УДК 004.056.53

С. В. БАЛАКИН, И. А. ЖУКОВ

Национальный авиационный университет, Украина

ОБНАРУЖЕНИЕ КОМПЬЮТЕРНЫХ АТАК С ПОМОЩЬЮ МЕТОДА ОТКЛОНЕНИЙ

Проведен анализ результатов обнаружения компьютерных атак с помощью метода отклонений (отклоняющихся значений). Обсуждается обнаружение компьютерных атак методом отклонений, а также его возможности в сравнении с традиционными подходами. По результатам анализа определены погрешности в расчетах отклонений процессов и внесены корректировки, которые значительно повышают показатели производительности. При этом разработана модель обнаружения атак на основе информации о поведении потоков информации в сети, а необходимая эффективность обеспечивается обнаружением отклоняющихся значений данных.

Ключевые слова: *атака, компьютерная система, отклонение, вторжение, информационная система, состояние объекта.*

Введение

Благодаря интенсивному использованию интернета безопасность сети становится ключевым фундаментом для всех веб-приложений. Обнаружение вторжений и выявление атак путем анализа информации записей в сетевых процессах – все это можно рассматривать как один из важных способов для эффективного решения проблем в области сетевой безопасности [1].

Вторжение может поставить под угрозу безопасность как данных, так и самой системы. С развитием информационных сетей и увеличением скорости передачи данных, возникают опасности злонамеренного использования интернета. Необходимы более надежные и эффективные системы контроля, решающие проблему защиты сетей без человеческого взаимодействия.

Использование инструментов обнаружения аномалий и атак затруднено сферами назначения. Чем уже область применения, тем проще применять к ней те или иные инструменты исследований. В открытом доступе находятся такие популярные сетевые системы как SNORT как WireShark [2].

Хорошую производительность показывают системы, которые базируются на работе с нейронными сетями (НС). Отличительной особенностью НС является то, что они не программируются, а обучаются. Это одно из главных преимуществ НС перед традиционными алгоритмами. Обучение состоит в связях между нейронами, которые определяют соотношение входных и выходных сигналов нейрона. НС базируется на "обучаемости" и не позволяет аналитически просчитывать уровень погрешностей. К недостаткам можно отнести то, что топология сети и веса узлов определяются только после достаточно большого количества проб и ошибок.

Некоторые виды вторжений в сеть отлично предупреждаются с помощью IDS (Intrusion Detection Systems). Системы обнаружения вторжений используются для обнаружения некоторых типов вредоносной активности, которая может нарушить безопасность компьютерной системы. К такой активности относятся сетевые атаки против уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к важным файлам, а также действия вредоносного программного обеспечения (компьютерных вирусов, троянов и червей).

Архитектура IDS включает:

– сенсорную подсистему, предназначенную для сбора событий, связанных с безопасностью защищаемой системы;

– подсистему анализа, предназначенную для выявления атак и подозрительных действий на основе данных сенсоров;

– хранилище, обеспечивающее накопление первичных событий и результатов анализа;

– консоль управления, позволяющая конфигурировать СОВ, наблюдать за состоянием защищаемой системы и СОВ, просматривать выявленные подсистемой анализа инциденты.

Существует несколько способов классификации IDS в зависимости от типа и расположения сенсоров, а также методов, используемых подсистемой

анализа для выявления подозрительной активности. Во многих простых IDS все компоненты реализованы в виде одного модуля или устройства.

Основные недостатки IDS НС:

– недопустимо высокий уровень ложных срабатываний и пропусков атак;

– слабые возможности по обнаружению новых атак;

– большинство вторжений невозможно определить на начальных этапах;

– трудно, иногда невозможно, определить атакующего, цели атаки;

– отсутствие оценок точности и адекватности результатов работы;

– невозможно определять «старые» атаки, использующие новые стратегии;

– сложность обнаружения вторжений в реальном времени с требуемой полнотой в высокоскоростных сетях;

– слабые возможности по автоматическому обнаружению сложных координированных атак;

– значительная перегрузка систем, в которых функционируют СОВ, при работе в реальном времени.

Для решения указанных проблем предложен новый подход к методу отклонений на основе IDS. Обнаружение отклонений производится в целях повышения точности и стабильности обнаружения.

Предложенный подход включает два этапа: обучение с нормальными наборами данных и тестирования с наборами данных с образцами вторжений. Набор различных данных используется для подготовки IDS на начальном этапе в распределенной среде хранения. Нормальные наборы данных повышают производительность системы обнаружения вторжений. При вторжении в набор данных, который используется для вычисления значения ошибки с обученными наборами данных. Если значение количества ошибок увеличивается от определенного порогового значения, то тестируемый набор данных необходимо рассматривать в качестве аномалии.

Различные способы могут быть использованы для обнаружения вторжения, но каждый из них является специфическим для конкретного метода.

Основная цель системы обнаружения вторжений - эффективно обнаруживать атаки. Важно выявить атаку на начальной стадии, чтобы уменьшить ее последствия. В работе предложен подход отклоняющихся значений, при котором аномалия набора данных измеряется факторами отклонений (NOF).

Модель обучения состоит из массивов данных с распределенной средой хранения для повышения производительности системы обнаружения вторжений. Экспериментальные результаты показали, что предложенный подход выявляет аномалии эффективней, чем известные методы.

Первые работы являлись концептуальными, так как в них делалась попытка использования не определенных фильтров или методов, а теории вероятности и математических подходов к решению задач.

Широко используются методы машинного обучения (искусственных нейронных сетей) для обнаружения вторжений основанных. Многие методы обнаружения вторжений реализованы в программных инструментах анализа сетевого трафика [3].

Разработке метода обнаружения атак на основе информации о поведении отклоняющихся значений в сети посвящена работа.

Постановка задачи

Классификация проблемы способствует подбору лучших подходов к решению задач. Системы обнаружения вторжений делятся на три категории:

– host-based IDS;

– сетевые IDS;

– IDS оценки уязвимости.

Известны основные модели, используемые для анализа событий и обнаружения атак:

– неправильное использование модели обнаружения – система обнаружения вторжений путем поиска уязвимостей или известных сигнатур вторжений;

– модель обнаружения аномалий – система обнаружения вторжений с помощью функции поиска отклонений сетевого трафика.

Некоторые IDS могут обнаруживать признаки вторжений без указания типов атак, но они чувствительны к ложным тревогам. Влиянию ложных тревог и сетевых аномалий на систему нужно уделять внимание при построении систем обнаружения вторжений [4]. В работе использован предложенный IDS подход, основанный на модели обнаружения аномалий [5].

Основная цель состоит в том, чтобы разработать IDS на основе модели обнаружения аномалий, которая имела бы низкий порог ложных тревог, была адаптивной и работала в реальном времени. На рис. 1 приведена архитектура системы, в которой пакеты принимаются из интернета, а свободная сетевая система SNORT используется для сбора данных. Системы изображенной на рисунке вполне достаточно для работы с потоками информации в данных условиях.

Первоначально функции, предлагаемые IDS вычисляют расстояние между извлеченными функ-

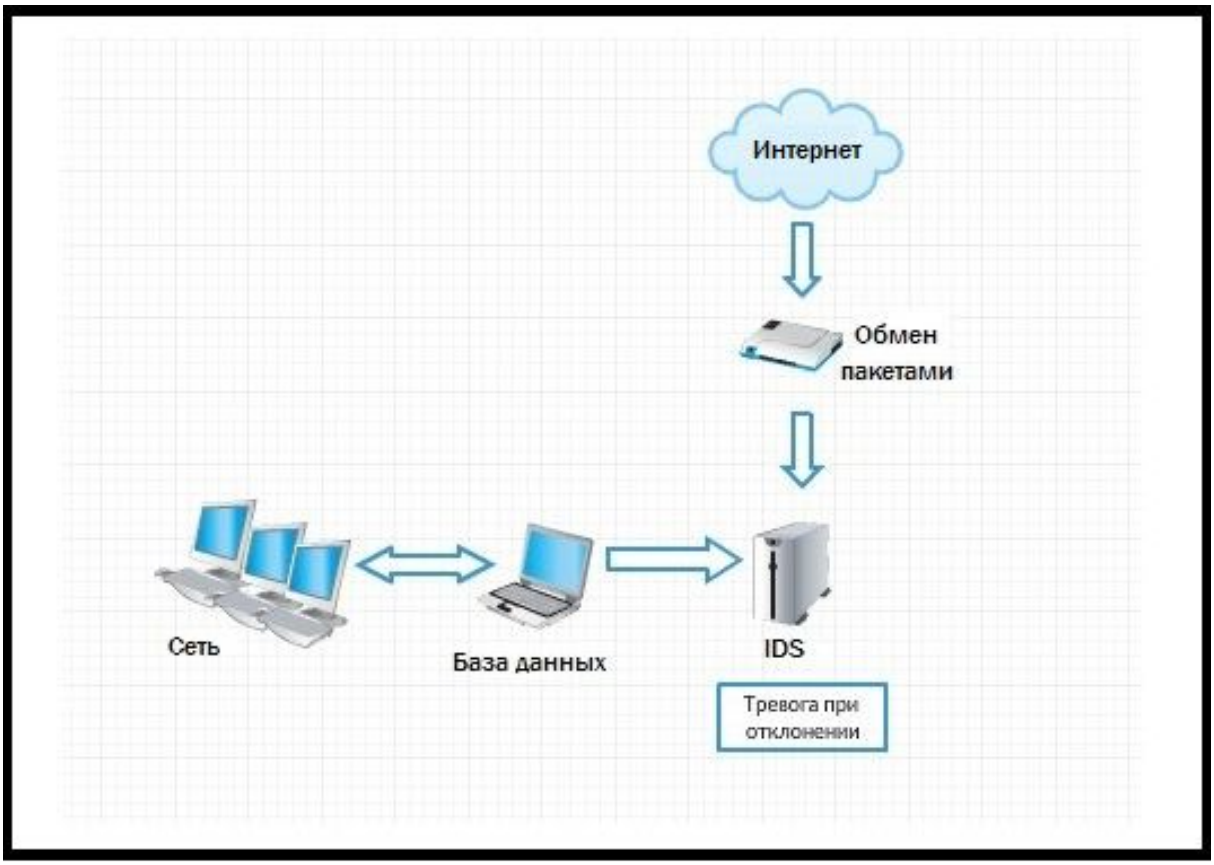

Рис. 1. Предлагаемая архитектура системы

циями и обученной моделью. Модель обучения состоит из больших массивов с распределенной средой хранения данных для повышения производительности системы обнаружения вторжений. Таким образом, если аномальное значение превышает заданный порог, то он генерирует ложную тревогу [6].

Обнаружение вторжений

Данные обычной выборки имеют плотную окрестность, тогда как при отклонениях они разбросаны далеко друг от друга. Выпадающие отклонения являются объектами внешних слоев [7].

Основная идея подхода заключается в том, чтобы назначить данные с фактором отклонения, и найти данные, чье поведение отличается по сравнению с большим количеством нормальных потоков информации.

Этапы алгоритма, используемого для расчета отклонений для данных примеров, следующие:

– вычисляется максимально допустимое отклонение (О) для каждого примера данных (Д);

– вычисляется расстояние достижимости для каждого из примеров Д относительно друг друга (п): максимальное расстояние (Д,п) = max{О(п), d(Д,п)} – это расстояние между данными примера Д и данными примера п;

– вычисляется локальная плотность достижимости для каждого примера Д, основываясь на обратном отношении доступности средних расстояний достижимости с помощью MinPts (минимальное количество объектов) и примеров Д с ближайшими соседями;

– определяются отклонения всех примеров Д по отношению к усредненным данным с коэффициентами плотности достижимости MinPts ближайших соседей.

Преимущества предложенного подхода отклонений показаны на рис. 2. Кластеры определяются как плотные множества связанных объектов. Простой двумерный массив данных берется с гораздо большим количеством выборок в кластере К1, а потом в К2. Таким образом, плотность К2 выше плотности К1. Для каждого примера рассмотрен объект внутри кластера К1, где расстояние между ним и его ближайшим соседом больше, чем расстояние между П2 и его ближайшим соседом из кластера К2. Поэтому П2 не рассматривается в качестве аномального значения.

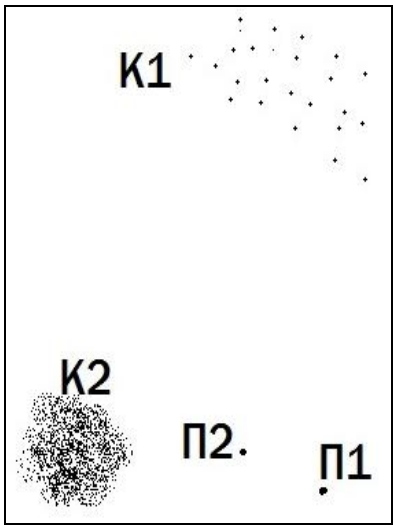

Рис. 2. Кучность обнаружения отклонений

Следовательно, обнаружение отклоняющихся значений находится в области статистики. Тем не менее, в П1 может быть обнаружено отклонение с использованием только ближайших соседних расстояний. В качестве альтернативы, отклонения способны захватить оба значения (П1 и П2) в связи с тем, что они считают кучность всех точек (рис. 2).

Результаты и обсуждение

При исследовании количество экспериментов было основано на извлеченных данных для измерения производительности системы IDS. Эксперименты проводились на основе конфигурации: Windows 8, Core2Duo (R), CPU T7300 2,90 ГГц.

Извлеченный набор данных включал более двух тысяч записей соединений. Тестовые данные включали пять тысяч записей подключений. Набор данных включал в себя признаки, полученные от каждого соединения, а также группы меток, идентифицирующих состояние записи соединения на наличие отклонений.

Расстояние и отклонение значений данных рассчитываются предложенным способом обнаружения отклонений. Приведенные расчеты показывают, что значения отклонений увеличиваются, если расстояние между извлеченными и тестовыми данными увеличиваются. Результаты приведены в таблице.

Заключение

В работе развит подход по обнаружению отклонений для выявления вторжений в компьютерную сеть. Модель обучения состоит из массивов данных с распределенной средой, что повышает производительность системы при обнаружении вторжений. Предложенный подход применен с использованием наборов данных KDD. Подходы машинного обучения обнаружения вторжений в компьютерной сети перспективны, так как существует возможность полной автоматизации обнаружения вторжений в сетях. При исследовании оценивается производительность предложенного метода, который может обнаружить большинство аномалий в компьютерной сети. Приведены результаты использования подхода обнаружений вторжений в компьютерных сетях.

Таблица

Зависимость расстояний и отклонений выборки

№	Расстояние	Отклонение
1	3,5	5
2	1,2	2
3	4,6	8
4	2,7	3
5	3,6	7
6	0,4	1
7	1,6	2
8	4,6	9
9	2,1	4
10	3,4	5
11	0,5	1
12	6,2	11
13	5,4	10
14	0,7	1
15	3,9	6

В дальнейших исследованиях планируется использование полученных результатов для моделей обучения выборок или тестирования данных.

Литература

1. Гамаюнов, Д. Ю. Модель поведения сетевых объектов в распределенных вычислительных системах / Д. Ю. Гамаюнов, Р. Л. Смелянский // Программирование. – 2007. – № 4. – С. 20–31.

2. Network forensics analysis using Wireshark [Text] / V. Ndatinya, Z. Xiao, V.R. Manepalli, K Meng, Y.Xiao // International Journal of Security and Networks. – 2015. – Vol. 10, No. 2. – P. 91-106.

3.. Маркин, Ю. В. Обзор современных инструментов анализа сетевого трафика [Электронный ресурс] / Ю. В. Маркин // Препринты. – 2014. – 165 с. – Режим доступа: http://www.ispras.ru/preprints/docs/prep_27_2014.pdf. – 23.10.2015.

4. Шелухин, И. О. Обнаружение вторжений в компьютерные сети. Сетевые аномалии [Текст] / И. О. Шелухин. – М. : Горячая линия, 2013. –220 с.

5. Корченко, А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / А. Г. Корченко. – М. : МК-Пресс, 2006. – 320 с.

6. Masayoshi, M. The Design and Implementation of Session Based NIDS [Text] / M. Masayoshi // IEICO. – 2005. – P.551-562.

References

1. Gamayunov, D. Y., Smelianskiy, R. L. *Model povedeniya setevih elementov v raspredilitel'nikh vicheslitel'nikh sistemakh* [Model of behavior of network objects in distributed computing systems]. *Programming*, 2007, no. 4, pp. 20–31.

2. Ndatinya, V., Xiao, Z., Manepalli, V., Meng, K, Xiao, Y. Network forensics analysis using Wireshark. *International Journal of Security and Networks*, 2015, vol. 10 no. 2, pp. 91-106.

3. Markin, Y. V. *Obzor sovremennikh instrumentov analiza setevogo traffika* [Review of modern tools of network traffic analysis]. Preprints, 2014, 165 p. Available at: http://www.ispras.ru/preprints/docs/prep_27_2014.pdf (accessed 23.10.2015)

4. Shelukhin, I. O. *Obnaruzenie vtorzeniy v kompiuternie seti. Setevie anomalii* [Intrusion detection in computer networks. Network anomalies]. Moskow, Goriachaya liniya Publ., 2013. 220 p.

5. Korchenko, O. G. *Postroenie system zashiti informacii na nechetkikh mnozestvakh. Teorija i prakticheskie reshenija* [Building security systems on fuzzy sets. Theory and practical decisions]. Moskow, MK-Press Publ., 2006. 320 p.

6. Masayoshi, M. The Design and Implementation of Session Based NIDS. *IEICO,* 2005, pp. 551-562.

Поступила в редакцию 18.02.2016, рассмотрена на редколлегии 14.04.2016

ВИЯВЛЕННЯ КОМП'ЮТЕРНИХ АТАК ЗА ДОПОМОГОЮ МЕТОДУ ВІДХИЛЕНЬ

С. В. Балакін, І. А. Жуков

Представлений аналіз результатів виявлення комп'ютерних атак за допомогою методу відхилень (значень відхилення). Обговорюється виявлення комп'ютерних атак методом відхилень, а також його можливості в порівнянні з традиційними підходами. За результатами аналізу визначено похибки в розрахунках відхилень процесів та внесені коректування, які значно підвищують показники продуктивності отримані раніше. При цьому розроблена модель виявлення атак на основі інформації про поведінку потоків інформації в мережі, а необхідна ефективність забезпечується виявленням значень даних, що мають відхилення.

Ключові слова: атака, комп'ютерна система, відхилення, вторгнення, інформаційна система, стан об'єкта.

DETECTION OF COMPUTER ATTACKS USING OUTLINER METHOD

S. V. Balakin, I. A. Zhukov

Results of detection of computer attacks by the method of variations (outliers) have been analyzed. Has been discussed detection of computer attacks by the method of deviations, as well as its capabilities in comparison with existing approaches. Given analysis identified errors in the calculation of deviation process significantly increased indicators of performance. Wherein designed model of intrusion detection system, that is based on the information about the behavior of the flow of information in the network, and its efficiency is provided while detecting deviating data values.

Key words: attack, computer system, deviation, intrusion, informational system, object.

Балакин Сергей Вячеславович – аспирант каф. компьютерных систем и сетей, Национальный авиационный университет, Киев, Украина, e-mail: desertq@yandex.ru.

Жуков Игорь Анатолиевич – д-р техн. наук, профессор, зав. каф. компьютерных систем и сетей, Национальный авиационный университет, Киев, Украина, e-mail: zhuia@ukr.net.

Balakin Sergii Viacheslavovich – Graduate of Dept. of Computer Systems and Networks, National Aviation University, Kiev, Ukraine, e-mail: desertq@yandex.ru.

Zhukov Igor Anatolievich – Doctor of Technical Sciences, Professor of Dept. of Computer Systems and Networks, National Aviation University, Kiev, Ukraine, e-mail: zhuia@ukr.net.