьевич – e-mail: mrv@security.tomsk.ru; тел.: 83822413426; д.т.н.; профессор.

Ходашинский Илья Александрович – e-mail: hodashn@rambler.ru; тел./факс: 83822900111; д.т.н.; профессор.

Gusakova Ekaterina Nikolaevna – Tomsk State University of Control Systems and Radioelectronics; e-mail: rouxrenard@list.ru; 40, Lenin Avenue, Tomsk, 634050, Russia; phone: +73822900111; postgraduate student.

Meshcheriakov Roman Valerievich – e-mail: mrv@security.tomsk.ru; phone +73822413426; dr. of eng. sc.; professor.

Hodashinsky Ilya Alexandrovich – e-mail: hodashn@rambler.ru; phone/fax: +73822900111; dr. of eng. sc.; professor.

УДК 004.056

М.Н. Жукова, Н.А. Коромыслов

МОДЕЛЬ ОЦЕНКИ ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ С ПРИМЕНЕНИЕМ АППАРАТА НЕЧЕТКОЙ ЛОГИКИ*

Рассматривается подход к построению защищенных автоматизированных систем. Проанализированы существующие решения в области анализа защищенности, показаны трудности их применения на территории РФ. Предложен и описан подход, основанный на применении аппарата нечеткой логики. Представлена модель оценки защищенности автоматизированной системы с применением аппарата нечеткой логики. Описаны основные составляющие модели и процедура интеграции статистических данных, накопленных автоматизированной системой в процессе функционирования. Предложено применение прецедентного подхода к разработке модифицированного алгоритма оценки защищенности автоматизированной системы. За счет применения механизмов нечеткой логики отсутствуют требования к строгой формализации данных и появляется возможность работы с качественными характеристиками. Однако остается проблемы предварительной настройки некоторых параметров, таких как, выбор представления лингвистических переменных; определение граничных значений термов; выбор метода дефаззификации. На основе предложенной модели разработан алгоритм автоматизированной системы на прецедентах оценки защищенности АС, представлена его схема. Таким образом, проведено объединение трех подходов к оценке и анализу защищенности АС: использование стандартизированного подхода; использование результатов работы СЗИ АС; использование аппарата нечеткой логики. Эффективное сочетание данных подходов позволяет, предусмотреть требования стандартов, учесть прецеденты ИБ, что позволит более динамично управлять АС и с большей эффективностью оценивать защищенность.

Информационная безопасность; автоматизированная система; оценка защищенности; нечеткая логика

M.N. Zhukova, N.A. Koromyslov

MODEL OF THE AUTOMATED SYSTEM SECURITY ASSESSMENT WITH USE OF THE FUZZY LOGIC

Approach to creation of the protected automated systems is considered. Existing decisions in the field of the security analysis are analysed, difficulties of their application in the territory of the Russian Federation are shown. The approach based on use of the fuzzy logic is offered and described. The model of an assessment of automated system security with use of the fuzzy logic is presented. The main components of model and procedure of statistical data integration which have been saved up by automated system in the course of functioning are described. Application of case approach to development of the modified algorithm of an assessment of the automated system security is offered. At the expense of use of the fuzzy logic mechanisms there are no requirements to strict formalization of data and there is a possibility to work with qualitative characteristics. However there are problems of preliminary control of some parameters, such as, a choice of linguistic variables representation; determination of boundary values of terms; choice of a

* Работа выполнена при финансовой поддержке РФФИ, соглашение НК 13-07-00222\13 от 09.04.2013 г.