УДК 681.3

МОДЕЛИРОВАНИЕ АТАК НА БЕСПРОВОДНЫЕ СЕТИ WIFI

А.С. Заворыкин, Н.Н Корнеева, Н.Н. Толстых, В.Г. Юрасов, В.И. Белоножкин

Проводится построение обобщённой модели атаки на беспроводную сеть WiFi с рассмотрением всех основных этапов на основе математического аппарата сетей Петри-Маркова

Ключевые слова: атака, беспроводная сеть, модель

Смоделируем атаку с помощью сети Петри-Маркова [1-3]. Обозначим элементы сети. Здесь s_i – позиции, t_j – переходы:

s_1 - целевая беспроводная сеть работает;

s_2 - злоумышленник подготовил оборудование, приблизился на достаточное расстояние к сети и настроил оборудование для изучения сети (перевёл радиоинтерфейс в режим прослушивания (monitoring) и т.д.);

t_1 - тщательный осмотр места развёртывания сети, определение её границ и уровня сигнала вдоль периметра;

s_3 - данные о сети получены;

t_2 - анализ данных о сети, планирование методики проведения атаки;

s_4 - данные проанализированы, первичный план атаки составлен;

t_3 - сбор, подготовка и конфигурирование оборудования и программного обеспечения непосредственно для выполнения запланированных действий по атаке;

s_5 - оборудование и программное обеспечение для атаки подготовлены;

t_4 - прослушивание сети и анализ трафика;

s_6 - на основе анализа трафика и поведения устройств в сети получена информация о мерах защиты сети, подготовлен способ обхода защиты (к примеру, подготовлено программное обеспечение для взлома пароля протокола аутентификации);

s_7 - определение дополнительных местоположений для проведения атак;

t_5 - преодоление обнаруженных мер противодействия;

s_8 - доступ к сети получен;

t_6 - подключение к беспроводной сети и анализ её структуры, а также структуры возможного проводного сегмента;

s_9 - получена информация о структуре беспроводной сети;

s_{10} - получена информация о структуре проводного сегмента сети;

t_7 - сбор и анализ трафика от хостов сети и оценка безопасности протоколов, используемых как в беспроводной сети, так и в проводном сегменте;

s_{11} - путём анализа трафика получена информация о настройках защиты сети, что позволяет выбрать цель для атаки (тип протокола или системы защиты, общающиеся посредством него хосты или использующие её);

t_8 - выбор предоставляющих интерес хостов и проведение против них активных атак;

s_{12} - против выбранных хостов успешно проведена атака;

t_9 - выход в Интернет или другую сеть через обнаруженные шлюзы и проверка возможности передачи файлов с компьютера взломщика или на него;

s_{13} - доступ к требуемой сети получен, связь с компьютером злоумышленника установлена, готовность к передаче данных.

Заворыкин Алексей Сергеевич – ВГТУ, студент, e-mail:sidewalker@bk.ru
Корнеева Наталья Николаевна – ВГТУ, студент, e-mail: mnac@comch.ru
Толстых Николай Николай – ВГТУ, д-р техн. наук, профессор, e-mail: mnac@comch.ru
Юрасов Владислав Георгиевич – ВГТУ, д-р техн. наук, профессор, email: mnac@comch.ru
Белоножкин Владимир Иванович – ВГТУ, д-р техн. наук, e-mail: mnac@comch.ru

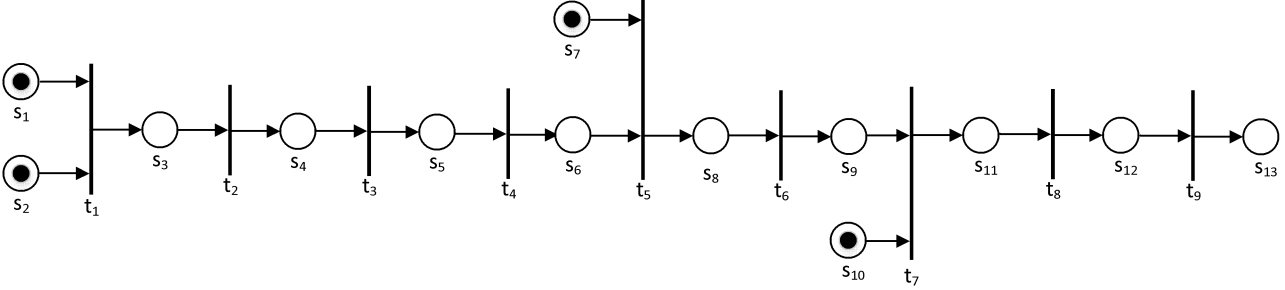

Рис. 1. Вид сети Петри-Маркова, характерной для атаки на беспроводную сеть

Для данной сети Петри-Маркова имеет место следующая система интегро-дифференциальных уравнений [1-5]:

$$\Phi_{S_1t_1}(t) = \pi_{11}\int_0^t f_{S_1t_1}(\tau)d\tau, \quad (1)$$

$$\Phi_{S_2t_1}(t) = \pi_{21}\int_0^t f_{S_2t_1}(\tau)d\tau, \quad (2)$$

$$\Phi_1(t) = \int_0^t f_{S_1t_1}(\tau)\,\Phi_{S_2t_1}(t) + f_{S_2t_1}(\tau)\Phi_{S_1t_1}(t)d\tau, \quad (3)$$

$$\Phi_{S_3t_2}(t) = \pi_{32}\int_0^t f_{S_3t_2}(\tau)\Phi_1(t-\tau)d\tau, \quad (4)$$

$$\Phi_{S_4t_3}(t) = \pi_{43}\int_0^t f_{S_4t_3}(\tau)\Phi_{S_3t_2}(t-\tau)d\tau, \quad (5)$$

$$\Phi_{S_5t_4}(t) = \pi_{54}\int_0^t f_{S_5t_4}(\tau)\Phi_{S_4t_3}(t-\tau)d\tau, \quad (6)$$

$$\Phi_{S_6t_5}(t) = \pi_{65}\int_0^t f_{S_6t_5}(\tau)\Phi_{S_5t_4}(t-\tau)d\tau, \quad (7)$$

$$\Phi_{S_7t_5}(t) = \pi_{75}\int_0^t f_{S_7t_5}(\tau)d\tau, \quad (8)$$

$$\Phi_2(t) = \int_0^t f_{S_7t_5}(\tau)\,\Phi_{S_6t_5}(t) + f_{S_6t_5}(\tau)\Phi_{S_7t_5}(t), \quad (9)$$

$$\Phi_{S_8t_6}(t) = \pi_{86}\int_0^t f_{S_8t_6}(\tau)\Phi_2(t-\tau)d\tau, \quad (10)$$

$$\Phi_{S_9t_7}(t) = \pi_{97}\int_0^t f_{S_9t_7}(\tau)\Phi_{S_8t_6}(t-\tau)d\tau, \quad (11)$$

$$\Phi_{S_{10}t_7}(t) = \pi_{107}\int_0^t f_{S_{10}t_7}(\tau)d\tau, \quad (12)$$

$$\Phi_3(t) = \int_0^t f_{S_{10}t_7}(\tau)\,\Phi_{S_9t_7}(t) + f_{S_9t_7}(\tau)\Phi_{S_{10}t_7}(t), \quad (13)$$

$$\Phi_{S_{11}t_8}(t) = \pi_{118}\int_0^t f_{S_{11}t_8}(\tau)\Phi_3(t-\tau)d\tau, \quad (14)$$

$$\Phi_{S_{12}t_9}(t) = \pi_{129}\int_0^t f_{S_{12}t_9}(\tau)\Phi_{S_{11}t_8}(t-\tau)d\tau, \quad (15)$$

где $f_{sitj}(t)$ — плотность вероятности времени перемещения из состояния s_i к переходу t_j, $\Phi_{sitj}(t)$ — соответствующий закон распределения, π_{ij} — вероятность срабатывания перехода, причем вероятности срабатывания всех переходов на данной траектории не зависят от времени, вероятность перемещения по всей сети рассчитывается по формуле

$$\pi_{\text{рез}} = \prod_{d_{ij}} \pi_{ij}, \quad (16)$$

d_{ij} — все полушаги сети.

Полагаем, что плотности распределения вероятностей являются экспоненциальными зависимостями и имеют вид:

$$f_{S_it_j} = \alpha_{ij}e^{-\alpha_{ij}t}$$

где $\alpha_{ij} = 1/\tau_{ij}$, τ_{ij} (i = 1,…,4; j = 1,…,2) – средние времена вышеперечисленных действий соответственно.Рассмотрим свойства потока этапов атаки:

- переходы от одного этапа к другому происходит с постоянной интенсивностью, т.е. поток стационарен;
- события смены этапов независимы друг от друга. Т.е. причины обусловившие переход от одного этапа к другому именно в тот, а не в другой момент, как правило, не связаны с аналогичными причинами для других переходов между этапами. Т.е. поток без последействия;
-этапы меняются подряд, по одному, а не парами, тройками и т.д, так как в один момент времени злоумышленник выполняет только одно действие (действие одного этапа). Т.е. поток смены этапов является ординарным.

Таким образом, даже если брать по отдельности атаки, часть этапов которых могут быть произведены несколькими методами, т.е. идут ординарные потоки этапов атаки и даже если они имеют последействие, то при их сложении получится поток в котором последействие ослабевает. Результирующий поток этапов атаки также будет ординарным и без последействия, то есть, относиться к типу пуассоновского.

Применяя пуассоновское приближение, получаем среднее время τ перемещения по сети Петри-Маркова из начальной позиции до конечного перехода и вероятность этого перемещения:

$$\tau_1 = \frac{\tau_{11}^2+\tau_{11}\tau_{21}+\tau_{21}^2}{\tau_{11}+\tau_{21}}, \quad (17)$$

$$\tau_2 = \tau_1 + \tau_{32}, \quad (18)$$

$$\tau_3 = \tau_2 + \tau_{43}, \quad (19)$$

$$\tau_4 = \tau_3 + \tau_{54} + \tau_{65}, \quad (20)$$

$$\tau_5 = \frac{\tau_4^2+\tau_4\tau_{75}+\tau_{75}^2}{\tau_4+\tau_{75}}, \quad (21)$$

$$\tau_6 = \tau_5 + \tau_{86} + \tau_{97}, \quad (22)$$

$$\tau_7 = \frac{\tau_6^2+\tau_6\tau_{107}+\tau_{107}^2}{\tau_6+\tau_{107}}, \quad (23)$$

$$\tau_8 = \tau_7 + \tau_{118}, \tau_9 = \tau_8 + \tau_{129}, \quad (24)$$

$$\tau = \frac{\tau_{11}^2+\tau_{11}\tau_{21}+\tau_{21}^2}{\tau_{11}+\tau_{21}} + \sum_{i=2}^{9}\tau_i, \quad (25)$$

$$P(t) = 1 - e^{-\frac{1}{\tau}t}, \quad (26)$$

где исходные параметры атаки принимают следующие значения:

τ_{21} = 120 мин - среднее время, необходимое для тщательного осмотра места развёртывания сети, определения её границ и уровня сигнала по периметру; $\tau_{11} = \tau_{21}$; анализ полученных данных о сети и планирование методики атаки занимают около τ_{32} = 30 мин; τ_{43} = 15 мин - среднее время настройки оборудования и ПО для выполнения выбранной атаки на систему защиты беспроводной сети; τ_{54} = 30 мин - среднее время, необходимое для сбора достаточного количества трафика и его анализа; τ_{65} = 20 мин - среднее время получения информации о мерах защиты сети и подготовки способа обхода защиты; τ_{75} = 60 мин - среднее время для определения дополнительных местоположений для проведения атак и выбора оптимального из них; τ_{86} = 30 мин - среднее время, необходимое для подключения к беспроводной сети и анализа её структуры и структуры возможного проводного сегмента; для обработки информации о настройках защиты сети и выбора цели для атаки требуется в среднем τ_{97} = 20 мин для беспроводной сети и τ_{107} = 10 мин для проводной сети; τ_{118} = 20 мин - среднее время проведения атаки против представляющих интерес хостов; τ_{129} = 5 мин - среднее время для выхода в сеть интернет или другую сеть через найденные шлюзы и проверки возможности передачи файлов. Тогда среднее время перехода по всей сети τ = 362 мин.

Зависимость вероятности реализации атаки на беспроводную сеть от времени приобретает вид, представленный на рис. 2.

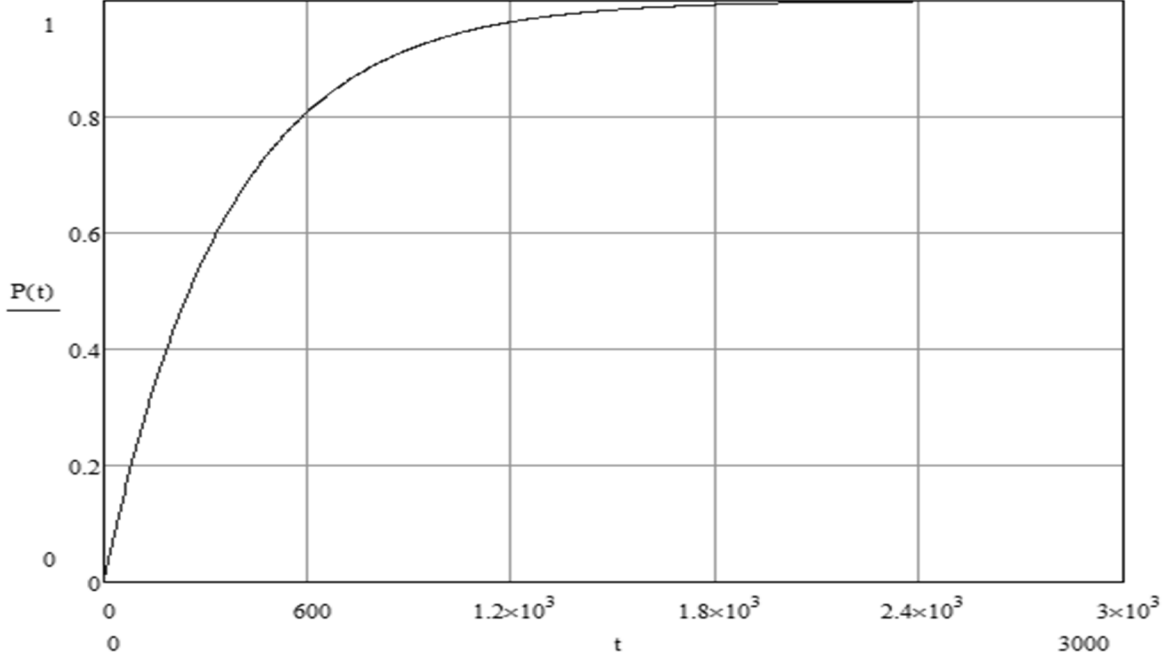

Рис. 2. Зависимость вероятности реализации атаки на беспроводную сеть от времени

Литература

1. Щербаков В.Б., Ермаков С.А. Безопасность беспроводный сетей: стандарт IEEE 802.11. М: РадиоСофт, 2010. -255 с.

2. Владимиров А.А. Wi-фу: «боевые» приемы взлома и защиты беспроводных сетей. - М.: НТ-Пресс, 2005. -463 с.

3. Радько Н.М., Скобелев И.О. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. // М.: РадиоСофт, 2010. -230 с.

4. Игнатьев В.М., Ларкин Е.В. Сети Петри-Маркова. — Тула: Тульский государственный университет, 1997. -163 с.

5. Вентцель Е.С. Исследование операций. Задачи, принципы, методология: Учебное пособие для вузов. 3-е изд., стереотип. — М.: Дрофа, 2004. –208 с.

Воронежский государственный технический университет
Voronezh state technical university

SIMULATING ATTACKS ON WIRELESS WIFI NETWORKS

A.S. Zavorykin, N.N. Korneeva, N.N. Tolstih, V.G. Yurasov, V.I. Belonoghkin

Constructed a generalized model of the attack on the wireless WiFi network with the consideration of all the main stages on the basis of mathematical Petri-Markov nets

Key words: attack, wireless network, model