Елена С. Басан, Александр С. Басан, Олег Б. Макаревич
*Южный федеральный университет «ЮФУ»,
Институт компьютерных технологий и информационной безопасности,
ул. Чехова, 2, г. Таганрог, 347922, Россия*
e-mail: ebasan@sfedu.ru, <http://orcid.org/0000-0001-6127-4484>
e-mail: asbasan@sfedu.ru, <http://orcid.org/0000-0002-2973-2737>
e-mail: obmakarevich@sfedu.ru, <http://orcid.org/0000-0003-0066-8564>

РАЗРАБОТКА И РЕАЛИЗАЦИЯ МЕТОДА ОБНАРУЖЕНИЯ АНОМАЛЬНОГО
ПОВЕДЕНИЯ УЗЛОВ В ГРУППЕ РОБОТОВ*

DOI: <http://dx.doi.org/10.26583/bit.2018.4.07>

Аннотация. Данная статья посвящена вопросам обеспечения безопасности в группе мобильных роботов при реализации злоумышленником атак, направленных на свойство доступности информации. Проанализированы основные методы и подходы к обнаружению атак и аномалий для мобильных роботов, выделены основные достоинства и недостатки существующих подходов. Основной целью является разработка метода обнаружения аномального поведения, который позволил бы избежать создания эталонного распределения, либо базы сигнатур, либо правил для группы мобильных роботов. Метод должен в текущих условиях при динамически изменяющейся структуре сети выявлять аномалии. В статье представлен метод обнаружения аномального поведения узла сети на основе анализа параметров: остаточной энергии и сетевой загруженности узлов сети. Проводится анализ поведения отдельных роботов группы относительно отклонения от общего поведения с использованием вероятностных методов. Разрабатываемый метод обнаружения аномального поведения основан на использовании вероятностной оценки событий. Определяются три типа состояний узлов сети, построен граф переходов узла в каждое из состояний, а также определены параметры, влияющие на данные переходы. Разработанный метод демонстрирует высокий показатель обнаружения атаки «отказ в обслуживании» распределенной атаки «отказ в обслуживании» при количестве злоумышленных узлов, не превышающем или незначительно превышающем количество доверенных узлов. А также обеспечивает обнаружение атаки Сивиллы. Проведено экспериментальное исследование, включающее в себя разработку модели, имитирующей группу мобильных роботов, в частности сетевое взаимодействие между роботами. Разработаны, реализованы сценарии атак для группы мобильных роботов, позволяющие оценить эффективность разработанного метода обнаружения аномального поведения. Для определения эффективности разработанного метода использовались показатели: время обнаружения атакующих узлов; количество узлов злоумышленника, которое позволяет обнаружить разработанный метод.

Ключевые слова: *мобильные роботы, аномальное поведение, вероятностные методы, групповое управление, атака, обнаружение.*

Для цитирования: БАСАН, Елена С.; БАСАН, Александр С.; МАКАРЕВИЧ, Олег Б. РАЗРАБОТКА И РЕАЛИЗАЦИЯ МЕТОДА ОБНАРУЖЕНИЯ АНОМАЛЬНОГО ПОВЕДЕНИЯ УЗЛОВ В ГРУППЕ РОБОТОВ. *Безопасность информационных технологий*, [S.l.], v. 25, n. 4, p. 75-85, 2018. ISSN 2074-7136. Доступно на: <<https://bit.mephi.ru/index.php/bit/article/view/1163>>. Дата доступа: 07 nov. 2018. doi:<http://dx.doi.org/10.26583/bit.2018.4.07>.

***Благодарности.** Работа выполнена при финансовой поддержке Министерства образования и науки Российской Федерации (Инициативные научные проекты № 2.6244.2017/8.9).

Elena S. Basan, Alexander S. Basan, Oleg B. Makarevich
*Southern Federal University "SFedU", Institute of Computer Technologies and Information Security,
str. Chekhov, 2, Taganrog, 347922, Russia*
e-mail: ebasan@sfedu.ru, <http://orcid.org/0000-0001-6127-4484>
e-mail: asbasan@sfedu.ru, <http://orcid.org/0000-0002-2973-2737>
e-mail: obmakarevich@sfedu.ru, <http://orcid.org/0000-0003-0066-8564>

**Development and implementation of a method to detect an abnormal behavior
of nodes in a group of robots***

DOI: <http://dx.doi.org/10.26583/bit.2018.4.07>

Abstract. The present paper examines the issues of security in a group of mobile robots in the implementation of malicious attacks aimed at the availability of information. The main methods and approaches for detecting attacks and mobile robots anomalies were analyzed. The major advantages and disadvantages of existing approaches were identified. The aim is to develop an attack detection method that allows avoiding a creation of either a reference distribution, or a signature database, or rules for a group of mobile robots. The method should detect anomalies within the current conditions with a dynamically changing network structure. The paper presents a method for detecting abnormal behavior of a network node based on analysis of parameters: the residual energy and network load. The behavior of individual robots of the group is analyzed with respect to the deviation from the general behavior using probabilistic methods, which avoids creating a reference distribution for describing the behavior of the node, as well as the creating of a signature database for detecting anomalies. The developed method of detecting abnormal behavior based on the probabilistic evaluation of events. Three types of a network node state were defined, a graph of node transitions to each state was constructed, and parameters that affect these transitions were determined. The developed method demonstrates a high detection rate of denial of service attacks and distributed denial of service attacks when the number of malicious nodes is not greater than or slightly greater than the amount trusted nodes. It also provides detection of the Sybil attack. An experimental study was carried out. It includes the development of a model to simulate a group of mobile robots, in particular a robot network. Scenarios of attacks were developed, implemented for a group of mobile robots. It allows evaluating the effectiveness of this method of anomalous behavior detection. To determine the effectiveness of the developed method, the following indicators were used: time of detection of attackers and the number of nodes of the attacker that can be detected.

Keywords: mobile robots, abnormal behavior, probabilistic methods, group control, attack, detection.

For citation: BASAN, Elena S.; BASAN, Alexander S.; MAKAREVICH, Oleg B. Development and implementation of a method to detect an abnormal behavior of nodes in a group of robots. IT Security (Russia), [S.l.], v. 25, n. 4, p. 75-85, 2018. ISSN 2074-7136. Available at: <<https://bit.mephi.ru/index.php/bit/article/view/1163>>. Date accessed: 07 nov. 2018. doi:<http://dx.doi.org/10.26583/bit.2018.4.07>.

****Acknowledgement.*** The work was supported by the Ministry of Education and Science of the Russian Federation (Initiative Science Projects No. 2.6244.2017 / 8.9).

Введение

Сети мобильных роботов являются достаточно уязвимыми к атакам злоумышленника. В статье [1] была представлена модель угроз для сети мобильных роботов. Также авторами был проведен анализ атак для группы мобильных роботов. На основании проведенного анализа было выявлено, что основной набор атак, которые злоумышленник может реализовать для группы мобильных роботов, представляет собой: «отказ в обслуживании» (DoS) [2], распределенная атака «отказ в обслуживании» (DDoS) [3], человек посередине (MITM) и атака Сивиллы, а также исчерпание ресурсов [4]. Обнаружение этих атак с минимальной затратой ресурсов мобильных роботов является основной задачей данного исследования [5].

Обнаружение аномального поведения для группы мобильных роботов возможно при контроле и анализе изменения параметров узла сети. При активной атаке злоумышленник может влиять на какой-либо физический параметр мобильного робота путем сетевого или физического воздействия [6]. Данное исследование ограничено спектром атак, которые направлены на свойство доступности информации или узла сети.

Рассмотрим некоторые работы авторов, посвященные проблеме обнаружения аномального поведения для одиночных мобильных роботов или групп роботов с централизованным управлением.

В статье [7] авторами рассмотрена система обнаружения атак на основе дерева принятия решений, с использованием алгоритма C5.0 для группы роботизированных автомобилей. Достоинством представленного подхода является то, что для обнаружения

кибератак авторы наряду с четырьмя признаками для анализа процесса коммуникации и обработки информации, которые называют киберфункциями ввода, используют четыре параметра для анализа физических свойств робота, которые авторы называют физическими характеристиками входного сигнала. Далее авторы проводят 5 типов деструктивного воздействия на робота и получают набор правил для построения дерева принятия решений. Недостатком подхода является то, что в данной работе рассмотрены атаки только на одного робота, а не на сеть роботов. Кроме того, в подобных системах имеется необходимость постоянного добавления правил для обнаружения новых атак.

В работе авторов [8] рассмотрена система обнаружения вторжений на основе сигнатурного анализа. Авторами проведен ряд экспериментов для создания эталонного шаблона, описывающего нормальное поведение робота при отсутствии внешнего воздействия, а также случайных аномалий поведения. Затем был промоделирован ряд ситуаций, при которых имело место аномальное поведение, вызванное условиями окружающей среды. На основании собранных данных строился шаблон нормального поведения робота с учетом весовых коэффициентов, рассчитанных на основании частоты возникновения того или иного типа аномального поведения. Авторами проведен ряд атак, которые влияют на определённый набор физических параметров узла. Данный подход демонстрирует большую эффективность при обнаружении злоумышленного узла, чем простой сигнатурный анализ, тем не менее имеются некоторые недостатки: например, необходимость постоянного обновления и пополнения базы данных сигнатур для контроля данных с неучтённых датчиков мобильного робота.

В статье [9] рассматривается система обнаружения атак на беспилотные летательные аппараты. При разработке данной системы использовался подход на основе создания базы данных сигнатур. Система работает следующим образом. Каждый узел сети имеет узел-монитор, которым может являться соседний беспилотный аппарат, фиксирующий поведение доверенного узла и записывающий его в матрицу. Узел-монитор постоянно наблюдает за поведением подопечного узла и выставляет ему оценки. Данные оценки зависят от того насколько поведение подопечного узла отклоняется от нормального шаблона поведения. Затем создается база данных правил и оценивается поведение узла. При этом оценка производится по 7 параметрам. К недостатку системы можно отнести необходимость постоянного контроля узлов друг за другом и анализа их поведения, что задействует вычислительную нагрузку и пропускную способность сети.

Таким образом, в результате рассмотрения работ, посвященных тематике обнаружения атак на мобильных роботов, можно выделить три основных недостатка существующих подходов:

1. Большинство систем основано на сигнатурном анализе либо на системе правил. В связи с этим имеются следующие ограничения: сложность обнаружения новых атак, не связанных с фиксируемыми шаблонами поведения злоумышленника, а также необходимость поддержания в актуальном состоянии базы правил или наборов сигнатур.
2. Системы, основанные на полностью распределенных методах обнаружения, требуют от узлов дополнительных затрат энергии, затрат вычислительной мощности и увеличивают пропускную способность.
3. При использовании централизованных методов узлов, выполняющий основные функции по обнаружению аномального поведения является наиболее уязвимым местом системы. При выведении его из строя нарушается работа сети полностью [10].

В данной статье предлагается разработка метода обнаружения аномального поведения злоумышленника или нескольких злоумышленников в рамках группы мобильных роботов на основе вероятностных методов [11]. При этом основное отличие данного метода состоит в том, что он не требует построения эталонного вероятностного распределения, как другие вероятностные методы. Отсутствие необходимости построения эталонного распределения обусловлено тем, что для выявления аномального поведения берутся текущие показания узлов группы, далее строится функция нормального распределения и вычисляется доверительный интервал значений. Таким образом,

появляется возможность оценивать вероятность отклонения поведения узла от общего поведения узлов группы.

Разработка и реализация метода обнаружения аномального поведения

В данной работе предлагается метод, разработанный для группы мобильных роботов. Особенность разработки метода для группы мобильных роботов заключается в том, что для формирования функции нормального распределения необходимо получение данных от нескольких узлов, выполняющих схожие функции. Для более точного определения степени отклонения текущих показаний узла от группы узлов необходимо, чтобы показатели группы узлов находились в одном диапазоне. В таблице 1 представлены параметры, по изменению которых можно судить о наличии аномальной активности в сети.

Таблица 1. Соотношение параметров сети и влияющих на них атак

Параметры сети	Атака злоумышленника
Пакеты с данными	Блокировка узла, блокировка узла с наличием условий, переадресация, отказ в обслуживании, задержка пакетов
Заряд батареи	Отказ в обслуживании, истощение ресурсов
Загруженность	Отказ в обслуживании, истощение ресурсов, атака Сивиллы, Flood-атаки, туннелирование

Под параметром «пакеты с данными» понимается факт передачи или перенаправления пакета, то есть оценивается доступность передаваемой информации. Если на сеть оказывается какое-либо воздействие со стороны злоумышленника, то могут возникать ситуации, когда пакеты отбрасываются, дублируются и т.п.

Под параметром «заряд батареи» может пониматься следующее: текущее потребление заряда аккумулятора (или потребляемая мощность), а также оставшийся в аккумуляторной батарее запас энергии, позволяющий устройству функционировать в сети.

Под параметром «загруженность» понимается общее количество пакетов, передаваемых в сети. Либо количество пакетов, передаваемых через один из узлов сети.

В случае реализации злоумышленником атаки «отказ в обслуживании» изменяется уровень трафика, передаваемый злоумышленным узлом сети, и уровень трафика, принимаемый жертвами атаки. Следовательно, целесообразным является оценивание изменений показателя «загруженность», который представляет собой общее количество принимаемых, отправляемых, перенаправляемых пакетов узла сети. При реализации атаки Сивиллы или атаки перенаправления влияния на себя, основной целью злоумышленника является изменение процессов и путей обмена данными в сети. Другими словами, злоумышленник добивается такой ситуации, что весь или большая часть трафика соседних узлов проходит через него.

В предыдущей работе авторов [12] помимо параметров «загруженность» и «остаточная энергия» рассматривался параметр «количество отброшенных пакетов» (P1). В данном исследовании он рассматриваться не будет, так как существенно не влияет на обнаружение перечисленных выше атак. Таким образом, рассмотрим два параметра: загруженность (P2) и остаточная энергия (P3). Изменение данных параметров влияет на состояние как узлов сети так и всей группы роботов в целом. Состояние узлов сети можно описать следующим образом: S1 – состояние, когда узел не подвержен атаке и сам не проводит атаку, т.е. является подлинным на текущий момент времени; S2 – состояние, когда поведение мобильного робота отклонилось от поведения большей части группы роботов, может наблюдаться при условии, что узел стал жертвой атаки, т.е. узел является неопределенным; S3 – когда поведение мобильного робота значительно отличается от узлов группы, т.е. вероятнее всего узел является злоумышленным. На рис. 1 представлен

граф переходов из одного состояния в другое, а также отражено влияние параметров и атрибутов друг на друга.

Рис. 1. Граф состояний узлов группы мобильных роботов, используемый при выявлении аномального поведения

(Fig. 1. The graph states of nodes a group of mobile robots, used for detecting anomalous behavior)

На параметр $P2 = L$ оказывают влияние следующие атрибуты узла: A_{21} – общее количество отправленных узлом пакетов, содержащих данные. A_{22} – общее количество пакетов управления, или beacon - пакетов, предназначенных для проверки соединения. A_{23} – общее количество пакетов, отправленных по протоколу маршрутизации. A_{24} – общее количество принятых пакетов данными. A_{25} – общее количество принятых управляющих пакетов. A_{26} – общее количество принятых пакетов маршрутизации. A_{27} – общее количество отброшенных пакетов с данными. A_{28} – общее количество отброшенных управляющих пакетов. A_{29} – общее количество отброшенных пакетов маршрутизации.

Таким образом, параметр L может быть представлен следующим выражением:

$$L = A_{21} + A_{22} + A_{23} + A_{24} + A_{25} + A_{26} + A_{27} + A_{28} + A_{29} \quad (1)$$

Параметр $P3=e$ можно характеризовать конечным множеством атрибутов A_{3j} . Представленные ниже атрибуты влияют на количество остаточной энергии узла, но кроме описанных ниже атрибутов на количество остаточной энергии влияет уровень загруженности узла, т.е. параметр $P2$: A_{31} – начальный запас энергии узла сети. $A_{31} = initialEnergy$; A_{32} – мощность передаваемого сигнала. $A_{32} = rxPower$; A_{33} – мощность приема сигнала, $A_{33} = txPower$; A_{34} – скорость перемещения узла. $A_{34} = speed$.

Остаточная энергия вычисляется путем уменьшения уровня начальной энергии A_{31} для каждого переданного и каждого полученного пакета в единицу времени:

$$e_{tx} = A_{31} - (A_{33} * txTime), e_{rx} = A_{31} - (A_{32} * rcvTime), \quad (2)$$

где e_{tx} и e_{rx} – уровень остаточной энергии после приема пакета и после передачи первого пакета; $rcvTime$ – время передачи пакета; $txTime$ – время приема пакета.

Процедура вычисления доверия работает по следующему алгоритму.

1. Расчет доверительных интервалов загруженности узлов, загруженности на временном интервале и энергии [13].

1.1. Вычисление дисперсии и среднеквадратического отклонения:

$$D_{Li} = \left(\sum_i^N (L_i - \bar{L})^2 \right) / n, \quad D_{ei} = \left(\sum_i^N (e_i - \bar{e})^2 \right) / n, \quad (3)$$

где D_{Li} , D_{ei} – дисперсия параметров L и e группы узлов в текущий интервал времени. Вычисление среднеквадратического отклонения:

$$\sigma_{ei} = \sqrt{D_{ei}}, \sigma_{Li} = \sqrt{D_{Li}}, \quad (4)$$

σ_{ei}, σ_{Li} - среднеквадратическое отклонение параметров L и e группы узлов в текущий интервал времени.

1.2. Вычисление верхних и нижних границ доверительных интервалов.

Верхняя граница доверительного интервала параметра e всегда равна максимально допустимому значению энергии, то есть $a_{max} = initialEnergy$. Это связано с тем, что узлы могут мигрировать из одной группы в другую, могут появляться новые узлы со значением остаточной энергии, равной начальному значению.

Вычисление нижней границы доверительного интервала производится только для значения остаточной энергии. Так как нижняя граница показателя L узла равна минимально необходимому количеству пакетов, прошедших через узел за один интервал времени L_{min} . Данные меры приняты по той причине, что мобильный робот может проявлять эгоистичное поведение, то есть отказаться принимать участие в работе сети для сбережения энергии, что может искусственно «занизить» границы интервала.

Далее представлены формулы для вычисления границ доверительного интервала.

$$a_{min} = \bar{e} - t \cdot \sigma_e / \sqrt{n}, a_{max} = A_{31}, a_{max} = A_{31}, a_{min} < a_{max}, \quad (5)$$

$$b_{min} = L_{min}, b_{min} = L_{min}, b_{max} = \bar{L} + t \cdot \sigma_L / \sqrt{n}, \quad (6)$$

где $t^* \sigma / \sqrt{n}$ - точность оценки; t - аргумент функции Лапласа, где $\Phi(t) = \frac{\alpha}{2}$ - функция Лапласа; α - заданная надежность, в данном исследовании значение коэффициента $\alpha = 0.98$, значит аргумент $t = 2.34$; n - общее количество узлов.

2. Выполнение подпунктов 2.1, 2.2 для каждого узла.

2.1. Определение вероятности аномального поведения мобильного робота на основе рассчитанных границ доверительных интервалов. Для того чтобы вычислить значение среднеквадратического отклонения и математического ожидания необходимо сократить интервал, для которого вычисляется значение, и учитывать только показатели узла в предыдущий временной интервал L_{i-1} , e_{i-1} и L_i , e_i показатели узла для текущего интервала.

$$P_e(a_{min} < e_i < a_{max}) = \Phi\left(\frac{a_{max} - \bar{e}_e}{\sigma_{e_e}}\right) - \Phi\left(\frac{a_{min} - \bar{e}_e}{\sigma_{e_e}}\right), \quad (7)$$

$$P_L(b_{min} < L_i < b_{max}) = \Phi\left(\frac{b_{max} - \bar{L}_e}{\sigma_{L_e}}\right) - \Phi\left(\frac{b_{min} - \bar{L}_e}{\sigma_{L_e}}\right), \quad (8)$$

где Φ - функция Лапласа; $P_{Q(E)}$, P_L - вероятность попадания остаточной энергии узла и уровня загруженности узла в пределы доверительного интервала.

$\bar{e}_e = (e_{i-1} + e_i) / 2$; $\bar{L}_e = (L_{i-1} + L_i) / 2$ - математическое ожидание величин e и L для выборочного интервала. $D_{e_e} = \left(\sum_i^N (e_i - \bar{e}_e)^2 \right) / n$ - дисперсия для выборочного интервала для e ;

$D_{L_e} = \left(\sum_i^N (L_i - \bar{L}_e)^2 \right) / n$ - дисперсия для выборочного интервала для значения загруженности узла; $\sigma_{e_e} = \sqrt{D_{e_e}}$ - среднеквадратическое отклонение для выборочного интервала для остаточной энергии. $\sigma_{L_e} = \sqrt{D_{L_e}}$ - среднеквадратическое отклонение для выборочного интервала L .

2.2. Вывод результатов в журнал трассировки.

3. Выполнение подпункта 3.1 для каждого узла.

3.1. Обновление следующих значений для каждого узла: загруженность на предыдущем временном интервале, остаточная энергия в предыдущий момент времени.

4. Блокирование злоумышленных узлов.

4.1. Примем пороговое значение вероятности того, что узел является аномальным, равное 0,5.

4.2. Когда узел достигает значение, равное 0,5 необходимо уменьшить уровень его остаточной энергии в два раза, тогда узел считается в неопределенном состоянии.

4.3. Далее если значение уровня доверия достигает уровня 0,4, то необходимо считать узел злоумышленным и уменьшить его уровень энергии до нуля, таким образом, узел исключается из работы сети [14].

Проведение экспериментального исследования, оценка эффективности разработанного метода

Для проведения экспериментального исследования была разработана модель группы роботов в среде моделирования NS-2.35. На рис. 2 изображена группа мобильных роботов в системе моделирования, включающая в себя 10 узлов. Из них один узел N4 является базовой станцией или центральным сервером. Узел N0 является лидером группы и выполняет функции сбора информации от роботов группы и перенаправляет ее центральному серверу. Узлы группы обмениваются информацией друг с другом и с лидером группы [15]. При этом узлы N6, N7, N8, N9, начиная с 50-й секунды работы сети, будут проводить DDoS атаку.

Рис. 2. Группа роботов в системе моделирования NS-2.35
(Fig. 2. Group of robots in the simulation system NS-2.35)

Реализация и обнаружение DoS атаки

Проводя атаку «отказ в обслуживании», злоумышленник создает такую ситуацию, когда узел сети становится недоступным для других узлов и не может отвечать на их запросы и работать в штатном режиме. Было проведено моделирование трех типов ситуаций. В первом случае проведена оценка расходуемой энергии узлами сети при отсутствии атаки. На рис. 3 данная ситуация представлена графиком синего цвета, помеченным ромбами.

Рис. 3. Изменение уровня остаточной энергии в зависимости от интенсивности трафика узлов сети.

(Fig. 3. The residual energy level changes depending on the intensity of traffic nodes)

Во втором случае на сеть проводилась атака, при этом интенсивность трафика злоумышленного узла $I_t \leq I_m \leq 2I_t$, где I_m – трафик злоумышленного узла, I_t – трафик подлинного узла, т.е. низкоинтенсивная атака. Третий график представляет собой ситуацию, когда атака проводится интенсивно и $I_m > 2I_t$. Из рис. 3 видно, что во время проведения низкоинтенсивной атаки уровень энергии узлов останется практически таким же, как и для случая, когда атака не проводится. То есть в данном случае атаку можно считать не эффективной, т.к. она существенным образом не влияет на истощение ресурсов узла. На графике, отражающем изменение уровня энергии во время проведения интенсивной атаки, видно резкое падение уровня энергии, что подтверждает эффективность атаки. В случае, когда атака является интенсивной, разработанный метод позволяет обнаружить злоумышленника через 10 секунд.

Реализация и обнаружение DDoS атаки

Обнаружение распределенной атаки «отказ в обслуживании» является более сложной задачей [16]. Это связано с тем, что когда количество злоумышленных узлов преобладает над количеством подлинных узлов, границы доверительного интервала значительно расширяются. Когда количество злоумышленных узлов составляет 45 %, метод позволяет сразу обнаружить все злоумышленные узлы и заблокировать их уже на втором интервале времени, т.е. через 20 секунд от начала проведения атаки. На рис. 4 (а) представлена гистограмма, демонстрирующая уровень попадания текущих показателей e и L злоумышленных узлов в доверительный интервал. На рис. 4 (б) представлена гистограмма, демонстрирующая уровень обнаружения злоумышленных узлов, когда количество злоумышленных узлов составляет 50 %. Узлы N_9 и N_8 выявлены на втором интервале, узлы N_5 и N_6 обнаружены на третьем интервале и узел N_7 на четвертом интервале времени начиная с того момента, когда началась атака. При этом в первом случае необходимо 30 секунд для обнаружения злоумышленника, а во втором 40 секунд. Когда количество злоумышленных узлов составляет 60 %, то злоумышленные узлы полностью обнаруживаются через 60 секунд.

Рис. 4. Уровень обнаружения узлов при распределенной атаке «отказ в обслуживании» для (а) 40 % злоумышленных узлов (б) для 50 % злоумышленных узлов и пяти подлинных узлов сети
 (Fig. 4. Nodes detection level for distributed denial of service attack for (a) 40 % malicious nodes (b) for 50 % malicious nodes and five authentic network nodes)

Реализация и обнаружение атаки Сивиллы

Атака Сивиллы заключается в том, что злоумышленник представляется несколькими узлами (сущностями) в сети и пытается перенаправить большую часть трафика на себя [17]. В работах авторов [18], как правило, встречаются методы с применением жесткой защиты: парольной защиты, криптографической защиты, а также сигнатурного анализа и группового обнаружения. Данные методы применяются в сетях MANET, IoF, P2P [19]. Разработанный метод обнаружения аномального поведения показывает эффективность обнаружения атаки Сивиллы даже при условии, что злоумышленник перенаправил трафик на себя и больше не предпринимает никаких действий [20]. В данном случае обнаружение возможно за счет изменения уровня загруженности узлов, которые проводят атаку на соседние узлы. Метод позволяет выявить 100 % злоумышленных узлов, когда их количество в сети составляет 45 %. При этом для обнаружения всех узлов злоумышленника необходимо 60 секунд.

Заключение

Вопросы, связанные с обеспечением безопасности мобильных роботов, достаточно актуальны в связи с широким распространением самих робототехнических систем. Разработанный метод позволяет выявлять аномальное поведение в группе узлов, когда имеется возможность проводить анализ поведения большинства узлов и выявлять единичные или массовые отклонения от общего поведения. Имеется возможность наращивания количества анализируемых параметров для расширения спектра атак. Метод позволяет обнаруживать все злоумышленные узлы в пределах 30 – 60 секунд. Ограничения метода заключаются в количестве злоумышленных узлов, которые проводят атаку на сеть, их количество не должно превышать 60 % по сравнению с количеством доверенных.

В отличие от существующих методов обнаружения аномального поведения, где приходится составлять базы данных сигнатур или банки данных правил, хранить их, а затем обновлять, разработанный метод позволяет выявлять аномалии в текущий момент времени и в зависимости от текущей ситуации. Данное достоинство является достаточно важным, так как мобильные роботы могут быть использованы в разных средах и для выполнения различных задач, при этом помимо протоколов сетевого взаимодействия между мобильными роботами могут меняться и условия среды. Данный метод учитывает пороговые значения, то есть допустимый уровень аномалий, что уменьшает количество ложных срабатываний.

СПИСОК ЛИТЕРАТУРЫ:

1. Басан А.С., Басан Е.С. Модель угроз для систем группового управления мобильными роботами // Системный синтез и прикладная синергетика. Сборник научных трудов VIII Всероссийской научной конференции. Ростов-на-Дону: Южный федеральный университет. 2017. С. 205 – 212. URL: <https://elibrary.ru/item.asp?id=29989970>
2. H.S. Kim, S.W. Lee. Enhanced novel access control protocol over wireless sensor networks // IEEE Transactions on Consumer Electronics. 2009. № 55 (2). pp. 492 - 498. DOI: 10.1109/TCE.2009.5174412
3. Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак // Информационная безопасность. Труды СПИИРАН. 2016. № 2(45). С. 207 – 244. URL: <http://proceedings.spiras.nw.ru/ojs/index.php/sp/article/view/3267/1883>
4. Petrovsky O. Attack on the drones // Proceedings of Virus bulletin conference. 2015. pp. 16 – 24. URL: <https://www.virusbulletin.com/uploads/pdf/conference/vb2015/Petrovsky-VB2015.pdf>
5. Garber L. Robot OS: A New Day for Robot Design // Computer. № 46 (12). 2013. pp. 16 – 20. DOI: 10.1109/MC.2013.434
6. Кожемякин И.В., Путинцев И.А., Семенов Н.Н., Чемоданов М.Н. Разработка подводного робототехнического комплекса, с использованием открытых средств моделирования движения, дополненных моделью гидроакустического взаимодействия // Известия ЮФУ. Технические науки. Раздел II. Морская робототехника. 2016. № 1 (174). С. 88 – 99. URL: <http://izv-tn.tti.sfedu.ru/wp-content/uploads/2016/1/7.pdf>
7. Vuong T. P., Loukas G., Gan D., Bezemskij A. Decision tree-based detection of denial of service and command injection attacks on robotic vehicles // Proceedings of 2015 IEEE International Workshop on Information Forensics and Security (WIFS). 2015. pp. 1 - 6. DOI: 10.1109/WIFS.2015.7368559.
8. Bezemskij A., Loukas G., Richard J. Gan D. Behavior-based anomaly detection of cyber-physical attacks on a robotic vehicle // Proceedings of 15th International Conference on Ubiquitous Computing and Communications and 2016. 8th International Symposium on Cyberspace and Security. 2016. pp. 61 - 68. DOI: 10.1109/IUCC-CSS.2016.017.
9. Mitchell R., Chen I.R. Adaptive Intrusion Detection of Malicious Unmanned Air Vehicles Using Behavior Rule Specifications // IEEE Transactions on Systems, Man, and Cybernetics: Systems. №44 (5). 2014. pp. 593 - 599. DOI: 10.1109/TSMC.2013.2265083.
10. Monshizadeh M., Khatri V., Kantola R., Yan Z. An Orchestrated Security Platform for Internet of Robots // Proceedings of Springer International International Conference on Green, Pervasive, and Cloud Computing. 2017. pp. 298 – 312. https://doi.org/10.1007/978-3-319-57186-7_59
11. Басан А.С., Басан Е.С., Макаревич О.Б. Метод противодействия активным атакам злоумышленника в беспроводных сенсорных сетях // Известия ЮФУ. Технические науки. №5 (190). 2017. С 16 – 25. DOI 10.23683/2311-3103-2017-5-16-25
12. Basan A., Basan E., Makarevich O. Methodology of Countering Attacks for Wireless Sensor Networks Based on Trust // Proceedings of 8th International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC). Chengdu, China. 2016. pp.409 – 412. DOI: 10.1109/CyberC.2016.85
13. He W., Yang S., Teng D., Hu Y. A Link Level Load-Aware Queue Scheduling algorithm on MAC layer for wireless mesh networks // Proceedings of International Conference on Wireless Communications & Signal Processing. 2009. Nanjing, China. pp. 1 – 16.
14. Basan A.S., Basan E.S., Makarevich O.B. Development of the Hierarchal Trust management System for Mobile Cluster-based Wireless Sensor Network // Proceeding SIN '16 Proceedings of the 9th International Conference on Security of Information and Networks. 2016. pp. 116 – 122.
15. Абрамов Е.С., Басан Е.С. Разработка модели защищенной кластерной беспроводной сенсорной сети // Известия ЮФУ. Технические науки. 2013. № 12(149). С. 48 – 56.
16. Пшихопов В.Х., Соловьев В.В., Титов А.Е., Финаев В.И., Шаповалов И.О. Групповое управление подвижными объектами в неопределенных средах // Под ред. В.Х. Пшихопова. М.: ФИЗМАТЛИТ. 2015. – С. 233 – 270.
17. Sargeant I., Tomlinson A. Maliciously Manipulating a Robotic Swarm // Proceedings of Int'l Conf. Embedded Systems, Cyber-physical Systems, & Applications. ESCS'16. 2016. pp. 122 – 128.
18. Abbas S., Merabti M., D. Llewellyn-Jones, K. Kifayat. Lightweight Sybil Attack Detection in MANETs // IEEE system journal, №. 7, (2). 2013. pp 236 – 248.
19. Patel S.T., Mistry N.H. A review: Sybil attack detection techniques in WSN // Proceedings of 4th International Conference on Electronics and Communication Systems (ICECS). 2017. pp. 184 – 188.
20. Wang G., Musau F., Guo S., Abdullahi M. B. Neighbor Similarity Trust against Sybil Attack in P2P E-Commerce // IEEE transactions on parallel and distributed systems. № 26 (3). 2015. pp. 824 – 833.

REFERENCES:

- [1] Basan A.S., Basan E.S. [Threat model for mobile robot group management systems]. System synthesis and applied synergetics. Collection of proceedings of the VIII All-Russian Scientific Conference. - Sistemnyy sintez i prikladnaya sinergetika. Sbornik nauchnykh трудов VIII Vserossiyskoy nauchnoy konferentsii. Rostov-on-Don: Southern Federal University. 2017. С. 205 – 212. (in Russian).

- [2] H.S. Kim, S.W. Lee. Enhanced novel access control protocol over wireless sensor networks]. IEEE Transactions on Consumer Electronics. 2009. № 55 (2). pp. 492 – 498.
- [3] Branitsky A.A., Kotenko I.V. [Analysis and classification of methods for detecting network attacks] Information security. Proceedings of SPIIRAN - Informatsionnaya bezopasnost'. Trudy SPIIRAN.2016. №2(45). pp. 207 – 244. (in Russian).
- [4] Petrovsky O. Attack on the drones. Virus bulletin conference. 2015. pp. 16 – 24.
- [5] Garber L. Robot OS: A New Day for Robot Design. Computer. № 46 (12). 2013. pp. 16 – 20.
- [6] Kozhemyakin I.V., Putintsev I.A., Semenov N.N., Chemodanov M.N. [Development of an underwater robotic complex, using open simulation tools, supplemented with a model of hydroacoustic interaction]. News of SFedU. Technical science. Section II. Marine robotics. - Izvestiya YUFU. Tekhnicheskiye nauki. Razdel II. Morskaya robototekhnika. 2016. № 1 (174). pp. 88 – 99. (in Russian).
- [7] Vuong T. P., Loukas G., Gan D., Bezemskij A. Decision tree-based detection of denial of service and command injection attacks on robotic vehicles. 2015 IEEE International Workshop on Information Forensics and Security (WIFS) 2015. pp. 1 – 6.
- [8] Bezemskij A., Loukas G., Richard J. Gan D. Behaviour-based anomaly detection of cyber-physical attacks on a robotic vehicle. 15th International Conference on Ubiquitous Computing and Communications and 2016 8th International Symposium on Cyberspace and Security. 2016. pp. 61 – 68.
- [9] Mitchell R., Chen I.R. Adaptive Intrusion Detection of Malicious Unmanned Air Vehicles Using Behavior Rule Specifications. IEEE Transactions on Systems, Man, and Cybernetics: Systems. №44 (5). 2014. pp. 593 – 599.
- [10] Monshizadeh M., Khatri V., Kantola R., Yan Z. An Orchestrated Security Platform for Internet of Robots. Springer International International Conference on Green, Pervasive, and Cloud Computing. 2017. pp. 298 – 312.
- [11] Basan A.S., Basan E.S., Makarevich O.B. [Method of counteracting active attacks of an attacker in wireless sensor networks]. Известия ЮФУ. Технические науки. №5 (190).2017. pp. 16 – 25. (in Russian).
- [12] Basan A., Basan E., Makarevich O. Methodology of Countering Attacks for Wireless Sensor Networks Based on Trust. 8th International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC).Chengdu. 2016. pp. 409 – 412.
- [13] He W., Yang S., Teng D., Hu Y. A Link Level Load-Aware Queue Scheduling algorithm on MAC layer for wireless mesh networks // Proceedings of International Conference on Wireless Communications & Signal Processing.2009. Nanjing, China. pp. 1 – 16.
- [14] Basan A.S., Basan E.S., Makarevich O.B. Development of the Hierarchal Trust management System for Mobile Cluster-based Wireless Sensor Network // Proceeding SIN '16 Proceedings of the 9th International Conference on Security of Information and Networks. 2016. pp. 116 – 122.
- [15] Abramov E.S., Basan E.S. Development of a model of a secure cluster wireless sensor network. Izvestia SFU. Technical science. 2013. No. 12 (149). pp. 48 – 56. (in Russian).
- [16] Pshikhopov V.Kh., Soloviev V.V., Titov A.E., Finaev V.I., Shapovalov I.O. [Group management of mobile objects in uncertain environments]. Ed. V.H. Pshihopova. M.: FIZMATLIT. - Pod red. V.KH. Pshikhopova. M.: FIZMATLIюT 2015. – pp. 233 – 270. (in Russian.).
- [17] Sargeant I., Tomlinson A. Maliciously Manipulating a Robotic Swarm // Proceedings of Int'l Conf. Embedded Systems, Cyber-physical Systems, & Applications. ESCS'16. 2016. pp. 122 – 128.
- [18] Abbas S., Merabti M., D. Llewellyn-Jones, K. Kifayat. Lightweight Sybil Attack Detection in MANETs // IEEE system journal, №. 7, (2). 2013. pp 236 – 248.
- [19] Patel S.T., Mistry N.H. A review: Sybil attack detection techniques in WSN // Proceedings of 4th International Conference on Electronics and Communication Systems (ICECS). 2017. pp. 184 – 188.
- [20] Wang G., Musau F., Guo S., Abdullahi M. B. Neighbor Similarity Trust against Sybil Attack in P2P E-Commerce // IEEE transactions on parallel and distributed systems. № 26 (3). 2015. pp. 824 – 833.

*Поступила в редакцию – 01 октября 2019 г. Окончательный вариант – 01 ноября 2018 г.
Received – October 01, 2018. The final version – November 01, 2018.*