УДК 004.942, 004.891.3

Д.С. Батурин

АНАЛИЗ МЕТОДОВ ОБНАРУЖЕНИЯ АТАК В ИНФОРМАЦИОННЫХ СЕТЯХ

В работе рассмотрены различные методы, используемые при создании гибридных интеллектуальных систем. Каждый из множества методов обладает своими преимуществами и недостатками для обработки потока трафика информационной сети.

Ключевые слова: гибридные интеллектуальные системы, сетевые атаки, обнаружение аномалий, обнаружение вторжений, обнаружение злоупотреблений, сетевой трафик.

Введение

Использование гибридных интеллектуальных систем (ГИС) получает все большее распространение в различных направлениях технической деятельности. Это обусловлено тем, что в настоящее время накоплены значительные объемы данных о различных объектах и разработано большое количество методов анализа накопленных данных. Анализ их дает возможность идентификации текущего состояния и распознавания смысловой составляющей состояния объекта и, как следствие, – часто позволяет спрогнозировать последующие состояния объекта с достаточно высокой вероятностью. Сложность современных объектов управления и объемы данных требуют автоматизированного подхода при анализе, иначе результаты будут получены значительно позднее того момента, когда понадобятся для принятия решения. При этом ГИС по сравнению с отдельными методами анализа временных рядов данных позволяют значительно повысить качество идентификации накопленных данных, уменьшая вероятность ошибки за счет сравнения результатов, полученных от различных отдельных методов, которые встроены в рамки ГИС. Анализ накопленных данных при помощи ГИС сводится к идентификации ряда данных текущего состояния объекта, к которому относятся данные с фрагментами рядов данных в накопленной базе по исследуемому объекту.

Основные направления анализа потока данных в информационных сетях

Информационная безопасность играет важную роль в современной действительности. Чаще всего утечка информации происходит через информационные сети, поэтому защита от кражи информации, от ее утечек за счет вторжения в сети злоумышленников – одно из наиболее актуальных направлений информационной безопасности. При этом традиционные методы обнаружения сетевых атак по заранее созданным шаблонам (по сигнатурам) становятся все менее эффективными из-за повышения уровня подготовки злоумышленников и их количества [1].

Сетевой трафик также представляет собой ряды данных, упорядоченных по времени прохождения пакетов в информационной сети через конкретный узел [1]. На состояние объекта (информационная сеть), кроме объемов пакетов, их количества, адресов источника и параметров назначения (адрес, порт), влияет время суток, день недели, месяца и в какой-то мере даже время года, а также накладывается общий тренд роста или падения загруженности информационной сети. К таким временным рядам данных можно применять общие методы анализа. При этом значительные отклонения от нормальных состояний в накопленных данных идентифицируются как аномальные. Далее такое состояние классифицируется либо как сервисное обслуживание, если инициатором трафика является

адрес администратора сети и при условии, что это место не может вызывать подозрений, либо как несанкционированное вторжение в информационную сеть, если инициатором аномального трафика являются внешние адреса или внутренние адреса, не входящие в доверенные. Аномальный трафик, инициированный из доверенных адресов, помечается в массиве данных особым образом как сервисный и исключается из общего анализа при оценке наличия несанкционированного вторжения в информационную сеть.

Обнаружение вторжений на основе интеллектуального анализа данных делится на две категории: обнаружение злоупотреблений и обнаружение аномалий. Системы обнаружения вторжений (СОВ), использующие обнаружение злоупотреблений, опираются в основном на выявление атак путем сравнения последовательности сетевого трафика с шаблонами, содержащимися в базе сигнатур. Они не способны выявить атаки нового вида, шаблонов которых нет в базе сигнатур, а также атаки, шаблоны которых имеются, но атака несколько модифицирована. В противоположность им системы, которые обнаруживают аномалии, способны определить новые или модифицированные вторжения, шаблоны которых отсутствуют в базе сигнатур, и распознать активность (модель поведения), отличающуюся от нормального состояния сети. При этом в последнее время полагаться на сигнатуры атак становится все сложнее, так как каждая атака достаточно легко модифицируется по отношению к предыдущим и сигнатуры последовательностей конкретных данных часто не помогут ее выявить.

В настоящее врем разработано много различных методов, помогающих выявить аномалии в рядах данных, формирующихся с течением времени и касающихся различных процессов. К такому виду временных рядов можно отнести и сетевой трафик.

Основные методы анализа трафика информационной сети

Среди методов обнаружения аномалий хорошо известны: нейронные сети, вейвлет-анализ, кластерный анализ, фрактальный анализ, нечеткая логика [6], иммунные системы, метод опорных векторов, статистический анализ, деревья решений, алгоритмы кластеризации, алгоритмы регрессий, байесовские сети, экспертные системы и сети Петри. Данный перечень не претендует на полноту, так как существует ряд модификаций и модернизаций перечисленных методов, кроме того, разработки в этом направлении продолжаются.

Указанные методы можно разбить на группы. Например, к первой группе (назовем ее статистической) можно отнести статистический анализ, вейвлет-анализ, кластерный анализ, фрактальный анализ, метод опорных векторов, ко второй (назовем ее «методы имитации логики») – генетические алгоритмы [4], иммунные системы, нейронные сети [5, 7], деревья решений, байесовские сети, экспертные системы.

Группа методов статистического анализа является основой ГИС для обнаружения аномалий в информационной сети [3]. К этой группе относят следующие методы: средний объем трафика в единицу времени $\overline{x}$, метод среднеквадратических отклонений σ:

$$\overline{x} = \frac{\sum_{i=1}^{N} x_i}{N}, i = \overline{1, N}, \quad (1)$$

$$\sigma = \sqrt{\frac{\sum_{i=1}^{n} (x_i - \overline{x})^2}{N}}, \quad (2)$$

где x_i – объем трафика за выбранную единицу времени t (например, секунда, минута, час и т.д.); N – количество промежутков времени t, по которым проводится усреднение.

Кроме того, к этой группе можно отнести метод цепи Маркова, метод χ-квадрат, анализ распределений интенсивности сетевого трафика и многие другие методы статистики.

Статистические методы без дополнительной обработки их результатов из-за неверного выбора набора наблюдаемых параметров или неверных размеров обобщения наборов исходных данных могут привести к тому, что модель описания потока сетевого трафика окажется слишком привязанной к конкретному промежутку времени либо слишком обобщенной. Это вызовет ложные тревоги системы или неспособность обнаружения вторжений.

Преимущества систем, работающих на основе группы статистических методов, – относительная ясность результатов, их адаптивность к изменению поведения пользователей сети, а также способность к обнаружению модифицированных атак.

Вейвлет-анализ помогает в большом объеме данных выделить наиболее весомые области, сгладив незначимые шумы. Суть его состоит в подборе коэффициентов для разложения исходного сигнала, описанного наборами данных, по базисным функциям. В качестве сигнала можно рассматривать объем сетевого трафика в единицу времени.

Самую весомую информацию вейвлет-анализ определяет на основании наиболее высокой амплитуды соответствующих колебаний сигнала, при этом колебания сигнала с меньшей амплитудой в результате обработки игнорируются. Выделение наиболее значимых сигналов сетевого трафика и их сравнение с сигналами в обучающей выборке помогают обнаружить вторжение в информационную сеть [8].

Фрактальный анализ помогает выявить в сетевом трафике самоподобные интервалы данных на отрезках времени различного масштаба, удовлетворяющие свойству самоподобия [9]. При этом установлено, что аномальный и нормальный трафики характеризуются разными значениями результирующего показателя фрактального анализа (показатель Херста). Это обстоятельство – очевидное преимущество данного метода анализа сетевого трафика, поскольку упрощает принятие решения о наличии вторжения при выявлении аномального трафика.

Кластерный анализ (КА) сетевого трафика помогает выявить в сетевом трафике такие характеристики, с помощью которых его можно будет разбить на отдельные, однозначно разделяемые группы, среди которых будут выделены группы нормального и аномального состояния [10]. Совпадение текущего состояния с одной из групп аномального состояния или несовпадение характеристик текущего состояния ни с одной из групп нормального состояния – сигнал об обнаружении вторжения. От классического метода классификации данный метод отличается тем, что классы не заданы заранее и формируются в ходе анализа.

Метод опорных векторов удобно применять, когда аномальные состояния сетевого трафика можно отделить от нормальных состояний линейной гиперплоскостью. Задача этого метода заключается в том, чтобы найти гиперплоскость, от которой ближайшие к ней объекты классов будут находиться максимально далеко, что необходимо для снижения или полного устранения ошибочной классификации.

$$a(x) = sign\left(\sum_{j=1}^{N} w_j x^j - b)\right), \quad j = \overline{1, N}, \tag{3}$$

где $x = \left(x^1, ..., x^N\right)$ – признаковое описание объекта; вектор $(w_1, ..., w_N) \in R^N$ и скалярный порог $b \in R$ являются параметрами метода.

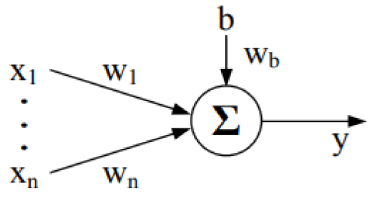

Рис. 1. Схема работы нейрона.

Применение метода значительно усложняется на практике, когда параметры не разделены линейной гиперплоскостью, поэтому исходные данные о сетевом трафике предварительно обрабатывают, – например, с помощью вейвлет-анализа [11].

Искусственная *нейронная сеть* представляет собой набор искусственных нейронов (рис. 1) и образует большую

группу методов анализа данных. Нейроны соединены между собой связями с заданным весом (синапсами), веса изменяются в ходе обучения нейронной сети. Основная характеристика нейрона – функция активации *f*, формирующая выходное значение *y* на основании суммы произведений входных сигналов *x* и соответствующих им весов:

$$y = f\left(\sum_{i=1}^{N} w_i x_i\right), \quad i = \overline{1, N}, \tag{4}$$

где $\left(x^1,...,x^N\right)$ – сигналы, поступающие на вход нейрона; $(w_1,...,w_N)$ – веса входных связей нейрона для соответствующих сигналов, устанавливаемых в ходе обучения; b – смещение с весом w_b.

Результатом обработки исходных данных является желаемый набор выходных значений с помощью подбора значений $(w_1,...,w_N)$. Нейронные сети могут состоять как из одного слоя нейронов (однослойные), так и из нескольких (многослойные). В многослойных нейронных сетях исходные данные поступают только на первый слой, а на все скрытые (внутренние) и выходной (последний) слои поступают результаты работы предыдущих слоев [12]. Возможно также применение нескольких нейронных сетей для дополнительной классификации видов сетевых атак, если первой сетью обнаружено вторжение [13]. Основной недостаток нейронных сетей – длительность обучения.

Метод анализа данных *дерево решений* (ДР) представляет собой структуру, состоящую из элементов трех видов: узлы – атрибуты, по значениям которых происходит переход к одному из ребер, исходящим от этого узла; ребра – элементы, соединяющие в структуре узлы; листья – метки для классификации данных, итоговые решения данного метода.

Классификация осуществляется последовательным рассмотрением соответствия данных атрибутам в узлах. Результат всегда соответствует только одному из ребер. В итоге данным присваивается класс одного из листьев [14].

Построение структуры дерева происходит итеративными алгоритмами.

Группа методов «байесовская сеть» в общем виде устанавливает вероятностные зависимости между данными, которые подвергаются анализу, при отклонении данных от установленных вероятностей можно идентифицировать аномалию сетевого трафика [15]. Частный случай этой модели – наивный байесовский классификатор, байесовский метод с предположениями об отсутствии смысловой зависимости входных переменных полностью основывается на статистической вероятности присутствия определенного типа данных a_i в обучающей выборке; в целом $P(c_i)$ за определенный интервал времени относит данные на этом интервале времени к классу c_i:

$$P(c_j) = \frac{N}{n_j}, \quad j = \overline{1, k}, \tag{5}$$

где N – число элементов a_i, принадлежащих классу c_i и входящих в выборку общим число всех элементов n_i; k – количество классифицируемых выборок.

Хотя данное предположение на практике не выполняется, на достаточно больших интервалах метод зарекомендовал себя как эффективный. В таком упрощении он очень близок к статистической группе методов.

Все методы, кроме методов статистической группы (СТГ), имитируют различные стороны человеческого мышления, поэтому далее будем называть их методами искусственного интеллекта (ИИ).

На данном этапе из всего многообразия необходимо проработать использование группы статистических методов как основы для дальнейшей их обработки методами искусственного интеллекта. Прямая обработка методами ИИ потока сетевого трафика потребует значительных объемов дополнительной памяти и длительного периода обучения методам ИИ.

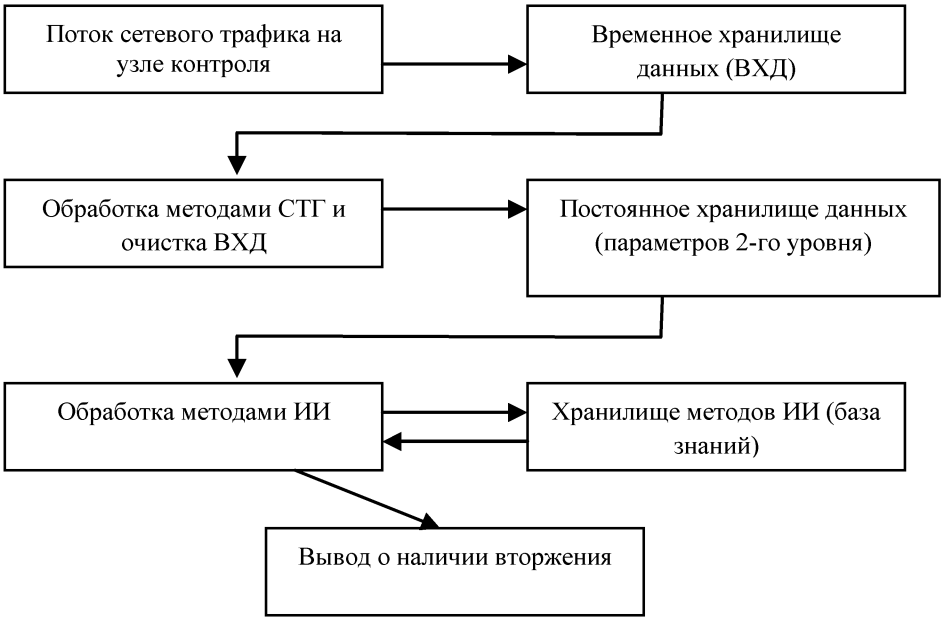

Рис. 2. Схема работы ГИС.

Методы СТГ наиболее приспособлены к обработке больших массивов данных, их применение на предварительном этапе исходного потока сетевого трафика снизит размеры необходимой памяти информационной системы, а также количество ошибочных выводов ГИС из-за большого количества шумов в исходных данных, за счет обработки меньшего объема данных методами ИИ повысит скорость работы ГИС в целом. При этом необходимо выбирать размеры периодов обобщения данных: слишком короткие будут давать все еще значительное количество шумов, а слишком длинные – сглаживать значимые сигналы (события), по которым заметно вторжение в информационную сеть; кроме того, увеличится время реакции на происходящее или подготавливаемое вторжение. Вероятнее всего, следует выбрать несколько размеров периодов обобщения и результаты обработки каждого из них методами СТГ хранить в памяти для обработки методами ИИ, а исходные данные после общения методами СТГ можно затирать вновь поступающими для сокращения необходимой памяти, в том числе для увеличения работы ГИС за счет уменьшения массивов данных, с которыми ей придется работать. Такие данные (результаты обработки методов СТГ) являются параметрами для методов ИИ в нашей ГИС – будем называть их «параметрами второго уровня» [16]. Далее параметры второго уровня обрабатываются методами ИИ и результаты обработки сохраняются в хранилище результатов обработки методов ИИ, которое будет также использоваться ИИ для самообучения (база знаний, содержащая информацию, являющуюся результатом решения предыдущих задач).

Заключение

Все перечисленные группы методов могут использоваться для создания систем обнаружения вторжений в ГИС. Однако, как уже было отмечено, статистические методы, как основа ГИС, должны быть использованы в первую очередь. Дальнейшие исследования будут связаны с тем, чтобы составить наиболее эффективную комбинацию из методов в рамках создаваемой математической модели ГИС, с возможностью обучения без учителя. Кроме того, в данную гибридную интеллектуальную систему необходимо встроить механизм внешнего указания ошибок со стороны администратора (эксперта), при этом ГИС должна (аналогично человеческому мышлению) внести в свои механизмы и методы принятия решений поправки, – например, в коэффициенты приоритета того или иного метода в зависимости от близости его к верному решению, выделив признаки, которые не были учтены в таких коэффициентах ранее. Такой подход можно отнести к обучению с учителем. При отсутствии ме-

тодов с выводами, близкими к верному решению, ГИС должна сообщить об отсутствии в ее арсенале методов подходящего направления и необходимости расширить арсенал методов или набор характеристик, на которые опираются методы при анализе состояния, либо, как в случае с нейронными сетями, увеличить количество нейронов или их слоев в нейронной сети. Таким образом, система получит общий механизм обучения.

---

1. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей. – М.: ФОРУМ; ИНФРА-М, 2008.

2. Крылов, В.В., Самохвалова, С.С. Теория телетрафика и ее приложения. – СПб.: БХВ-Петербург, 2005.

3. Шелухин, О.И., Филинова, А.С, Васина, А.В. Обнаружение аномальных вторжений в компьютерные сети статистическими методами // T-Comm: Телекоммуникации и транспорт. – 2015. – Т.9, №10. – С. 42-49.

4. Lu, W., Traore, I. Detecting New Forms of Network Intrusion Using Genetic Programming // Computational intelligence. – 2004. – Vol. C-20, № 3. – P. 475-494.

5. Jiang, H., Ruan, J. The Application of Genetic Neural Network in Network Intrusion Detection // Journal of computers. – 2009. – Vol. C-4, № 12. – P. 1223-1230.

6. Ireland, E. Intrusion Detection with Genetic Algorithms and Fuzzy Logic // UMM CSci senior seminar conference. – 2013. – P. 1-6.

7. De Castro, L.N., Von Zuben, F.J. Artificial Immune Systems: Part I – Basic Theory and Applications // Universidade Estadual de Campinas, Dezembro de, Technical Report. – 1999. – 95 p.

8. Амосов, О.С., Баена, С.Г. Вейвлет-алгоритмы оценивания нестационарных процессов с фрактальной структурой, имеющих неоднородности и нарушения // Информатика и системы управления. – 2017. – № 2 (52). – С. 85-99.

9. Громов, Ю.Ю., Земской, Н.А., Иванова, О.Г., Лагутин, А.В., Тютюнник, В.М. Фрактальный анализ и процессы в компьютерных сетях: учеб. пособие. – Изд. 2-е, стереотип. – Тамбов: Изд-во Тамб. гос. техн. ун-та, 2007. – 108 с.

10. Конин, А.В., Коробейников, А.В. Кластеризация статистических характеристик сетевого трафика для обнаружения аномалий. Информационные технологии в науке, промышленности и образовании // Сборник трудов региональной научно-технической очно-заочной конференции. – Ижевск: Изд-во Ижевского гос. техн. ун-та им. М.Т. Калашникова.

11. Zhang, R., Zhang, S., Muthuraman, S., Jiang, J. One Class Support Vector Machine for Anomaly Detection in the Communication Network Performance Data // 5th WSEAS Int. Conference on Applied Electromagnetics, Wireless and Optical Communications, Tenerife. – 14-16 Dec., 2007.

12. Abuadlla, Y., Kvascev, G., Gajin, S., Jovanović, Z. Flow-Based Anomaly Intrusion Detection System Using Two Neural Network Stages // Computer Science and Information Systems. – 2014. – № 11 (2). – P. 601-622.

13. Vrushali, D. M., Pawar, S.N. Anomaly based IDS using Backpropagation Neural Network // International Journal of Computer Applications. – 2016. – 136 (10).

14. Шампандар, А. Дж. Искусственный интеллект в компьютерных играх: как обучить виртуальные персонажи реагировать на внешние воздействия. – М.: Вильямс, 2007. – 768 с.

15. Барсегян, А.А., Куприянов, М.С., Холод, И.И., Тесс, М.Д., Елизаров, С.И. Анализ данных и процессов: учеб. пособие. – СПб.: БХВ-Петербург, 2009. – 512 с

16. Батурин, Д.С. Классификация параметров, используемых для прогнозирования временных рядов в гибридных интеллектуальных системах. – М.: научно-информ. изд. центр «Институт стратегических исследований», 2019. – С. 179-182.