Понимание этих аномалий и возможностей этих инструментов имеет решающее значение для разработки эффективных мер безопасности. Организациям и частным лицам крайне важно знать об этих рисках и использовать надежное шифрование, безопасные сетевые конфигурации и обучение пользователей, чтобы снизить угрозу MITM-атак, проводимых на уровне операционной системы.

Список использованных источников

1. Вахитова, Э. М. Моделирование сетевых атак в условиях учебной лаборатории / Э. М. Вахитова // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: Сборник материалов VI Всероссийской молодежной научно-практической конференции с международным участием, Уфа, 19–20 мая 2023 года. – Уфа: Уфимский университет науки и технологий, 2023. – С. 71-73. – EDN DCTJEB.

2. Казаков, М. Б. MITM-атаки и их предотвращение / М. Б. Казаков // Информационные технологии в деятельности органов внутренних дел : Сборник научных статей Всероссийской научно-практической конференции, Москва, 20 апреля 2023 года. – Москва: Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2023. – С. 32-33. – EDN HPQFWX.

3. Canteaut, A. Sieve-in-the-middle: Improved MITM attacks / A. Canteaut, M. Naya-Plasencia, B. Vayssière // Lecture Notes in Computer Science. – 2013. – Vol. 8042 LNCS, No. Part 1. – P. 222-240. – DOI 10.1007/978-3-642-40041-4_13. – EDN RHGBWB.

Вахитова Элина Маратовна, студент каф. управления информационной безопасностью, uber73lolu@gmail.com

Фатхелисламов Альфир Фирдависович, старший преподаватель каф. управления информационной безопасностью, Alfir93@mail.ru

УДК 004.056.53

ИССЛЕДОВАНИЕ МЕТОДА ОБНАРУЖЕНИЯ АНОМАЛИЙ В СЕТЕВОМ ТРАФИКЕ НА ОСНОВЕ ОПТИМАЛЬНОГО ФИЛЬТРА КОЛМОГОРОВА-ВИНЕРА

А.И. Плаван

Поволжский государственный университет телекоммуникаций и информатики, г. Самара

Ключевые слова: обнаружение аномалий, сетевой трафик, фильтр Колмогорова-Винера, среднеквадратическая ошибка фильтрации.

Злоумышленники зачастую используют сеть как транспорт для доставки вредоносных программ до целевой системы или для доступа к конфиденциальным данным на недостаточно защищенных сетевых ресурсах. Возникновение нового источника трафика приводит к изменению общего состояния и значений статистических характеристик сети.

Необычный трафик также может быть вызван ошибками в настройках сетевого оборудования. Такой трафик называется аномальным, или просто аномалией.

В работе [1] предлагается метод на основе среднеквадратической ошибки фильтрации применительно к последовательности интервалов между поступлениями пакетов. Индикатором аномалии служит отклонение значения СКО от эталонного значения, вычисленного для нормального трафика.

В работе [2] предложен метод, основанный на корреляции между значениями переменных MIB протокола SNMP. Для обнаружения аномалий используется нормализованная минимальная среднеквадратическая ошибка фильтра Колмогорова-Винера. Пороговые значения получаются из собственных значений корреляционной матрицы нормального трафика.

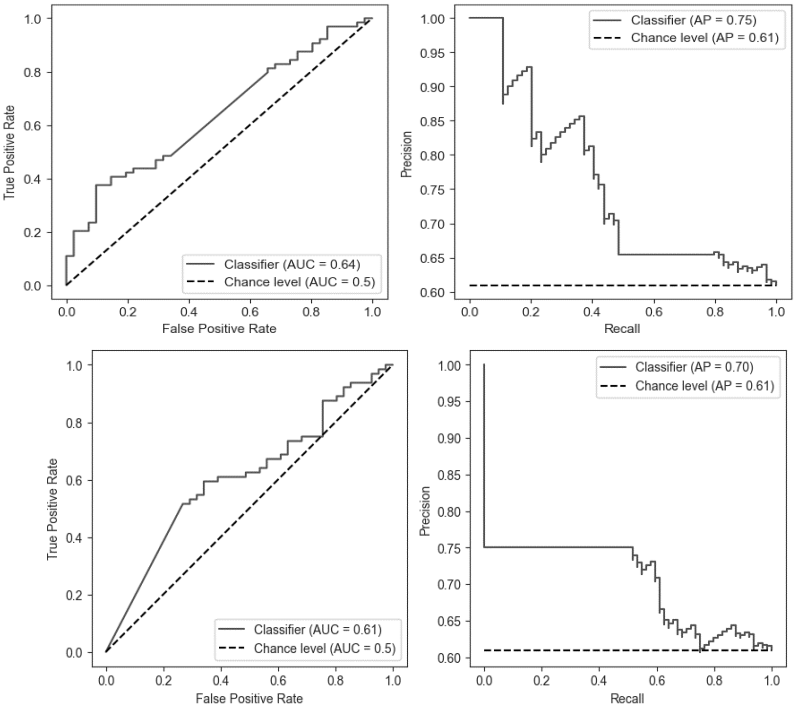
В данной работе предлагается метод обнаружения аномалий в сетевом трафике, позволяющий учитывать случайный «шум» наблюдений, вызванный изменениями параметров сети и другими факторами.

Фильтр Винера обеспечивает оптимальную (по критерию минимума среднеквадратической ошибки) фильтрацию стационарного сигнала из смеси с шумом. Сетевой трафик, представленный в виде интервалов между поступлениями пакетов, либо количества пакетов или байт в единицу времени, может быть описан как случайная последовательность. Во время периода обучения анализируется нормальный трафик, выявляются его характеристики, и на их основе синтезируется оптимальный линейный фильтр Винера. Для обнаружения аномалий этот фильтр применяется к текущему трафику, и, если отклонение ошибки фильтрации превышает некоторый порог, это считается признаком аномалии. При использовании нормализованной (относительно дисперсии нормального трафика) среднеквадратической ошибки [3], максимальное пороговое значение можно задать равным единице, а минимальное равным минимальному значению ошибки для фильтра. Изменяя пороговое значение между этими границами, возможно регулировать чувствительность и вероятность ложноположительных срабатываний.

Для проверки метода использовался набор записей сетевого трафика из архива MAWI WIDE за одну неделю. Трафик был разбит на минутные интервалы. 64 из 105 интервалов (60%) были признаны аномальными на основе на основе наличия аномалий в исходном датасете, что говорит о практически сбалансированном датасете. Обнаружение аномалий производилось путем синтеза фильтра для одного дня, условно признанного «нормальным» и применения фильтра к интервалам остальных дней.

На рисунке 1 представлены графики ROC-кривой и кривой Precision-Recall (точности-полноты) для одного дня, для трафика, представленного в

виде интервалов между поступлениями пакетов (сверху), и количества байт в единицу времени (снизу) построенные при изменении порогового значения.



Classifier – значения для предлагаемого метода, Chance level – значения для слепого угадывания, AUC – площадь под кривой, AP – средняя точность

Рисунок 1 – Графики ROC-кривой и кривой Precision-Recall

В зависимости от того трафик в какой день считался «нормальным», графики имеют различный вид, среднее значение AUC составляет 0,6. Полученное значение AUC недостаточно высоко для самостоятельного обнаружения аномалий данным методом. Однако значения среднеквадратической ошибки могут быть дополнительным признаком для улучшения эффективности других методов машинного обучения.

Список использованных источников

1. Карташевский В.Г. Фильтрация наблюдаемого трафика как способ обнаружения вторжений / В.Г. Карташевский, И.С. Поздняк // Вестник УрФО. – 2019. – Т. 19. – № 1 (31). – С. 17-22, DOI: https://doi.org/10.14529/secur190103

2. Al-Kasassbeh M. Network intrusion detection with wiener filter-based agent / M. Al-Kasassbeh // World Appl. Sci. J. – 2011. – Т. 13. – № 11. – С. 2372-2384.

3. Плаван А.И. Среднеквадратическая ошибка фильтрации как критерий обнаружения аномалий сетевого трафика / А.И. Плаван, В.Г. Карташевский // Вестник Российского нового университета. Серия: Сложные системы модели, анализ и управление. – 2023. – № 1. – С. 94-101, DOI: https://doi.org/10.18137/RNU.V9187.23.01.P.94

Плаван Алексей Игоревич, аспирант каф. информационной безопасности, aleksej-plavan@ya.ru

УДК 004.8, 004.93

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ПРЕДВАРИТЕЛЬНОЙ ОБРАБОТКИ РАЗНОРОДНОЙ ИНФОРМАЦИИ

А.К. Гришко, А.М. Мазанов, Е.А.Данилова, А.Умурзаков
Пензенский государственный университет, г. Пенза

Ключевые слова: интеллектуальная система, символьно-графическая информация.

Ввод разнородной документационной информации, представленной в виде учетно-статистических бланков, технологических карт, финансово-экономической информации и т.д., является до сих пор актуальной задачей. Текстовая или графическая часть обрабатываемой информации может быть нанесена различными способами, с различными видами шрифтов, цветом знака, документ может иметь различную контрастность и дефекты изображения [1,2].

Максимальную скорость и достоверность распознавания при оптимальных аппаратурных затратах можно получить при объединении способов аппаратурной и алгоритмической обработки. При этом устройство предварительной обработки, состоящее из считывающей, анализирующей и обрабатывающей частей должны адаптивно изменять свои характеристики в зависимости от характера и качества документа. Считывающая часть включает в себя рецептор с заданными спектральными свойствами и аналого-цифровой преобразователь. Анализирующая часть содержит блок повышения контрастности, блок коррекции, блок анализа и селекции по толщине и блок описания изображений. Обрабатывающая часть предполагает алгоритмическую обработку по идентификации изображений. Варьируя контрастными характеристиками изображения η и ξ анализирующими свойствами измерителя γ и мешающими параметрами E и, ν а также заданием $t_{\min}$ и $t_{\max}$ минимальной и максимальной толщины линий можно либо вручную, либо с ЭВМ управлять параметрами данных блоков. На выходе блока описания формируется кодовое описание знака, которое обрабатывается в ЭВМ по определенной иерархической системе.