УДК 681.3

ОБ АНАЛИЗЕ ЭФФЕКТИВНОСТИ ИДЕНТИФИКАЦИИ АТАК НА БЕСПРОВОДНЫЕ СЕНСОРНЫЕ СЕТИ

© 2022 Я. Е. Львович, Ю. П. Преображенский, Е. Ружицкий

Воронежский государственный технический университет (Воронеж, Россия)
Воронежский институт высоких технологий (Воронеж, Россия)
Панъевропейский университет (Братислава, Словакия)

В статье обсуждаются некоторые вопросы, связанные с характеристиками атак в беспроводных сенсорных сетях. Дан перечень таких характеристик. Был сформирован новый список критериев, по которым можно оценивать, насколько эффективно проводится идентификация угроз на беспроводные сенсорные сети. Приведены показатели, обуславливающие эффективность идентификации угроз.

Ключевые слова: беспроводная сеть, управление, автоматизация, информационная безопасность.

Чтобы оценить, насколько эффективной является система определения атак (СОА), применяют большое количество самых разных характеристик. Как правило, ими являются:

1) архитектурный вид системы обнаружения вторжений (может быть единым или модульным);
2) место расположения;
3) протоколы поддержки сети и ОС;
4) список доступных информационных источников (наличие возможности получить информацию о происходящих событиях);
5) список доступных действий ответа на угрозы (наличие возможности совершать определенные действия при возникновении атак);
6) наличие возможности осуществлять управление удаленным способом;
7) обеспечение устойчивости к отказам связи, при взаимодействии агентов системы обнаружения вторжений и основного модуля [1];
8) наличие оперативности, а также качества устанавливаемых обновлений;
9) способность добавить сигнатуры пользователей. В том случае, когда необходимо доработать СОА под определенную систему, отличающуюся от стандартной системы. Наличие такой способности позволяет более тонко настроить СОА;
10) удобность функционирования и проведения настроек;
11) большая производительность;
12) цена.

Поскольку в нашей работе не ведется разработка полноценной системы обнаружения вторжений, только лишь ее компоненты, которые способны осуществлять сетевой мониторинг, часть представленных параметров не будет подходить для того, чтобы произвести оценку. В связи с этим, мы сформировали новый список критериев, по которым будем оценивать, насколько эффективно проводится идентификация угроз на беспроводные сенсорные сети (БСС). Проведя анализ работ, в данный список вошли такие показатели как:

1) число угроз, которые были идентифицируемы;
2) число признаков, которые нужны для того, чтобы провести идентификацию;
3) наличие точности, аккуратного исполнения и полноты идентификации [2];
4) топологическая схема БСС;
5) оказание влияния на БСС (проведение активного или же пассивного ее мониторинга);
6) уровень сложности алгоритмов, применяемых при анализе;
7) способность осуществить расширение;
8) применение актуального информационного набора.

Львович Яков Евсеевич – Воронежский государственный технический университет, профессор, e-mail: office@vivt.ru.
Преображенский Юрий Петрович – Воронежский институт высоких технологий, профессор, e-mail: petrovich@vivt.ru.
Ружицкий Евгений – Панъевропейский университет, канд. техн. наук, доцент, e-mail: rush_evg_br53@yandex.ru.

Но применять такое большое число показателей не имеет смысла, в связи с чем, мы решили применить только четыре из них:

1) число угроз, которые были идентифицируемы;

2) число признаков, которые нужны для того, чтобы провести идентификацию;

3) уровень точности идентификации;

4) уровень полноты идентификации.

Кроме того, было произведено присвоение данным показателям весовых коэффициентов, значение которых зависит от того насколько часто они появляются в представленных исследованиях. Все это показано в таблице.

Таблица

Показатели, обуславливающие эффективность идентификации угроз

Показатели	Вес показателей в процентах
Число угроз, которые были идентифицируемы	15
Число признаков, которые нужны для того, чтобы провести идентификацию	25
Уровень точности идентификации	30
Уровень полноты идентификации	30

Соответственно, эффективность идентификации мы можем выразить при помощи выражения:

$$Q = q_1 * 0{,}15 + q_2 * 0{,}25 + q_3 * 0{,}3 + q_4 * * 0{,}3, \quad (1)$$

при общем весе представленных показателей в сто процентов.

Резюмируя вышесказанное, стоит признать наличие необходимости создания методического и научного аппарата, позволяющего идентифицировать угрозы на беспроводные сенсорные сети [3] на сетевом уровне. Чтобы это реализовать, нами предложено применение поведенческого анализа, который основывается на осуществлении мониторинга сетевого поведения. В этом исследовании поведение сети определяется в виде совокупности ее признаков в какое-либо время. Основным компонентом данной задачи, будет являться идентификация угроз (атак). Под идентификацией понимается сопоставление того, как сеть ведет себя на данный момент времени и тем поведением, которое было известно ранее. Задачей идентификации является проведение классификации [4]. В стандартном понимании классификация представляется следующим образом. Есть определенное множество различных объектов – $X = \{x_1, \dots, x_n\}$, с его подмножествами, где существуют объекты исследования X_c.. То есть те, которые принимаются к рассмотрению при решении задачи. Кроме того существуют классы $Y = \{C_0, \dots, C_m\}$, и любой из них является набором объектов, представляющий собой подмножество O_s,, которые соединены между собой: $\forall Ci \in Y(Ci \subset X\text{c})$.

Произведем ввод дополнительного отображения $\lambda : C \to \{0, \dots, m\}$, при помощи которого каждый класс получает свой номер (еще его называют меткой): $\forall Ci \in Y\lambda(Ci) == i, i = 0, m$.

Примем, что любой из объектов *x,* будет соответствовать одному классу. То есть будет существовать определенная зависимость, которая нам неизвестна – $y^*: X_c \to \lambda(Y)$. И поэтому, X_c будет выступать в качестве дизъюнктивного соединения множеств, которые соединяют разные классы $Ci(i = 0, \dots, m): X\text{c} = \bigvee_{i=0}^{m} C_i$. При ситуации, когда будет необходимо осуществить мульти – классификацию, при которой один объект относится к нескольким классам, ее проводят используя дополнительные признаки, дающие возможность четко исполнить целевую зависимость y^*. Любой из объектов $x \in X_c$ имеет свой набор признаков $x = (x_1, \dots ., x_k)$ – т. е. является их вектором. В этом случае, чтобы решить задачу классификации, нужно создание алгоритма, который будет относиться ко всем алгоритмам A, - $a: X_c \to \{1, \dots, m\}$, максимизирующий соотношение тех объектов, которые были правильно классифицированы, к суммарному числу объектов $x \in X_c$:

$$\Omega(a, X_c) = \frac{1}{\#X_c} * \#\{x | (\exists C_i \in C, x \in C_i) \wedge a(x) = \lambda(x)\}_{x \in X_c} \to \max_{a \in A}. \quad (2)$$

Задачу, которую мы поставили в нашем исследовании можно решить, используя следующий алгоритм. Существует определенное количество классов, которые определяют поведение БСС *C*: обычное, поведение при наличии атаки. K – является множеством признаков, которые определяют поведение, а также поведения, которые изучаются – X_c. Осуществим выделение из K несколько признаков, являющихся самыми информативными: $K_I \subseteq K$. Любое из поведений имеет свой вектор признаков, у которого размерность составляет $k = \#K_I$.. Примем что X_{cKI} – являются объектами исследования, которые представляет вектор признаков $k \in K_I$. Применив определенное правило *R,* создадим выборку обучения, в которую входят векторы поведения с маркировкой

$$\Xi_{X_c^L} = \{(x'_i, \bar{c}_i)\}_{i=0}^{M} = \bigcup_{C_i \in C} \bigcup_{x \in C_i \cap X_c^L} (x, \lambda\,(\mathrm{C})).$$

Здесь $X_c^L \subseteq X_c$ – является множеством векторов обучения, а$x'_i \in C_{i_{\bar{c}_i}}$ – является отношением принадлежности.

В этом случае, для того чтобы решить задачу, обозначенную выше, используя выборку обучения $\Xi_{X_c^L}$, необходимо осуществить решение задачи оптимизации. Произведем ввод еще одного множества $G = K_{I_1}, \dots, K_{I_k}$, с условием, что $K_{I_i} \subseteq K_I, \#K_{I_1} = i$, вместе с дополнительной функцией, играющей вспомогательную роль $\psi: G \to \{X_{c_{K_{I_1}}}, \dots, X_{c_{K_{I_k}}}\}$. Здесь $X_{c_{K_{I_i}}}$ являются объектами исследования $x \in X_c$, которые представляются при помощи вектора, имеющего длину *i*. Нужно, имея установленный уровень эффективности σ, минимизировать число применяемых признаков $k \in K_I$:

$$\Lambda(a, X_c, \sigma) = \min_{i \in \{1,\dots,k\}} \left\{ \#K_{I_i} \middle| K_{I_i} \in G, \Omega\left(a, \psi(Ki)\right) \geq \sigma \right\}. \quad (3)$$

Здесь – $\Lambda(a, X_c, \sigma)$ является функцией определяющей оценку наименьшего количества признаков поведения сети; σ – является изначально установленным положительным числом.

Выводы. В работе проведено исследование возможностей идентификации атак в беспроводных сетях. Показаны особенности решаемой задачи классификации.

СПИСОК ИСТОЧНИКОВ

1. Щукин А. А. Проведение численных экспериментов для оценки характеристик обнаружения на математической модели радиолокационной станции / А. А. Щукин, А. Е. Павлов // Моделирование, оптимизация и информационные технологии. – 2022. – Т. 10. – № 1 (36).

2. Мишуков С. В. Особенности имитационного моделирования измерительных схем емкостных датчиков / С. В. Мишуков // Моделирование, оптимизация и информационные технологии. – 2022. – Т. 10. – № 1 (36).

3. Львович И. Я. Исследование модели спутникового канала связи / И. Я. Львович, А. П. Преображенский, О. Н. Чопоров // Системы управления и информационные технологии. – 2018. – № 3 (73). – С. 17-21.

4. Preobrazhenskiy A. P. Radar characteristic prediction for objects having radio-absorbing coatings over a wavelength range / A. P. Preobrazhenskiy // Telecommunications and Radio Engineering. – 2004. – Т. 62. – № 6. – С. 569-576.

ANALYSIS OF THE EFFICIENCY OF ATTACK IDENTIFICATION ON WIRELESS SENSOR NETWORKS

© 2022 Ya. E. Lvovich, Yu. P. Preobrazhensky, E. Ruzhitsky

Voronezh State Technical University (Voronezh, Russia)
Voronezh Institute of High Technologies (Voronezh, Russia)
Pan-European University (Bratislava, Slovakia)

The paper discusses some issues related to the characteristics of attacks in wireless sensor networks. A list of such characteristics is given. A new list of criteria has been formed by which it is possible to evaluate how effectively the identification of threats to wireless sensor networks is carried out. The indicators that determine the effectiveness of threat identification are given.

Keywords: wireless network, control, automation, information security.