УДК 004.75

ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ ИССЛЕДОВАНИЯ ЭФФЕКТОРОВ ОБНАРУЖЕНИЯ СЕТЕВЫХ ВТОРЖЕНИЙ

А.В. Скатков, А.А. Брюховецкий, Л.П. Луговская

ФГАОУ ВО Севастопольский государственный университет
г. Севастополь, ул. Университетская, 33
E-mail:a.alexir@mail.ru

Предлагается подход к построению модели исследования эффекторов для процессов обнаружения сетевых вторжений. Целевое требование к модели – обеспечение диалогового режима поддержки принятия решений в процессе тестирования детекторов в режиме стендовых испытаний на основе моделирующих имитационных алгоритмов и учета экспертных суждений.

Введение. Основная тенденция развития современных телекоммуникаций – создание глобального информационного пространства и глобальных сетей. Развитие информационных технологий на базе телекоммуникационных сетей (ТКС) приводит к повышению эффективности промышленного производства и многих инфраструктур в энергетической, транспортной, социальной сферах, в области мониторинга и экологического контроля окружающей среды. Данный факт накладывает безусловные ограничения на требования к гарантоспособности и безопасности ТКС. ТКС должна обеспечивать высокую реактивность, достоверность и своевременность передачи информации между функциональными подсистемами инфраструктуры. Отказ или нарушение работы ТКС может привести к дезорганизации функционирования всей инфраструктуры и, следовательно, опасности возникновения критических ситуаций. Так сбои в работе систем экологического мониторинга, вызванные сетевыми атаками на элементы ТКС, могут иметь катастрофические последствия, вплоть до экологической катастрофы.

ТКС является сложной территориально, функционально, структурно распределенной системой, характеризующейся наличием множества взаимодействующих компонентов, системных и прикладных информационных и телекоммуникационных процессов. Поэтому, безопасность ТКС является комплексным понятием, включающим в себя аппаратную, программную, технологическую безопасность [1, 2], а так же безопасность, связанную с наличием актов нарушения прав доступа и вирусных атак в ТКС.

Вышесказанное подтверждает актуальность проблемы обеспечения информационной безопасности, в автоматизированных системах контроля окружающей среды (СКОС), которая обусловлена следующими факторами [2]:

1. Современные уровни и темпы развития средств защиты информации в ТКС СКОС значительно отстают как от темпов развития информационных технологий в целом, так и от развития методов и типов атак в ТКС.

2. Рост числа пользователей ТКС, среди которых увеличивается и количество злоумышленников, стремящихся нарушить безопасность сетей с той или иной целью.

3. Увеличение частоты использования систем облачного хранения в СКОС, обработки информации, и, как следствие, увеличение возможных точек атак.

Основная проблема в обнаружении вторжений состоит в проведении объективной оценки состояния контролируемого источника вторжений с точки зрения его правильной классификации. В настоящее время для ее решения используются различные статистические модели оценки вероятности появления заданных значений (событий) [3–6], скрытые марковские модели [7], модели на основе нечеткой логики [8], а также методы интеллектуальной обработки данных, такие как нейронные сети [9], ассоциативные правила [10], решающие деревья [11], кластеризация данных [12], искусственные иммунные системы (ИИС) [13] и другие.

На основе результатов проведенного аналитического обзора литературных источников следует констатировать, что на сегодняшний день не существует однозначно надежного способа защиты от неизвестных атак. Объясняется это рядом причин:

- большинство существующих методов обнаружения вторжений не учитывают особенностей современного состояния IT-отрасли;
- известные модели не дают ни четких ответов, ни рекомендаций по ряду ключевых вопросов, например, как выбирать параметры наблюдения и настройки, как устанавливать границы для шкал измерения параметров, как оценивать достоверность контроля трафика при малых выборках и другие;
- встречающиеся в литературе модели СОВ имеют серьезные недостатки, которые ограничивают их широкое применение. Главные из них – это высокий уровень ложных тревог, который во многом обусловлен изменяющимся состоянием сети, отсутствием периодической модификации правил классификации, сложность реконфигурации системы при введении нового объекта наблюдения и др.

Таким образом, наиболее актуальными проблемами, требующими своего разрешения уже сегодня, являются: повышение уровня достоверности классификации состояний трафика, распознавание атак на ранних стадиях обнаружения, снижение числа ложных тревог, классификации событий при малых выборках, принятие решений в условиях нестационарного трафика. Для разрешения указанных проблем, перспективными, на наш взгляд, являются следующие направления синтеза эффективных детекторов и построения решающих правил, базирующиеся на следующих подходах:

1. Адаптивной интеллектуальной обработке данных (нечеткие системы, экспертные системы, гибридные нейросетевые детекторы, методы искусственного иммунитета). Данное направление характеризуется достаточно высокой достоверностью обнаружения аномалий (А-событий), а так же возможностью обнаружения неизвестных ранее типов. К недостаткам этих методов следует отнести: потребность в высоких вычислительных мощностях, сравнительно длительное время обнаружения А-события.

2. Классических методах статистического анализа данных. Детекторы, построенные на основании данного метода, позволяют за сравнительно небольшой временной промежуток с заданным уровнем достоверности определить наличие А-события в ТКС, в том числе ранее неизвестного типа или вида. Недостаток: трудно обнаруживаются вторжения, которые приводят к незначительным, медленным изменениям системных показателей ТКС.

В работе развиваются методы на основе комплексного решения задачи обнаружения вторжений с использованием моделей адаптивной интеллектуальной обработки данных и классических статистических моделей.

Целью настоящей работы является разработка методов исследования эффекторов обнаружения сетевых вторжений. Под термином «эффекторы» будем понимать комплексное качество, описывающее совокупность факторов и системных свойств, которые определяют эффективность как векторную величину в факторном пространстве настраиваемых параметров. Описание допускает в рамках статистической интерпретации соблюдение метрик теории принятия гипотез и теории принятия решений.

Для достижения конечной цели необходимо разработать программное обеспечение для исследования эффективности методов обнаружения вторжений. Использование системного подхода позволяет сформулировать основные принципы, которым должна удовлетворять разрабатываемая система.

1. Предлагается использовать комплексный подход к обнаружению вирусных атак, который сочетает две дополняющие друг друга технологии. Первая позволяет предвосхищать будущие угрозы вирусных вторжений и базируется на методах интеллектуального анализа данных, в то время как вторая использует

информацию об изменении вектора системных показателей ТКС.

2. Для реализации подходов требуется разработка структуры СОВ, которая содержит следующие функциональные модули: предварительной обработки; понижения размерности входных данных; настройки и тестирования, оптимизации настроечных параметров; классификации состояний сетевого трафика; адаптации параметров решающих правил к текущему состоянию трафика; поддержки принятия решений по формированию выходного сигнала о текущем состоянии трафика; определения достоверности контроля сетевого трафика в условиях дефицита априорной информации об источнике вторжений, включая определение ошибок первого и второго рода, объемы контролируемых выборок, моментов времени модификации решающих правил и др.

3. Функционирование СОВ должно поддерживаться ЛПР на основе многократных результатов измерений, получаемых при оценке значений контролируемых параметров нестационарного сетевого трафика за различные временные интервалы.

4. Тестирование системы должно быть не одноразовым, а постоянным в процессе функционирования СОВ, поскольку контролируемая среда является нестационарной и со временем информативность настраиваемых параметров решающих правил уменьшается.

5. Неизбежность использования средств имитационного моделирования, которое повышает быстродействие принятия решений при настройке параметров системы и восполняет дефицит контролируемой информации.

6. Концепция разработки СОВ должна иметь ограниченные возможности по ознакомлению с принципами ее построения. Это позволит уменьшить эффект от потенциальных угроз, которые могут быть осуществлены злоумышленниками.

7. Установлено, что программная подсистема для исследования мощности статистических критериев является сложной системой. Системообразующим фактором является процесс вычисления статистических критериев, что определяет структуру подсистемы и связи между её модулями.

8. Необходимо определить функции задачи исследования мощности статистических критериев, выделить структуру программного комплекса и связи между элементами структуры.

9. При дальнейшем совершенствовании программного комплекса следует руководствоваться накопленным к этому моменту опытом его эксплуатации.

Учитывая сформулированные требования к разрабатываемой системе определим её основные функции:

- генерация случайных выборок с априорно заданными параметрами;
- оценивание статистических вероятностей гипотез нахождения ошибок первого и второго рода;
- модификация решающих правил поддержки принятия решений;
- измерение значений параметров с целью их адаптации к текущему состоянию сетевого трафика;
- статистическое управление на основе управляемых генераторов;
- реализация методики статистической обработки по целевым программам эксперта, ЛПР;
- обеспечение взаимодействия эксперта с системой посредством диалогового интерфейса и предоставление возможности исследователю управлять комплексом.

Для реализации указанных функций требуется разработка архитектуры программной системы, в состав которой входят следующие модули: выбора режима работы СОВ и задания параметров выборок; выбора модели интеллектуального анализа данных; выбора модели статистического анализа; модуль обучения, тестирования и настройки; модуль адаптации и оценки достоверности результатов анализа; блок принятия решений об А-событии; блок принятия решений о модификации правил и параметров моделей; модуль пополнения базы образцов сетевого трафика из сети интернет.

Проектируемая система может развиваться за счет:

– увеличения скорости вычисления статистических критериев и подсчета статистических вероятностей допущения ошибок первого и второго рода путем оптимизации внутренних структур модулей, а так же использования параллельных и распределенных вычислений;

– пополнения используемых методов интеллектуальной обработки данных;

– пополнения библиотеки исследуемых статистических критериев.

С другой стороны, можно объединить все подсистемы в один модуль с целью его применения в системах более высокого иерархического уровня.

С целью дальнейшего совершенствования предлагаемого подхода представляется перспективным рассмотреть многомерную задачу классификации на множестве альтернативных признаков, Парето-подхода для задач многомерной оптимизации, а также целесообразность предварительной фильтрации трафика.

Работа выполнена по теме №3866 в рамках базовой части государственного задания.

СПИСОК ЛИТЕРАТУРЫ

1. *Искусственные* иммунные системы и их применение / под ред. Д. Дасгупты: пер. с англ. – М.: Физматлит, 2006. – 344 с.
2. *Информационные* технологии для критических инфраструктур: моногр. / под ред. А.В. Скаткова. – Севастополь: СевНТУ, 2012. – 306 с.
3. *Varghese S.M., Jacob K.P.* Anomaly detection using system call sequence sets // Journal of software. – 2007. – № 2 (6). – P. 14–21.
4. *Yeung D.Y., Ding Y.* Host-Based Intrusion Detection Using Dynamic and Static Behavioral Models // Journal of Pattern Recognition. – 2003. – № 36. – P. 229–243.
5. *Shon T., Moon J.* A. Hybrid Machine Learning Approach to Network Anomaly Detection // Journal of Information Sciences. – 2007. – № 177. – P. 3799–3821.
6. *Kabiri P., Ghorbani A.* Research in Intrusion Detection and Response. A Survey // International Journal of Network Security. – 2005. – № 1. – P. 84–102.
7. *Khanna R., Liu H.* System Approach to Intrusion Detection Using Hidden Markov Model // *IWCMC*, July 3–6, Vancouver, British Columbia, Canada. – P. 349–354.
8. *Castro P.A.* Designing Ensembles of Fuzzy Classification Systems: An Immune-Inspired Approach // Proceedings of the 4th International Conference on Artificial Immune Systems (ICARIS), Lecture Notes in Computer Science, Springer-Verlag, Berlin. – 2005. – № 3627. – P. 469–482.
9. *Beghdad R.* Critical Study of Neural Networks in Detecting Intrusions // Journal of Computers and Security. – 2008. – № 27. – P. 168–175.
10. *Sheikhan M., Jadidi Z.* Misuse Detection Using Hybrid of Association Rule Mining and Connectionist Modeling // World Appl. Sci. J., Vol.7 (Special Issue of Computer & IT), 2009. – Vol. 7. – P. 31–37.
11. *Брюховецкий А.А., Скатков А.В.* Обнаружение уязвимостей в критических приложениях на основе решающих деревьев // Радиоэлектронные и компьютерные системы. – Харьков: Изд-во ХАИ, 2013. – № 5 (64). – С. 18–23.
12. *Abraham A., Jain R.* Soft Computing Models for Network Intrusion Detection Systems. Classification and Clustering for Knowledge Discovery Studies // Journal Computational Intelligence. – 2005. – P. 191–207.
13. *Брюховецкий А.А., Скатков А.В.* Адаптивная модель обнаружения вторжений в компьютерных сетях на основе искусственных иммунных систем // Электротехнические и компьютерные системы. – 2013. – № 12 (88). – С. 102–111.