Оценка эргодичности и робастности процесса функционирования сетевых устройств, имеющих множественную адресацию

А. А. Москвин, e-mail: tema.kg9012@gmail.com
М. С. Бадякин
С. С. Каверин

Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М. Штеменко

Аннотация. *Традиционно используемые в качестве протоколов транспортного уровня TCP/UDP имеют известные уязвимости и ограничения, которые снижают эффективность маскирования сети передачи данных. Данные ограничения снимаются при применении протокола транспортного уровня SCTP, способного создавать многоадресные сетевые соединения. В статье приведена оценка эргодичности и робастности моделируемого процесса функционирования сетевых устройств, имеющих множественную адресацию.*

Ключевые слова: *проактивная защита, сеть передачи данных, многоадресность, компьютерная атака, сетевые соединения, транспортные протоколы, сетевая разведка.*

Введение

На фоне внешнеполитической деятельность нашей страны специалистами в области информационной безопасности в 2022 году отмечено беспрецедентное увеличение количества компьютерных атак. Так, согласно исследованиям, продолжительность атак выросло с 12 минут (феврале - март 2021 года) до 30 часа в нынешний период. До 35% жертв этих атак - финансовые организации, еще 33% - органы власти.

При этом отмечено, что основу таких атак составили нападения активистов, выражающих свой социальный протест посредством организации кибератак, а в качестве средств координации для выбора цели атаки, методов и сроков нападения они обычно используют обычные мессенджеры. Например, для совершения DDOS-атак, злоумышленнику необходимо всего лишь скачать инструкцию

с telegram-канала, внести необходимые сведения (IP-адрес, порт взаимодействия, URL), и начать атаку.

Таким образом, несмотря на применяемые средства защиты информации, не исключена реализация следующих угроз безопасности информации:

– угроза использования слабостей протоколов сетевого/локального обмена данными;

– угроза приведения системы в состояние «отказ в обслуживании».

В качестве мер, направленных на снижения реализации вышеуказанных угрозы, нормативно-правовыми актами в области информационной безопасности, предусмотрено:

– управление сетевыми соединениями;

– перевод информационной системы в безопасное состояние.

Реализация указанных мер возможна за счет выполнения мероприятий по маскированию сети передачи данных (далее – СПД) [1-11], выраженных в снижении информативности информационных направлений, имитации (навязывании) ложной информации о структуре СПД, динамическом изменении структурно-функциональных характеристик СПД.

Однако эффективная реализация указанных мер ограничивается тем, что традиционно используемые в качестве протоколов передачи данных TCP/UDP имеют известные уязвимости [12], которые зачастую использует злоумышленник для осуществления компьютерных атак, а перевод СПД в безопасное состояние и вовсе приводит к разрыву сетевых соединений.

Данные ограничения снимаются при применении протокола транспортного уровня SCTP, функциональные возможности которого рассмотрены в статье [13].

Оценка эргодичности и робастности

Моделируемый процесс функционирования сетевых устройств, имеющих множественную адресацию (далее - процесс функционирования системы S), может быть представлен в виде размеченного графа его состояний (Рис. 1), где переход из состояния в состояние (описание состояний представлено в таблице) осуществляется при появлении соответствующих служебных пакетов с интенсивностью λ.

Моделируемый процесс функционирования системы S рассматривается как марковский случайный процесс с соблюдением свойств простейшего потока событий.

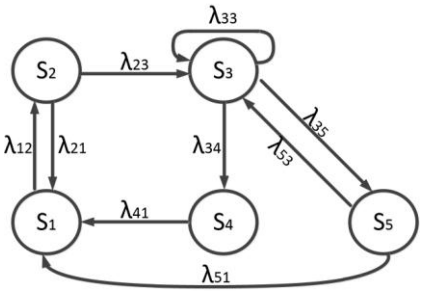

Рис. 1. Граф состояний системы S

Таблица

Дискретные состояния сетевых устройств

Состояния	Описание состояния
S1	ожидание получения служебного пакета INIT
S2	ожидание получения служебного пакета DATA
S3	ожидание получения служебного пакета HEARTBEAT/SHUTDOWN
S4	ожидание получения служебного пакета SHUTDOWN COMPLETE
S5	ожидание получения служебного пакета HEARTBEAT ACK

Марковский случайный процесс с конечным числом состояний имеет стационарный режим, если он обладает эргодическим свойством. Случайный процесс обладает эргодическим свойством, если:

граф состояний не должен иметь ни одного состояния без входных и выходных потоков событий;

все потоки событий, переводящие систему из состояния в состояние, должны быть простейшими (с постоянными интенсивностями).

Оценить эргодичность процесса возможно аналитически. Для этого необходимо, чтобы собственные значения матрицы A1 интенсивности появления служебных пакетов принимали отрицательные значения.

Для того, чтобы найти собственные значения матрицы A1, необходимо, найти определитель матрицы:

$$\left|A_1 - xE\right| = \begin{vmatrix} a_{11} - x & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} - x & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} - x \end{vmatrix} = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \qquad (1)$$

Таким образом, собственные значения матрицы A1 являются корнями характеристического уравнения (1).

Результат расчетов собственных значений матрицы интенсивности A1 при варьируемых значениях λ12 и λ35 представлен на Рис. 2.

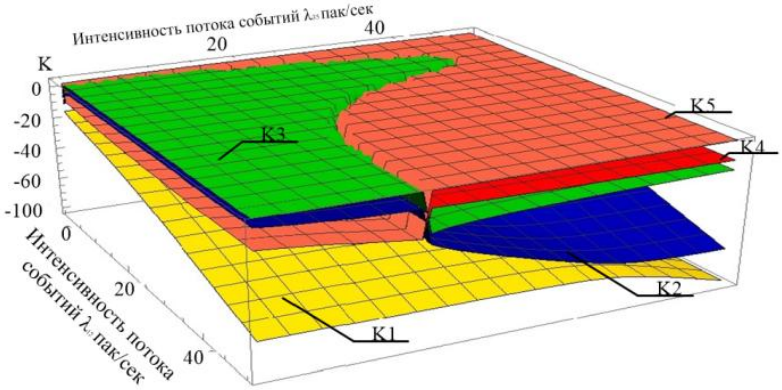

Рис. 2. Собственные значения матрицы интенсивности A_1

Робасность определяет устойчивость выходных параметров к погрешности исходных данных и выражается через число обусловленностей матрицы интенсивности A1:

$$cond(A_1) = \left\|A_1\right\| \bullet \left\|A_1^{-1}\right\| \qquad (2)$$

где $\left\|A_1\right\|$ - Евклидова норма матрицы интенсивности A_1, которая вычисляется по формуле:

$$\left\|A_1\right\| = \sqrt{\sum_{i=1}^{n}\sum_{j=1}^{n}(a_{ij})^2} \qquad (3)$$

Интерпретация интервалов значений числа обусловленности:
$1 \le cond(A_1) \le 100$ – модель робастная (устойчивая);
$100 \le cond(A_1) \le 1000$ – модель слабо робастная (слабоустойчивая);
$cond(A_1) \ge 1000$ – модель неробастная (неустойчивая) система.

Результат расчета числа обусловленности при варьируемых значениях λ_{12} и λ_{35} представлен на Рис. 3.

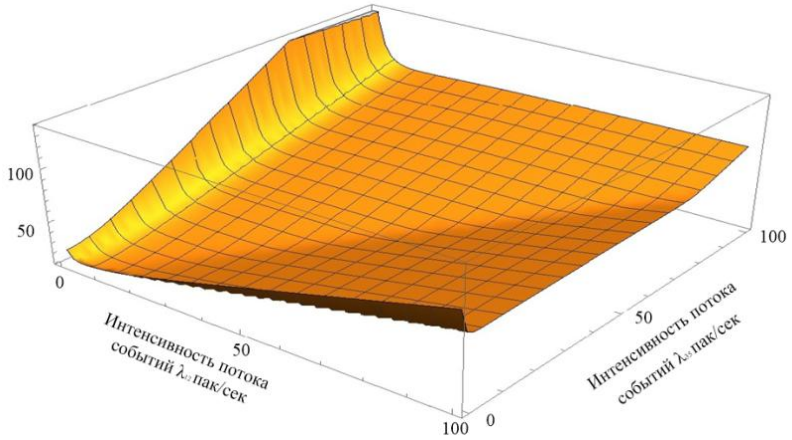

Рис. 3. Число обусловленности

Заключение

Оценка робастности процесса функционирования системы S позволяет сделать выводы об адекватности модели, разрабатываемой для исследования процесса функционирования сетевых устройств, имеющих множественную адресацию.

Оценка эргодичности позволяет сделать выводы о наличии стационарного режима для процесса функционирования сетевых устройств, имеющих множественную адресацию, что, в свою очередь, дает возможность найти вероятностно-временные характеристики исследуемого процесса.

Список литературы

1. Maximov, R. V. Model of client-server information system functioning in the conditions of network reconnaissance / R. V. Maximov, S. P. Sokolovsky, A. P. Telenga // CEUR Workshop Proceedings. – 2020. – № 2603. – С. 44-51.

2. Maximov, R. V. Methodology for substantiating the characteristics of false network traffic to simulate information systems / R. V. Maximov, S. P. Sokolovsky, A. P. Telenga // Selected Papers of the XI Anniversary International Scientific and Technical Conference on Secure Information Technologies. – Moscow, 2021. – С. 115-124.

3. Maximov, R. V. Honeypots network traffic parameters modeling / R. V. Maximov, S. P. Sokolovsky, A. P. Telenga // Selected Papers of the XI Anniversary International Scientific and Technical Conference on Secure Information Technologies. – Moscow, 2021. – С. 229-239.

4. Максимов, Р. В. Модель и методика маскирования адресации корреспондентов в киберпространстве / Р. В. Максимов, В. В. Кучуров, Р. С. Шерстобитов // Вопросы кибербезопасности. – 2020. – № 6 (40). – С. 2-13.

5. Максимов, Р. В. Алгоритм и технические решения динамического конфигурирования клиент-серверных вычислительных сетей / Р. В. Максимов, С. П. Соколовский, И. С. Ворончихин // Информатика и автоматизация. – 2020. – № 5. – С. 1018-1049.

6. Маскирование структуры распределенных информационных систем в киберпространстве / И. С. Ворончихин, [и др.] // Вопросы кибербезопасности. – 2019. – № 6 (34). – С. 92-101.

7. Максимов, Р. В. Модель и алгоритм функционирования клиент-серверной информационной системы в условиях сетевой разведки / Р. В. Максимов, Д. Н. Орехов, С. П. Соколовский // Системы управления, связи и безопасности. – 2019. – № 4. – С. 50-99.

8. Шерстобитов, Р. С. Маскирование интегрированных сетей связи ведомственного назначения / Р. С. Шерстобитов, С. Р. Шарифуллин, Р. В. Максимов // Системы управления, связи и безопасности. – 2018. – № 4. – С. 136-175.

9. Пат. 2716220 Российская Федерация, МПК H 04 L, G 06 F. Способ защиты вычислительных сетей / Максимов Р. В., Соколовский С. П., Ворончихин И. С., заявитель и патентообладатель Краснодарское высшее военное училище. – № 2019123718; заявл. 22.07.2019; опубл. 06.03.2020, Бюл. № 7. – 12 с.

10. Пат. 2726900 Российская Федерация, МПК H 04 L, G 06 F. Способ защиты вычислительных сетей / Максимов Р. В., Соколовский С. П., Ворончихин И. С. [и др.] , заявитель и патентообладатель Краснодарское высшее военное училище. – № 2019140769; заявл. 09.12.2019; опубл. 16.07.2020, Бюл. № 20. – 45 с.

11. Пат. 2739151 Российская Федерация, МПК H 04 L, G 06 F. Способ маскирования структуры сети связи / Максимов Р. В., Починок В. В., Теленьга А. П. [и др.] , заявитель и патентообладатель Краснодарское высшее военное училище. – № 2020112143; заявл. 24.03.2020; опубл. 24.12.2020, Бюл. № 22. – 30 с.

12. Бекенева, Я. А. Анализ актуальных типов DDoS-атак и методов защиты от них/ Я. А. Бекенева // Информатика и компьютерные технологии. – 2016 г. – № 1. – С. 7-13.

13. Москвин, А.А. Технологии управления информационными потоками в сетях передачи данных / А.А.Москвин // Информатика: проблемы, методы, технологии: сборник материалов XXII Международной научно-методической конференции. – Воронеж: ВГУ. – 2022. – С. 803-810.