ИССЛЕДОВАНИЕ ВЛИЯНИЯ АКТИВНЫХ СЕТЕВЫХ АТАК НА ГРУППУ МОБИЛЬНЫХ РОБОТОВ[1]

Басан Е.С.[2], Басан А.С.[3], Макаревич О.Б.[4], Бабенко Л.К.[5]

Цель статьи: *разработка методики анализа эффективности активных сетевых атак при их воздействии на кибер-параметры группы мобильных роботов.*

Метод: *основан на применении математической статистики для анализа результатов и статистической информации, полученных путем моделирования поведения группы мобильных роботов. Методика включает в себя последовательность вычислений и их оценку с целью выявления аномалий в сети.*

Результаты: *Проведен статистический анализ изменения параметров узла сети во время проведения атаки и при отсутствии атаки. Определён набор параметров, на которые оказывают влияние различные атаки. Разработаны и реализованы сценарии активных сетевых атак, учитывающие разную степень интенсивности атаки. Данные сценарии при соответствующей доработке могут лечь в основе методики анализа защищённости групп мобильных роботов. Разработана методика оценки эффективности сети, а также обнаружения аномального поведения узлов. Проведено экспериментальное исследование, определившее наборы параметров для каждой атаки, которые целесообразно анализировать при ее выявлении. Сеть мобильных роботов, особенно беспилотных летательных аппаратов, может работать ограниченное количество времени, поэтому эффективность и интенсивность атаки играет ключевую роль при воздействии на сеть. Проведенное исследование позволяет определить, в каких случаях воздействие максимально эффективно, чтобы в дальнейшем суметь снизить риск возникновения возможного воздействия. Кроме того, исследование является вспомогательным для разработки системы обнаружения атак, так как выявляет новые зависимости и позволяет оценить воздействие атак на изменения в шаблонах трафика и поведении узлов. Основной областью применения данной работы является информационная безопасность и противодействие киберугрозам безопасности.*

Ключевые слова: *беспроводная сеть, уязвимости, активные атаки, Raspberry Pi, математическая статистика, потребление энергии, сетевой трафик, аномалии.*

DOI: 10.21681/2311-3456-2019-1-35-44

Введение

Уязвимости беспроводных сетей известны давно и активно исследуются учеными. Тем не менее, беспроводные технологии активно развиваются и области применения беспроводных сетей на сегодняшний день достаточно разнообразны [1]. Это связано с относительно недорогой стоимостью развертывания беспроводной сети, а также возможностью устройств, подключенных к сети, сохранять мобильность. Беспроводные сети применяются, в том числе, для установления взаимодействия между мобильными роботами, беспилотными летательными аппаратами, а также для «Интернета вещей» [2].

На сегодняшний день наблюдается тенденция, связанная с ростом популярности использования; к примеру, по данным «Национальной ассоциации участников рынка робототехники», только в промышленной робототехнике с 2010 по 2014 гг. средний рост продаж в год составлял 17%. При этом многие вопросы, связанные с обеспечением безопасности робототехнических систем, остаются нерешенными, в том числе проблемы обнаружения атак и аномального поведения. Прежде чем вводить в эксплуатацию систему мобильных устройств или робототехническую систему, необходимо провести анализ ее защищенности, минимизировать риски, связанные с обнаруженными угрозами и реализовать систему защиты в робототехнической системе.

Разработанная методика основана на анализе статистической информации о передаваемом трафике в сети. Основная идея заключается в следующем, чем интенсивнее сетевая атака, тем больше влияния она оказывает на структуру и состав сетевого трафика. Как правило,

1 Работа выполнена при поддержке гранта РФФИ №18-07-00212 «Разработка метода и протокола принятия решений для обнаружения аномального поведения узла в системах группового управления автономными мобильными роботами»

2 Басан Елена Сергеевна, кандидат технических наук, ассистент кафедры Безопасности информационных технологий Института компьютерных технологий и информационной безопасности Южного Федерального Университета «ЮФУ», г. Таганрог, Россия. E-mail: ebasan@sfedu.ru, ORCID 0000-0001-6127-4484

3 Басан Александр Сергеевич, кандидат технических наук, доцент кафедры Безопасности информационных технологий Института компьютерных технологий и информационной безопасности Южного Федерального Университета «ЮФУ», г. Таганрог, Россия. E-mail: asbasan@sfedu.ru, ORCID 0000-0002-2973-2737

4 Макаревич Олег Борисович, доктор технических наук, профессор кафедры Безопасности информационных технологий Института компьютерных технологий и информационной безопасности Южного Федерального Университета «ЮФУ», г. Таганрог, Россия. E-mail: obmakarevich@sfedu.ru, ORCID 0000-0003-0066-8564

5 Бабенко Людмила Климентьевна, доктор технических наук, профессор кафедры Безопасности информационных технологий Института компьютерных технологий и информационной безопасности Южного Федерального Университета «ЮФУ», г. Таганрог, Россия. E-mail: lkbabenko@sfedu.ru

основным назначением сетей мобильных устройств или роботов является исследование или фиксирование параметров окружающей среды.

Вне зависимости от того, какая атака проводится, она оказывает воздействие на загруженность узлов сети и тем самым меняется картина трафика в сети. При выполнении групповой задачи мобильные устройства (будь то роботы либо сенсорные узлы) обмениваются между собой информацией, причем данный процесс строго структурирован, и мобильные роботы действуют согласно заданному алгоритму. Кроме того, так как узлы сети обмениваются информацией по беспроводному каналу, они вынуждены его делить. Выделенные лидеры группы задают ритм работы, делят время на активные и неактивные периоды определённой длины. Каждый активный период начинается с посылки координатором специального пакета-маячка, который подчиненные узлы используют для синхронизации своей активности. После посылки маячка следует структурированный период активности [3]. Такой способ передачи сообщений позволяет сэкономить запас аккумулятора мобильного робота. За определённый период времени узлы обмениваются примерно равным количеством пакетов. Когда злоумышленник начинает проводить ту или иную активную атаку, направленное на свойство доступности, то картина трафика меняется. Чем интенсивнее атака, тем сильнее заметны изменения. Мобильные устройства имеют ограниченный заряд батареи и могут работать ограниченный промежуток времени [4]. Большую часть энергетических ресурсов узлы тратят на перемещение и фиксирование параметров окружающей среды, а также передачу пакетов. Если злоумышленник совершает атаку типа отказ в обслуживании, заставляя узел постоянно реагировать на его запросы, это приведет к дополнительным расходам на электроэнергию и не даст узлу уйти в «спящий режим», если это предусмотрено. В данной статье исследуется степень влияния сетевых атак на изменения различных параметров беспроводной сети и узлов сети. Определение порога эффективности атаки позволит улучшить качество системы предотвращения вторжений.

Необходимость подобного исследования может быть обусловлена тем, что сети мобильных устройств сами по себе уязвимы для воздействия среды и некоторые изменения могут быть ошибочно приняты за атаку или аномальную активность.

Существует несколько работ, посвященных разработке систем обнаружения атак и вторжений для мобильных роботов. В данных работах в качестве параметров, которые позволяют обнаружить атаку, берутся различные характеристики, в основном физические параметры. Так, в работе [5] в качестве индикаторов атаки взяты следующие:

- Подготовка к использованию оружия вне зоны боевых действий.
- Отличия показаний сенсорной системы узла от показаний узла-монитора.
- Плохие рекомендации доверенным узлам группы.
- БПЛА разворачивает шасси, когда находится вне базы.
- Узел отправляет пакеты неавторизованным узлам.
- БЛА использует контрмеры без наличия угрозы и т.п.

Данные индикаторы в основном позволяют определять поведение мобильного робота с позиции физического устройства. Основной недостаток подхода в том, что если необходимо использовать данную систему обнаружения атак не для БЛА, то необходимо изменять набор индикаторов. В работе [6] рассматривается параметр отсутствие связи, который помогает обнаружить атаку отказ в обслуживании. В статье [7] авторы используют следующие метрики для выявления атаки: репутация узла, оценка поведения, оценка расстояния. Такие метрики позволяют выявить атаки, направленные на изменение поведения узла.

В статье [8] авторами рассмотрена система обнаружения атак на основе использования дерева принятия решений. Достоинством названного подхода является то, что авторы рассматривают кибер-атаки. Для обнаружения данных атак авторы наряду с четырьмя признаками для анализа коммуникации и обработки информации, которые называются кибер-функциями ввода, используют четыре параметра для анализа физических свойств робота, которые авторы называют физическими характеристиками входного сигнала.

Таким образом, авторы чаще всего исследуют поведенческие особенности роботов или изменения физической среды. В данном исследовании предлагается методика для оценки эффективности сетевых атак. Подобное исследование представлено в статье [9] для мобильной Ad-Hoc сети. Но в данном исследовании авторы в основном рассматривают атаки, связанные с протоколом маршрутизации AODV. Несмотря на то, что данный протокол достаточно часто используется для построения Ad-Hoc сетей, существуют и другие протоколы. Данное исследование достаточно узкоспециализированное.

Таким образом, предлагаемая методика анализа эффективности атак позволит исследователям определить, как быстро их система обнаружения атак вычисляет атаку, а также какая при этом степень ущерба может быть нанесена сети. Это также позволит понять, на изменение каких параметров необходимо обратить внимание, чтобы зафиксировать атаку.

1. Методика оценки эффективности активных атак на беспроводные мобильные устройства

Методика включает в себя следующую последовательность действий:

1. Расчет общего объема трафика, проходящего через узел сети (сетевая загруженность узла):

$$L_{Total} = \sum_N s_{data}(\Delta t) + \sum_N s_{routing}(\Delta t) + \sum_N r_{data}(\Delta t) + \sum_N r_{routing}(\Delta t) + \\ + \sum_N d_{data}(\Delta t) + \sum_N d_{routing}(\Delta t) + \sum_N f_{data}(\Delta t) + \sum_N f_{routing}(\Delta t), \quad (1)$$

где S_{data} – общее количество сегментов, отправленных на транспортном уровне; $S_{routing}$ – общее количество переданных по протоколу маршрутизации; R_{data} – общее количество сегментов, принятых на транспортном уровне; $R_{routing}$ – общее количество принятых пакетов маршрутизации. ddata общее количество отброшенных сегментов, передаваемых на транспортном уровне; $D_{routing}$ – общее количество отброшенных пакетов маршрутизации. F_{data}

– общее количество сегментов перенаправленных на транспортном уровне; $F_{routing}$ – общее количество перенаправленных пакетов маршрутизации. N – общее количество узлов в сети.

Необходимо оценивать рост этой метрики. Если в сети наблюдается интенсивный рост данной метрики, то это может служить признаком атаки отказ в обслуживании.

2. Второй шаг – оценка степени рассеивания параметра загруженность узлов сети относительно среднего значения. Для этого необходимо вычислить генеральную дисперсию для значения загруженность узла на текущем интервале для каждого узла сети:

$$D_{Lg} = \left(\sum_{i=1}^{N} (L_i - \bar{L}_g)^2 \right) / N, \quad (2)$$

где D_{Lg} – генеральная дисперсия параметра загруженность сети, $\bar{L}_g$ – это генеральная средняя для показателя загруженность узла сети, L_i – уровень загрузки текущего узла, N общее количество узлов сети.

Если в процессе работы сети наблюдается рост значения метрики, то можно сделать вывод о том, что в сети присутствует аномалия.

3. Расчет соотношения отправленных и принятых пакетов.

$$RSRP = r_{i,n,cbr} / s_{i,n,cbr}, \quad (3)$$

где $RSRP$ – соотношение между принятыми и отправленными пакетами.

Ключевым аспектом проведения атаки отказ в обслуживании и атаки распределенный отказ в обслуживании является увеличение количества запросов на стороне жертвы. При нормальной работе сети количество принятых сегментов по протоколу транспортного уровня должно приблизительно совпадать с количеством отправленных пакетов, возможны небольшие отклонения. Если измерить соотношение отправленных и принятых пакетов, можно обнаружить аномальное поведение узла. Если узел становится жертвой атаки отказ в обслуживании, то наблюдается преобладание принятых сегментов.

4. Отклонение от общей средней показателей количество принятых пакетов и отправленных пакетов для каждого узла сети:

$$Dev_{N,i,s}(\Delta t) = (s_{n,i}(\Delta t) - \bar{s}_i(\Delta t)) / N, \quad (4)$$

$$Dev_{N,i,r}(\Delta t) = (r_{n,i}(\Delta t) - \bar{r}_i(\Delta t)) / N. \quad (5)$$

где $Deviation_{N,i,s_{cbr}}$, $Deviation_{N,i,r_{cbr}}$ - отклонение от общей средней параметра – количество отправленных и принятых сегментов транспортного уровня для каждого узла сети за текущий интервал времени. $\bar{s}_{i,cbr}, \bar{r}_{i,cbr}$ - среднее значения для параметров – количество принятых и отправленных пакетов с данными за текущий интервал времени для всех узлов.

При нормальной работе сети данное значение колеблется от -10 до 10. Соответственно, если проводится интенсивная атака, то данные границы будут значительно расширены.

5. Расчет отношения отброшенных пакетов в заданный момент времени для текущего узла от нормальной работы сети:

$$Ratio_{i,d}(\Delta t) = d_i(\Delta t) / d_{norm_i}(\Delta t). \quad (6)$$

При нормальной работе сети узлы могут отбрасывать пакеты могут быть отброшены в результате возникновения коллизий, переполнения очереди пакетов. Таким образом, при нормальной работе сети допустимое количество отброшенных пакетов составляет 1%.

Если наблюдается превышение уровня отброшенных пакетов более чем в 3 раза, можно говорить о наличие аномальной активности в сети. Отброшенные пакеты могут возникать не только при проведении атаки Черная дыра, но также во время атаки отказ в обслуживании, так как узлы не успевают обрабатывать пакеты и отбрасывают их из очереди.

6. Сравнительный коэффициент переданных пакетов, принятых пакетов, и потерянные пакеты:

$$Ratio_{sent} = \frac{(\sum s_{total}(\Delta t))}{L_{Total}} * 100\% \quad (7)$$

$$Ratio_{received} = \frac{(\sum r_{total}(\Delta t))}{L_{Total}} * 100\%, \quad (8)$$

$$Ratio_{dropped} = \frac{(\sum d_{total}(\Delta t))}{L_{Total}} * 100\%, \quad (9)$$

где $Ratio_{sent}$ – процентное содержание отправленных пакетов в общем трафике, $Ratio_{received}$ – процентное содержание принятых пакетов в общем трафике, $Ratio_{dropped}$ --процентное содержание из отброшенных пакетов в общем трафике. $s_{total}(\Delta t)$ - общее количество отправленных пакетов для текущего временного интервала всеми узлами сети, $r_{total}(\Delta t)$ – общее количество принятых пакетов для текущего временного интервала, для всех узлов сети, $d_{total}(\Delta t)$ – общее количество потерянных пакетов для текущего временного интервала.

По сути, данные метрики позволяют построить общую «картину» трафика и оценить преобладание одного из типов пакетов в сети.

7. Мониторинг потребления электроэнергии проводился с использованием тестера KEWEISI KWS-V21 в корпусе с рабочим напряжением 3-20 В и рабочим током 0-3,3 А. Этот тестер отображает следующие характеристики: напряжение (U), ток питания (A), потребляемая емкость аккумулятора (мАч), время.

2 Разработка экспериментального стенда для проведения активных атак

2.1. Разработка натурной модели группы мобильных устройств

Одним из компонентов стенда является программно-аппаратное средство для реализации атак на беспроводную сеть. Программно-аппаратное средство для тестирования безопасности беспроводных сетей должно обладать следующими свойствами: мобильность; малые размеры; модульная структура; простота использования; низкая цена; поддержка операционных систем семейства Linux; низкое энергопотребление. Для удовлетворения вышеуказанным требованиям была выбрана одноплатная платформа Raspberry Pi 3 model B [10]. Устройство управляется удаленно и оснащено небольшой батареей емкостью 10 000 мАч, операционная система - Raspbian, версия ядра 4.9. Кроме того, экспериментальный стенд включает в себя WiFi-маршрутизатор D-Link, модель 320.

Рис. 1. Разработанный экспериментальный стенд для реализации методики оценки эффективности активных атак на беспроводные мобильные устройства.

На рисунке 1 представлена схема разработанного экспериментального стенда, включающего в себя перечисленные выше компоненты.

Несмотря на то, что доступ к беспроводному маршрутизатору защищен паролем, злоумышленник может прослушивать частоту, на которой работает маршрутизатор и получать данные, передаваемые на канальном уровне.

В дополнение к натурной модели была также создана модель в симуляторе NS-2.35. Первоначально все эксперименты проводились на модели, чтобы определить параметры, на которые влияет атака. Затем атаки были реализованы на полномасштабной модели мобильных устройств, и результаты экспериментов были подтверждены.

2.2 Сценарии атак на беспроводные мобильные устройства

2.2.1 Атака отказ в обслуживании

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 выполнять свою деятельность в штатном режиме. На сегодняшний день существует множество способов реализации атаки отказ в обслуживании [11]. Одним из способов реализации атаки для разработанного экспериментального стенда является атака SYN-flood [12]. Злоумышленник может проводить данную атаку с различной интенсивностью. Интенсивность атаки может меняться в зависимости от интервала между посылкой пакетов или в зависимости от числа жертв атаки. При реализации атаки в сети мобильных роботов необходимо учитывать, что работа сети мобильных роботов ограничена во времени. К примеру, сеть БЛА может полноценно работать только на протяжении 30 минут, выполняя какие-либо задачи [13]. Так что проведение низкоинтенсивной атаки или распределенной во времени атаки не имеет смысла. Одной из задач проведения атаки отказ в обслуживании является исчерпание ресурсов узла, поэтому увеличение расхода энергии является одной из важных характеристик атаки. Вторым параметром, который позволит обнаружить аномальную активность, является интенсивность трафика.

Для анализа эффективности атаки отказ в обслуживании и выявления параметров узла, на которые оказывает влияния данная атака, было разработано три сценария атаки. Первый сценарий заключается в том, что один узел злоумышленника активно атакует один доверенный узел, так что в сети имеется одна жертва атаки. Во втором сценарии узел злоумышленника атакует 25% доверенных узлов. В третьем сценарии атаке подвергается 50% узлов. Так как из 10 узлов один является внутренним злоумышленником и один узел центральный сервер. Принцип атаки заключается в том, что атакующий отправляет SYN-запросы и переполняет очередь соединений для жертвы атаки. В очереди появляются полуоткрытые соединения, ожидающие подтверждения со стороны клиента.

2.2.2 Атака Черная дыра и Серая дыра

На рисунке 2 показана схема атаки Черная дыра. Атака заключается в том, что злоумышленник находится между двумя доверенными узлами и вместо пересылки пакетов он отбрасывает их [14]. Как правило, узлы, находящиеся на значительном расстоянии от базовой станции или лидеры группы, могут стать жертвой такой атаки. В то же время злоумышленник может отбрасывать только пакеты, переданные по определенному протоколу или в соответствии с определенными временными интервалами, и в этом случае проводится атака Серая - дыра [15].

На рисунке 2 представлена следующая ситуация. Узлы N10-15 являются злоумышленными и отбрасывают пакеты, которые доверенные узлы пытаются передать лидеру группы. Кроме того, узлы могут обмениваться пакетами в двустороннем направлении. Если между ними не расположен узел злоумышленника, то пакеты будут успешно отправляться и передаваться. Из рисунка 2 видно, что узлы 8,9,7,1,4,3,5 подвержены атаке. Толь-

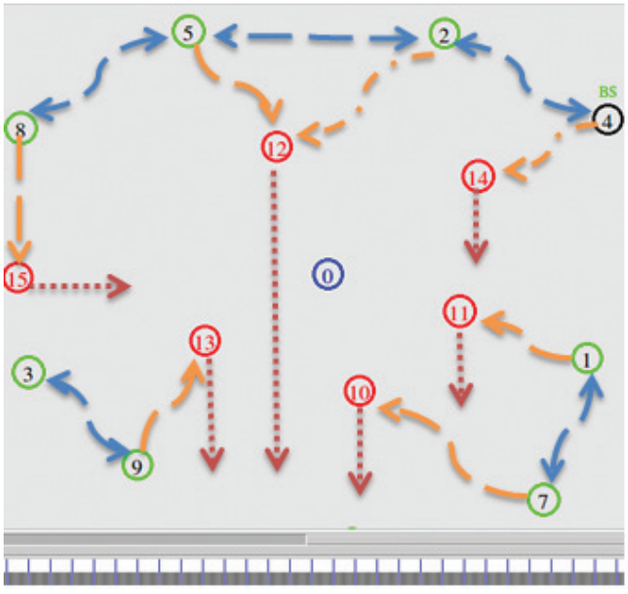

Рис.2. Схема проведения атаки Черная-дыра и Серая дыра

ко узел 2 может общаться с базовой станцией в обход лидера группы. Узлы 1,7,3,5 становятся полностью изолированными и могут общаться только друг с другом. Таким образом, чем больше пакетов отброшено злоумышленными узлами, тем эффективнее проходит атака. Когда сеть работает в штатном режиме, то отброшенные пакеты могут появляться, но их количество незначительное [16]. Для реализации данной атаки в систему моделирования NS-2.35 был добавлен тип поведения узла, когда он отбрасывает пакеты, перенаправляемые через него.

Атака Серая-дыра похожа на атаку Черная-дыра отличием является то, что злоумышленные узлы отбрасывают пакеты не постоянно, а с учетом заданного условия. В данном исследовании атака была реализована таким образом, что злоумышленные узлы отбрасывали пакеты в определенные временные интервалы. Для проведения данной атаки, в файлы NS-2.35 был добавлен злоумышленник, который отбрасывает пакеты, которые проходят через него: $ns at 0.0 «[$node(12) set ragent_] malicious». Для того чтобы «вернуть» злоумышленнику нормальное поведение, был добавлен доверенный тип поведения, когда узел не отбрасывает пакеты: $ns at 10.0 «[$node(12) set ragent_] trusted. Ниже приведен пример для узла 15, по которому он будет отбрасывать пакеты. С 1 по 17 секунду узел будет отбрасывать пакеты, потом он будет передавать пакеты в штатном режиме. Затем начиная с 33 секунды, узел опять начнет отбрасывать пакеты:

$ns at 1 «[$node(15) set ragent_] malicious»
$ns at 17.0 «[$node(15) set ragent_] trusted»
$ns at 33.0 «[$node(15) set ragent_] malicious»
$ns at 50.0 «[$node(15) set ragent_] trusted»
$ns at 60.0 «[$node(15) set ragent_] malicious»

Реализация атаки для натурной модели группы мобильных узлов представлена на рисунке 3. Одно из устройств является сервером, а другое клиентом. Для каждого из них были написаны соответствующие сокеты (сервер, клиент) на языке Python. Клиент отправляет строку «com1» серверу, а сервер в ответ отправляет её же клиенту. Трафик идет через маршрутизатор. Цель

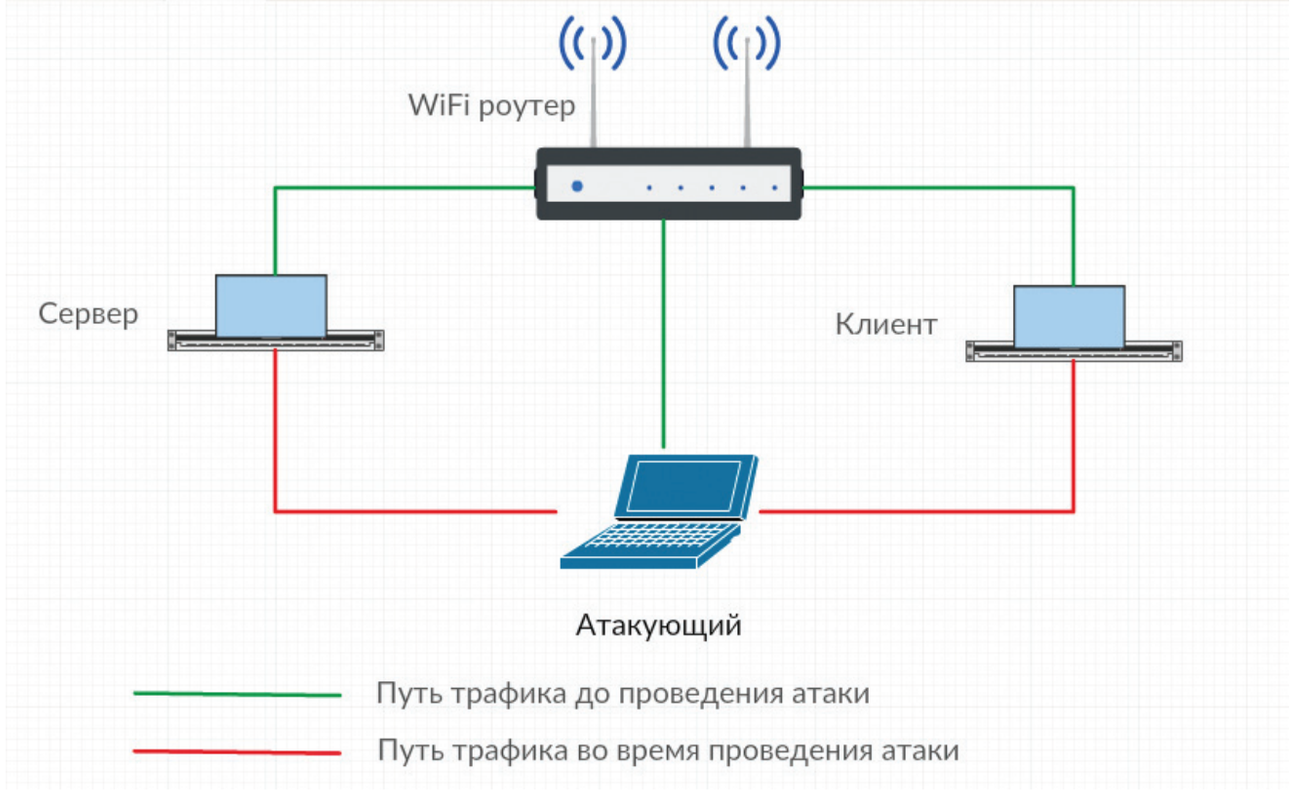

Рис. 3. Схема реализации атак Человек посредине и Черная дыра для натурной модели беспроводной сети мобильных устройств

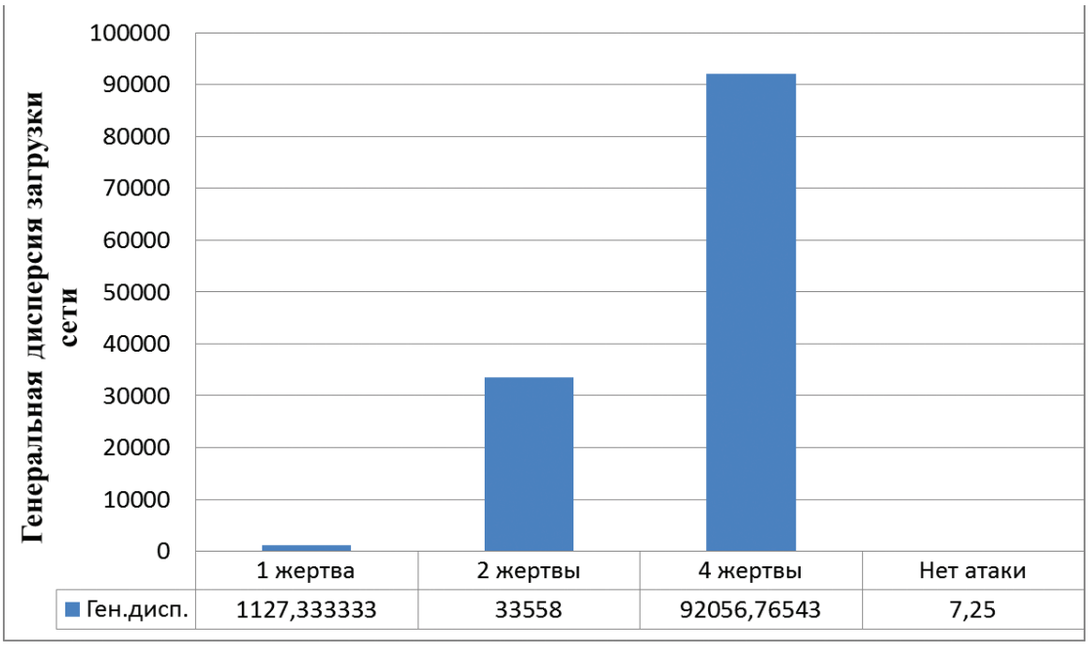

Рис.4. Дисперсия параметра загрузка сети для узлов при DoS атаке с различным числом жертв

злоумышленника перехватить данные отправленные сервером в ответ клиенту и подменить строку «com1» на «com2». В итоге сервер, получив строку «com1», отправит её клиенту, но клиент должен получить в ответе «com2».

Данная атака реализована с помощью инструментов habu и nfqsed [17]. Для правильной работы программы следует направить трафик на вход программы nfqsed. Для этого вводятся следующие правила для iptables:

iptables -A OUTPUT -p tcp -m string --string «com1» --algo kmp -j NFQUEUE // проверка на вхождение в пакет строки «com1», если есть вхождение, то пакет отправляется на вход программы для модификации;

iptables -A OUTPUT -p tcp -j ACCEPT //если вхождения строки нет, то отработает данное правило, пакет отправляется как есть.

Если злоумышленнику необходимо выполнить атаку Черная дыра, тогда правила iptables будут сконфигурированы таким образом, чтобы злоумышленник отбрасывал пакеты, проходящие через него.

iptables -A OUTPUT -p tcp -j DROP.

3. Результаты экспериментального исследования

3.1 Атака отказ в обслуживании

На рисунке 4 представлено изменение метрики генеральная дисперсия для параметра сетевая загрузка узлов сети (2). Из рисунка видно, что с ростом числа жертв дисперсия значительно увеличивается. Это означает то, что загруженность узлов (1) достаточно сильно отличается от среднего значения. Это происходит потому, что уровень сетевой загрузки злоумышленного узла значительно превышает узел загруженности доверенных узлов. А также уровень загруженности узлов-жертв также вырос по сравнению с нормальным состоянием [18].

При нормальной работе сети, когда узлы отправляют пакеты по заданному алгоритму и функционируют в штатном режиме, уровень дисперсии может достигать 7-10. Таким образом, аномальная активность в сети присутствует. Наличие атаки отказ в обслуживании достаточно точно определяется с помощью метрики соотношение отправленных и принятых пакетов (3). Из рисунка 5 видно, что узлы, подверженные атаке принимают больше пакетов, чем отправляют. Причем разница составляет более, чем в 2-2,5 раза. В таком случае атака считается эффективной.

Из рисунка 5 видно, что при нормальной работе сети данное соотношение стремится к единице. Если же атака проводится, то у узлов-жертв соотношение больше одного, а у злоумышленника меньше. Предположим, что атака отказ в обслуживании является наиболее эффективной, если значительно влияет на энергопотребление узлов сети [19]. Помимо того, что расходуются ресурсы жертв атаки, в значительной степени расходуются ресурсы злоумышленника и его энергопотребление растет. На рисунке 6 представлен график энергопотребления для злоумышленника, жертвы атаки и узла, неподверженного атаке. Анализируя изменение данного параметра можно вывить атаку и определить степень ее интенсивности.

3.2 Атака Черная дыра и Серая дыра

Во время атаки Черная дыра значение генеральной дисперсии (2) составляло 829,3, что значительно превышает дисперсию при нормальных условиях. Это указывает на аномальную активность в сети. Эффективным параметром при обнаружении этой атаки является оценка роста отброшенных пакетов (6). Из рисунка 7 видно, что по мере увеличения количества вредоносных узлов количество отброшенных пакетов увеличивается по сравнению с нормальной работой. Большее количество узлов атаковано и изолировано от лидера группы.

На рисунке 8 представлены результаты вычисления сравнительных коэффициентов для переданных пакетов,

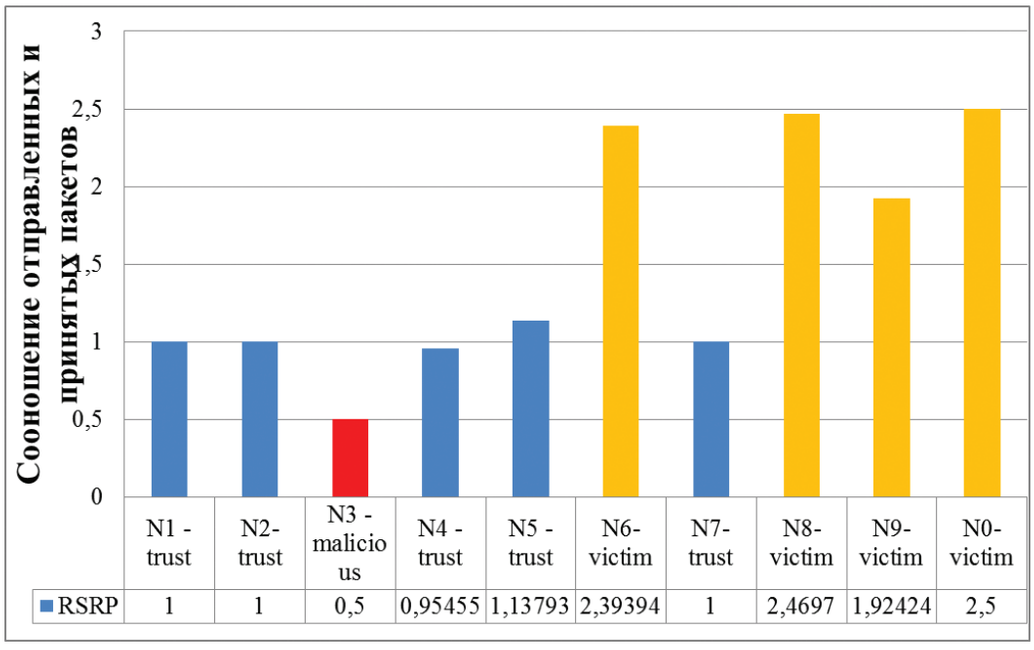

Рис. 5. Соотношение отправленных к полученным пакетам (RSRP) для доверенных узлов (trust), узлов-жертв (victims) и вредоносных узлов (malicious) во время проведения DoS-атаки

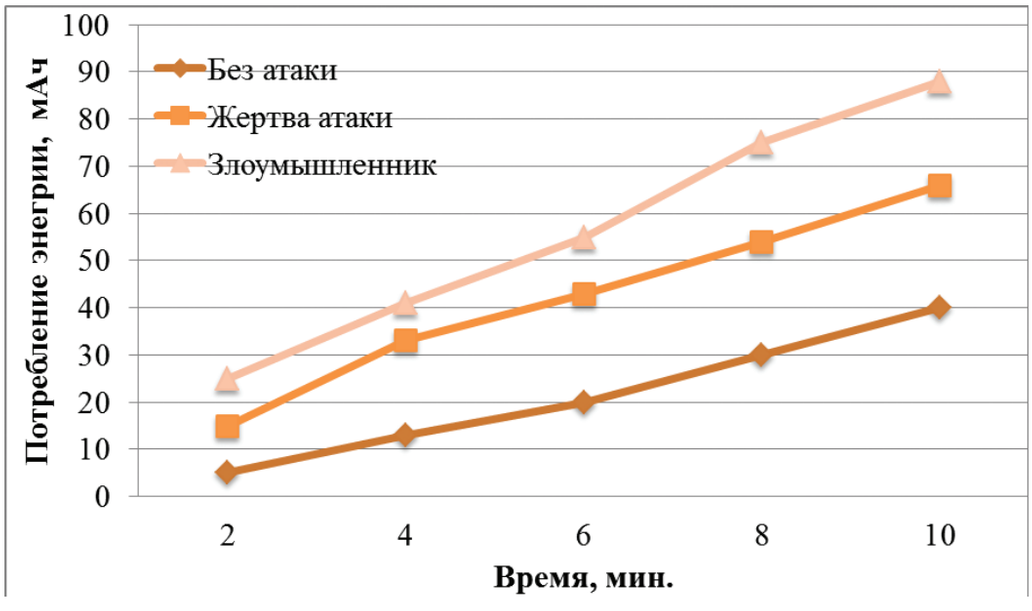

Рис. 6. Энергопотребление устройства при атаке и в нормальных условиях

принятых пакетов, и потерянные пакеты в трех случаях.

Рисунок 8 (a) демонстрирует ситуацию, когда узел был подвержен интенсивной атаке, в сеть было внедрено 50% злоумышленных узлов, которые блокировали передачу пакетов. Тем не менее, не все пакеты были отброшены, так как основная цель злоумышленника была заблокировать общение между узлами сети и центральным узлом [20]. Между собой узлы могут поддерживать общение, что составляет 20% трафика. При нормальной работе сети наблюдается соотношение отправленных и полученных пакетов в равных частях, и небольшое количество отброшенных пакетов (см. Рис. 8 (c)). Посторенние подобных диаграмм в реальном режиме времени может позволить определять степень интенсивности атаки, а также обнаруживать ее присутствие. Что касается уровня потребления энергии, оно существенно не изменилась. Можно сказать, что наблюдалось еще более низкое потребление, так как узел жертвы не тратил энергию на получение пакета.

Заключение

В заключение следует отметить следующее. Во-первых, для того, чтобы атака нарушила работу сети, она должна быть достаточно интенсивной и, предпочтительно, распределяться между несколькими атакующими. В случае атаки на отказ в обслуживании можно определить степень эффективности воздействия на жертву по уровню потребления энергии, а также изменения соот-

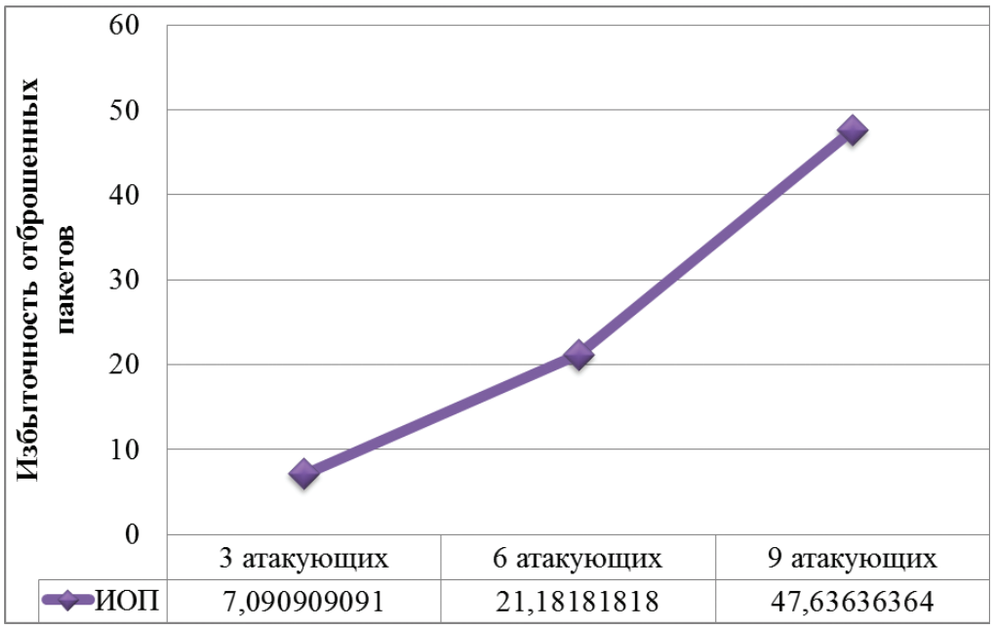

Рис.7. Изменение количества отброшенных пакетов под воздействием атаки Черная дыра по сравнению с нормальной работой сети

(a) *(б)* *(c)*

Рис.8. Диаграмма структуры трафика для сети при атаке Черная дыра с изменением количества вредоносных узлов (a), для 50% вредоносных узлов (b), для 25% вредоносных хостов (c) отсутствовали вредоносные узлы

ношения отправленных и полученных пакетов жертв и злоумышленников и общее увеличение сетевой нагрузки узлов. В случае атаки Черная дыра можно говорить о высокой эффективности атаки, когда наблюдалось большое количество жертв, то есть заблокированных узлов. Атака оказывала влияние на отношение отправленных, принятых и отброшенных пакетов. Данная атака не влияет на потребление энергии. Во-вторых, довольно эффективно применять метрику генеральная дисперсия для сетевой загрузки узла. Чем больше значение дисперсии, тем больше отклонение сетевой загрузки узлов от среднего значения в группе. Большее влияние злоумышленника на сеть наблюдалось, когда дисперсия была в 100 раз больше по сравнению с обычными условиями. В будущем использование этих параметров обеспечит разработку системы обнаружения вторжений для группы мобильных роботов.

Литература:

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 - Южный федеральный университет, 2017. С. 205-212.
2. Varshney K.K., Samundiswary P. Performance analysis of malicious nodes in IEEE 802.15.4 based wireless sensor network // Proceedings of International Conference on Information Communication and Embedded Systems (ICICES2014). 2014. P. 1 – 5. DOI: 10.1109/ICICES.2014.7033873.
3. Basan A., Basan E., Makarevich O. A Trust Evaluation Method for Active Attack Coun-teraction in Wireless Sensor Networks // Proceedings of International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. 2017. P. 369-372. DOI 10.1109/CyberC.2017.14.
4. 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, Vol. 44, No5. May 2014. P. 2168-2216. DOI: 10.1109/TSMC.2013.2265083.
5. Choi Y., Hong Y.-G. Study on coupling of software-defined networking and wireless sensor networks // Proceedings of Eighth International Conference on Ubiquitous and Future Networks (ICUFN). 2016. P. 900 – 902. DOI: 10.1109/ICUFN.2016.7536926.

6. Shailendra, Singh M. Khan Md. A., Singh V., Patil A.; Wadar S. Attendance management system // Proceedings of 2nd International Conference on Electronics and Communication Systems (ICECS). 2015. P. 418 – 422. DOI: 10.1109/ECS.2015.7124938
7. Shetty S., Adedokun T., Keel L.-H. Cyberphyseclab: A testbed for modeling, detecting and responding to security attacks on cyber physical systems // Proceedings of BigData/SocialCom/CyberSecurity Conference - Stanford University. May 27-31, 2014. P. 1-6.
8. Oliva G., Manna D. L., Fagiolini A., Setol R. Distance-constrained data clustering by combined k-means algorithms and opinion dynamics filters // Proceedings of 22nd Mediterranean Conference on Control and Automation. 2014. P. 612 – 619. DOI: 10.1109/MED.2014.6961441.
9. Vuong T. P., Loukas G., Gan D., Bezemskij A. Decision tree-based detection of denial of service and command injection attacks on robotic vehicle // Proceedings of IEEE International Workshop on Information Forensics and Security (WIFS). 2015. P. 1-6. DOI: 10.1109/WIFS.2015.7368559.
10. Mejaele L., Ochola E. O. Analysing the impact of black hole attack on DSR-based MANET: The hidden network destructor. // Proceedings of Second International Conference on Information Security and Cyber Forensics (InfoSec). 2015. P. 140 – 144. DOI: 10.1109/InfoSec.2015.7435519.
11. Vasconcelos G., Carrijo R., Miani J., Souza V. The Impact of DoS Attacks on the AR.Drone 2.0. // Proceedings of XIII Latin American Robotics Symposium and IV Brazilian Robotics Symposium (LARS/SBR). 2016. P. 127 – 132.
12. Chadha K., Jain S. Impact of black hole and gray hole attack in AODV protocol // Proceedings of International Conference on Recent Advances and Innovations in Engineering (ICRAIE), 2014. P. 1-7. DOI: 10.1109/ICRAIE.2014.6909188.
13. Maheshwaran P., Rajagopal S. A scheme for detecting the types of misbehavior and identifying the attacks using reputation mechanism in a mobile ad-hoc network // Proceedings of International Conference on Communication and Electronics Systems (ICCES). 2016. P. 1-6. DOI: 10.1109/CESYS.2016.7889961
14. Basan A., Basan E., Makarevich O. Analysis of Ways to Secure Group Control for Autonomous Mobile Robots // Proceedings of 10th International Conference on Security of Information And Networks (SIN 2017). 2017. P.134-139. DOI:10.1145/3136825.3136879.
15. Басан А.С., Басан Е.С., Степенкин А.А. Анализ и реализация угроз для систем управления мобильными роботами // Материалы XIII Всероссийской научно – практической конференции: Математические методы и информационно - технические средства. 2017. С.20-23.
16. Loukas G. Cyber-Physical Attacks: A Growing Invisible Threat / Imprint: Butterworth-Heinemann - Elsevier. ISBN: 978-0-12-801290-1. 2015. P. 270.
17. Dong Qi., Hayashi K., Kaneko M. Adaptive modulation and coding design for communication-based train control systems using IEEE 802.11 MAC with RTS/CT // Proceedings of IEEE 18th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC). 2017. P. 1 - 5. DOI: 10.1109/SPAWC.2017.8227786
18. Geetha K., Sreenath N. SYN flooding attack — Identification and analysis // Proceedings of International Conference on Information Communication and Embedded Systems (ICICES2014). 2014. P.1 – 7. DOI: 10.1109/ICICES.2014.7033828
19. Sargeant I., Tomlinson A. Maliciously Manipulating a Robotic Swarm // Proceedings of Int'l Conf. Embedded Systems, Cyber-physical Systems, & Applications. ESCS'16. 2016. P. 122- 128.
20. Vadavi J. V., Ashwini G. Sugavi. Detection of black hole attack in enhanced AODV protocol // Proceedings of International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN). 2017. P. 118 – 123. DOI: 10.1109/IC3TSN.2017.8284462.

Рецензент: *Цирлов Валентин Леонидович, кандидат технических наук, доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, Москва, Россия. E-mail: v.tsirlov@npo-echelon.ru*

STUDYING THE IMPACT OF ACTIVE NETWORK ATTACKS ON A MOBILE ROBOTS GROUP

Basan E.S.[6], Basan A.S.[7], Makarevich O.B.[8], Babenko L.K.[9]

Purpose: *Developing a procedure to analyze the effectiveness of active network attacks affecting cyber parameters of a mobile robots group.*

Research methods: *Based on using mathematical statistics to analyze the results and statistical information obtained by modeling the behavior of a mobile robots group. The procedure includes a sequence of calculations and their evaluation in order to identify anomalies in the network.*

6 Elena S. Basan, Ph.D. Assistant at Department of Information Technology Security Institute of Computer Technologies and Information Security of Southern Federal University (SFedU), Taganrog, Russia. E-mail ebasan@sfedu.ru, ORCID 0000-0001-6127-4484

7 Alexander S. Basan, Ph.D., Assistant Professor at Department of Information Technology Security Institute of Computer Technologies and Information Security Southern Federal University (SFedU), Taganrog, Russia. E-mail: asbasan@sfedu.ru, ORCID 0000-0002-2973-2737

8 Oleg B. Makarevich, Doctor of Technical Sciences, Head of Department of Information Technology Security Institute of Computer Technologies and Information Security of Southern Federal University (SFedU), Taganrog, Russia. E-mail: obmakarevich@sfedu.ru, ORCID 0000-0003-0066-8564

9 Lyudmila K. Babenko, Doctor of Technical Sciences, Professor at Department of Information Technology Security Institute of Computer Technologies and Information of Security Southern Federal University (SFedU). Taganrog, Russia. E-mail: lkbabenko@sfedu.ru

Results: *A statistical analysis of changes in the network node parameters during and in the absence of attack was conducted. A set of parameters affected by various attacks was determined. Scenarios for active network attacks that take into account varying degrees of attack intensity were developed and implemented. If fine-tuned, these scenarios can form the basis of the procedure for analyzing security of the mobile robots group. A procedure for assessing the network effectiveness and detecting anomalous node behavior was developed. An experimental study was conducted that identified parameter sets for each attack, which should be analyzed whenever an attack is detected. A network of mobile robots, especially drones, can work for a limited amount of time, so the attack effectiveness and intensity play a key role in influencing the network. The study helps determine when the effect is maximum, so that the risk of possible impact can be subsequently reduced. Furthermore, the study is auxiliary for developing an attack detection system, since it reveals new dependencies and allows one to evaluate the impact of attacks on changes in traffic patterns and node behavior. The key applications of this work are information security and countering cyber security threats.*

Keywords: *wireless network, vulnerabilities, active attacks, Raspberry Pi, mathematical statistics, power consumption, network traffic, anomalies.*

References:

1. Basan A.S., Basan E.S. Model' ugroz dlya sistem gruppovogo upravleniya mobil'nymi robotami // Sistemnyy Sintez i prikladnaya sinergetika // Sbornik nauchnykh trudov VIII Vserossiyskoy nauchnoy konferentsii - Yuzhnyy federal'nyy universitet [System Synthesis and applied synergetics. Collection of scientific papers of the VIII All-Russian Scientific Conference - Southern Federal University], 2017. pp. 205-212..
2. Varshney K.K., Samundiswary P. Performance analysis of malicious nodes in IEEE 802.15.4 based wireless sensor network // Proceedings of International Conference on Information Communication and Embedded Systems (ICICES2014). 2014. P. 1 – 5. DOI: 10.1109/ICICES.2014.7033873.
3. Basan A., Basan E., Makarevich O. A Trust Evaluation Method for Active Attack Coun-teraction in Wireless Sensor Networks // Proceedings of International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. 2017. P. 369-372. DOI 10.1109/CyberC.2017.14.
4. 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, Vol. 44, No5. May 2014. P. 2168-2216. DOI: 10.1109/TSMC.2013.2265083.
5. Choi Y., Hong Y.-G. Study on coupling of software-defined networking and wireless sensor networks // Proceedings of Eighth International Conference on Ubiquitous and Future Networks (ICUFN). 2016. P. 900 – 902. DOI: 10.1109/ICUFN.2016.7536926.
6. Shailendra, Singh M. Khan Md. A., Singh V., Patil A.; Wadar S. Attendance management system // Proceedings of 2nd International Conference on Electronics and Communication Systems (ICECS). 2015. P. 418 – 422. DOI: 10.1109/ECS.2015.7124938
7. Shetty S., Adedokun T., Keel L.-H. Cyberphyseclab: A testbed for modeling, detecting and responding to security attacks on cyber physical systems // Proceedings of BigData/SocialCom/CyberSecurity Conference - Stanford University. May 27-31, 2014. P. 1-6.
8. Oliva G., Manna D. L., Fagiolini A., Setol R. Distance-constrained data clustering by combined k-means algorithms and opinion dynamics filters // Proceedings of 22nd Mediterranean Conference on Control and Automation. 2014. P. 612 – 619. DOI: 10.1109/MED.2014.6961441.
9. Vuong T. P., Loukas G., Gan D., Bezemskij A. Decision tree-based detection of denial of service and command injection attacks on robotic vehicle // Proceedings of IEEE International Workshop on Information Forensics and Security (WIFS). 2015. P. 1-6. DOI: 10.1109/WIFS.2015.7368559.
10. Mejaele L., Ochola E. O. Analysing the impact of black hole attack on DSR-based MANET: The hidden network destructor. // Proceedings of Second International Conference on Information Security and Cyber Forensics (InfoSec). 2015. P. 140 – 144. DOI: 10.1109/InfoSec.2015.7435519.
11. Vasconcelos G., Carrijo R., Miani J., Souza V. The Impact of DoS Attacks on the AR.Drone 2.0. // Proceedings of XIII Latin American Robotics Symposium and IV Brazilian Robotics Symposium (LARS/SBR). 2016. P. 127 – 132.
12. Chadha K., Jain S. Impact of black hole and gray hole attack in AODV protocol // Proceedings of International Conference on Recent Advances and Innovations in Engineering (ICRAIE), 2014. P. 1-7. DOI: 10.1109/ICRAIE.2014.6909188.
13. Maheshwaran P., Rajagopal S. A scheme for detecting the types of misbehavior and identifying the attacks using reputation mechanism in a mobile ad-hoc network // Proceedings of International Conference on Communication and Electronics Systems (ICCES). 2016. P. 1-6. DOI: 10.1109/CESYS.2016.7889961
14. Basan A., Basan E., Makarevich O. Analysis of Ways to Secure Group Control for Autonomous Mobile Robots // Proceedings of 10th International Conference on Security of Information And Networks (SIN 2017). 2017. P.134-139. DOI:10.1145/3136825.3136879.
15. Basan A.S., Basan E.S., Stepenkin A.A Analiz i realizatsiya ugroz dlya sistem upravleniya mobil'nymi robotami // Materialy XIII Vserossiyskoy nauchno – prakticheskoy konferentsii: Matematicheskiye metody i informatsionno - tekhnicheskiye sredstva. 2017. [Proceedings of the XIII All-Russian Scientific and Practical Conference: Mathematical methods and information technology tools]. C.20-23.
16. Loukas G. Cyber-Physical Attacks: A Growing Invisible Threat / Imprint: Butterworth-Heinemann - Elsevier. ISBN: 978-0-12-801290-1. 2015. P. 270.
17. Dong Qi., Hayashi K., Kaneko M. Adaptive modulation and coding design for communication-based train control systems using IEEE 802.11 MAC with RTS/CT // Proceedings of IEEE 18th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC). 2017. P. 1 - 5. DOI: 10.1109/SPAWC.2017.8227786
18. Geetha K., Sreenath N. SYN flooding attack — Identification and analysis // Proceedings of International Conference on Information Communication and Embedded Systems (ICICES2014). 2014. P.1 – 7. DOI: 10.1109/ICICES.2014.7033828
19. Sargeant I., Tomlinson A. Maliciously Manipulating a Robotic Swarm // Proceedings of Int'l Conf. Embedded Systems, Cyber-physical Systems, & Applications. ESCS'16. 2016. P. 122- 128.
20. Vadavi J. V., Ashwini G. Sugavi. Detection of black hole attack in enhanced AODV protocol // Proceedings of International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN). 2017. P. 118 – 123. DOI: 10.1109/IC3TSN.2017.8284462.