УДК 004.728.3

Описательная модель процедуры распределенного управления мощностью передачи данных в сетях цифровой радиосвязи стандартов IEEE 802.11s и IEEE 802.11p

Перегудов М. А., Уманский А. Я., Жданова А. А.

Постановка задачи: *Важное практическое значение в работе сетей цифровой радиосвязи стандартов IEEE 802.11s и IEEE 802.11p имеет процедура распределенного управления мощностью передачи данных. От эффективности функционирования этой процедуры, особенно в условиях компьютерных атак, зависит не только вхождение новых абонентских терминалов в сеть, но и организация и проведение сеанса связи. Однако сегодня описательная модель процедуры распределенного управления мощностью передачи данных в сетях цифровой радиосвязи указанных стандартов, учитывающая возможные компьютерные атаки со стороны злоумышленника, отсутствует.* ***Цель работы:*** *выявление потенциально возможных компьютерных атак, эксплуатирующих уязвимости процедуры распределенного управления мощностью передачи данных в сетях цифровой радиосвязи стандартов IEEE 802.11s и IEEE 802.11p.* ***Методы:*** *системный анализ совокупности взаимосвязанных процессов процедуры.* ***Новизна:*** *в отличие от известных работ в данной работе приведены обобщенный алгоритм функционирования процедуры распределенного управления мощностью передачи данных, частные алгоритмы определения мощностей передачи данных как при разомкнутом, так и при замкнутом управлении мощностью передачи данных, а также компьютерные атаки и используемые ими уязвимости в этих алгоритмах.* ***Результат:*** *при распределенном управлении мощностью передачи данных в сетях цифровой радиосвязи стандартов IEEE 802.11s и IEEE 802.11p компьютерными атаками, потенциально способными привести к нарушению доступности информации радиосети, являются: на этапе регистрации элементов сети – передача от имени ведущего элемента сети кадра ответа на запрос ассоциации «Association Response» с отказом от ассоциации в сети цифровой радиосвязи; на этапе установления сеанса связи – передача от имени ведущего элемента сети синхронизирующего кадра «Beacon» с принудительно установленными значениями параметров мощности; на этапе проведения сеанса связи – передача от имени равноправного элемента сети кадра с ответом на запрос уровня мощности передачи «Transmission Power Control Report» с принудительно установленными значениями параметров мощности.* ***Практическая значимость:*** *результаты применимы при разработке аналитических и имитационных моделей, позволяющих осуществить оценку эффективности функционирования сетей цифровой радиосвязи в условиях компьютерных атак.*

Ключевые слова: *сеть цифровой радиосвязи, процедура, распределенное управление, разомкнутое управление, замкнутое управление, мощность передачи данных, уязвимость, компьютерная атака.*

Актуальность

На текущий момент, когда беспроводные технологии передачи данных играют незаменимую роль в жизни как отдельных людей, так и общества в це-

Библиографическая ссылка на статью:
Перегудов М. А., Уманский А. Я., Жданова А. А. Описательная модель процедуры распределенного управления мощностью передачи данных в сетях цифровой радиосвязи стандартов IEEE 802.11s и IEEE 802.11p // Системы управления, связи и безопасности. 2022. № 3. С. 90-104. DOI: 10.24412/2410-9916-2022-3-90-104.

Reference for citation:
Peregudov M. A., Umanskiy A. Ya., Zhdanova A. A. The descriptive model of the distributive transmitter power control procedure of digital radio communication networks for IEEE802.11s and IEEE802.11p standards. *Systems of Control, Communication and Security*, 2022, no. 3, pp. 90-104 (in Russian). DOI: 10.24412/2410-9916-2022-3-90-104.

лом, огромное распространение получили сети цифровой радиосвязи (СЦР) семейства стандартов IEEE 802.11 [1-4]. Оценка эффективности функционирования таких сетей имеет большое практическое значение не только на этапе их проектирования, но и на этапе эксплуатации, особенно в условиях компьютерных атак (КА) со стороны злоумышленников и применения современных технологий защиты от них [5, 6].

Сети цифровой радиосвязи семейства стандартов IEEE 802.11 имеют сложную структуру, основанную на трех нижних уровнях эталонной модели взаимодействия открытых систем (ЭМВОС): физическом, канальном и сетевом. Порядок функционирования этих сетей раскрыт в работах отечественных и зарубежных авторов [1, 7-13]. Так, в [1] предложена описательная модель канального уровня СЦР семейства стандартов IEEE 802.11, которая учитывает взаимосвязанные процедуры, отвечающие за регистрацию абонента в сети, установление и проведение его сеанса связи. В работе [7] приведено общее описание алгоритма функционирования таких сетей. В работах [8, 9] проведена оценка помехоустойчивости СЦР семейства стандартов IEEE 802.11 при воздействии помех. В работах [10-13] приведены модели отдельных процедур СЦР семейства стандартов IEEE 802.11 в условиях КА. В частности, в [10, 11] разработаны аналитические модели централизованного доступа к среде, в [12, 13] – централизованной синхронизации элементов сетей. В работах [11, 13] в качестве показателя эффективности функционирования исследуемых процедур выступает вероятность успешной передачи для централизованного доступа пользовательского кадра «*Data*», а для централизованной синхронизации – синхронизирующего кадра «***Beacon***».

В семействе стандартов IEEE 802.11 есть стандарты IEEE 802.11s и IEEE 802.11p, которые предназначены для развертывания самоорганизующихся сетей типа MANET (наземная самоорганизующаяся сеть с малоподвижными и стационарными абонентами), VANET (наземная самоорганизующаяся сеть с высокоподвижными абонентами) и FANET (воздушная самоорганизующаяся сеть с высокоподвижными абонентами). Эти стандарты в сравнении с остальными стандартами семейства имеют ряд особенностей, изложенных в [14]. Они заключаются в уникальности используемых в стандартах IEEE 802.11s и IEEE 802.11p процедур распределенной синхронизации элементов сетей и распределенного управления мощностью передачи данных.

Для количественной оценки эффективности КА злоумышленника при распределенной синхронизации элементов СЦР в [15] предложена аналитическая модель, базирующаяся на описательной модели, рассмотренной в [16]. Учет КА позволил получить новые зависимости вероятности успешной передачи синхронизирующего кадра «***Beacon***» от интенсивности и длительности таких воздействий и оценить их вклад в снижение эффективности функционирования СЦР.

В свою очередь, функционирование процедуры распределенного управления мощностью передачи данных в СЦР стандартов IEEE 802.11s и IEEE 802.11p оказывает существенное влияние как на эффективность функционирования отдельных элементов сети, так и на сеть в целом. Так, нарушение

функционирования этой процедуры влечет за собой не только снижение количества доставленных данных за счет увеличения коллизий внутри сети, но и быстрый расход энергии элементом питания (то есть аккумулятором, гальваническим элементом или их батареей) элементов сети.

Однако описательная модель процедуры распределенного управления мощностью передачи данных в сетях цифровой радиосвязи стандартов IEEE 802.11s и IEEE 802.11p, учитывающая возможные КА злоумышленника, отсутствует. Такая модель необходима для разработки программного обеспечения распределенного управления мощностью передачи данных в сетях указанных стандартов, способного в режиме реального времени обеспечить их работоспособность в условиях КА. Поэтому разработка описательной модели процедуры распределенного управления мощностью передачи данных в сетях цифровой радиосвязи стандартов IEEE 802.11s и IEEE 802.11p является актуальной задачей.

Цель работы – выявление потенциально возможных КА, эксплуатирующих уязвимости процедуры распределенного управления мощностью передачи данных в СЦР стандартов IEEE 802.11s и IEEE 802.11p. Для достижения поставленной цели необходимо разработать описательную модель этой процедуры в условиях КА, включающую описание ее общего алгоритма и алгоритмов реализации основных правил распределенного управления мощностью передачи данных.

Общее описание распределенного управления мощностью передачи данных в сетях цифровой радиосвязи стандартов IEEE 802.11s и IEEE 802.11p

Согласно спецификации [14] при распределенном управлении мощностью передачи данных в СЦР стандартов IEEE 802.11s и IEEE 802.11p информационное взаимодействие между элементами этих сетей осуществляется по правилам разомкнутого и замкнутого управления. Разомкнутое управление применяется на этапах регистрации нового элемента в сети и установления сеанса связи. При этом выделяются ведущий и ведомый элементы сети, которые осуществляют передачу данных с разной мощностью. Замкнутое управление применяется на этапе проведения сеанса связи. Все элементы сети при этом равноправны.

В СЦР стандартов IEEE 802.11 при разомкнутом управлении роль ведущего элемента передается от одного элемента другому. Элемент, передавший в канале передачи данных последним синхронизирующий кадр «***Beacon***», называется ведущим. Он выполняет роль ведущего до момента появления в канале синхронизирующего кадра «***Beacon***» от другого элемента.

На рис. 1 представлен обобщенный алгоритм распределенного управления мощностью передачи данных в СЦР стандартов IEEE 802.11s и IEEE 802.11p. Данный алгоритм заключается в следующем.

Шаг 1. Передача элементом, проходящим регистрацию в СЦР, кадра запроса ассоциации «***Association Request***» (это делается для проверки совместимости нового элемента СЦР требованиям сети) с указанием в качестве адреса

отправителя своего MAC-адреса, а в качестве адреса получателя – MAC-адреса ведущего элемента СЦР. Структура этого кадра приведена на рис. 2.

Шаг 2. Если ведущий элемент получил кадр запроса ассоциации «***Association Request***» (или кадр запроса повторной ассоциации «***Reassociation Request***»), то переходят к шагу 3, в противном случае – к шагу 1.

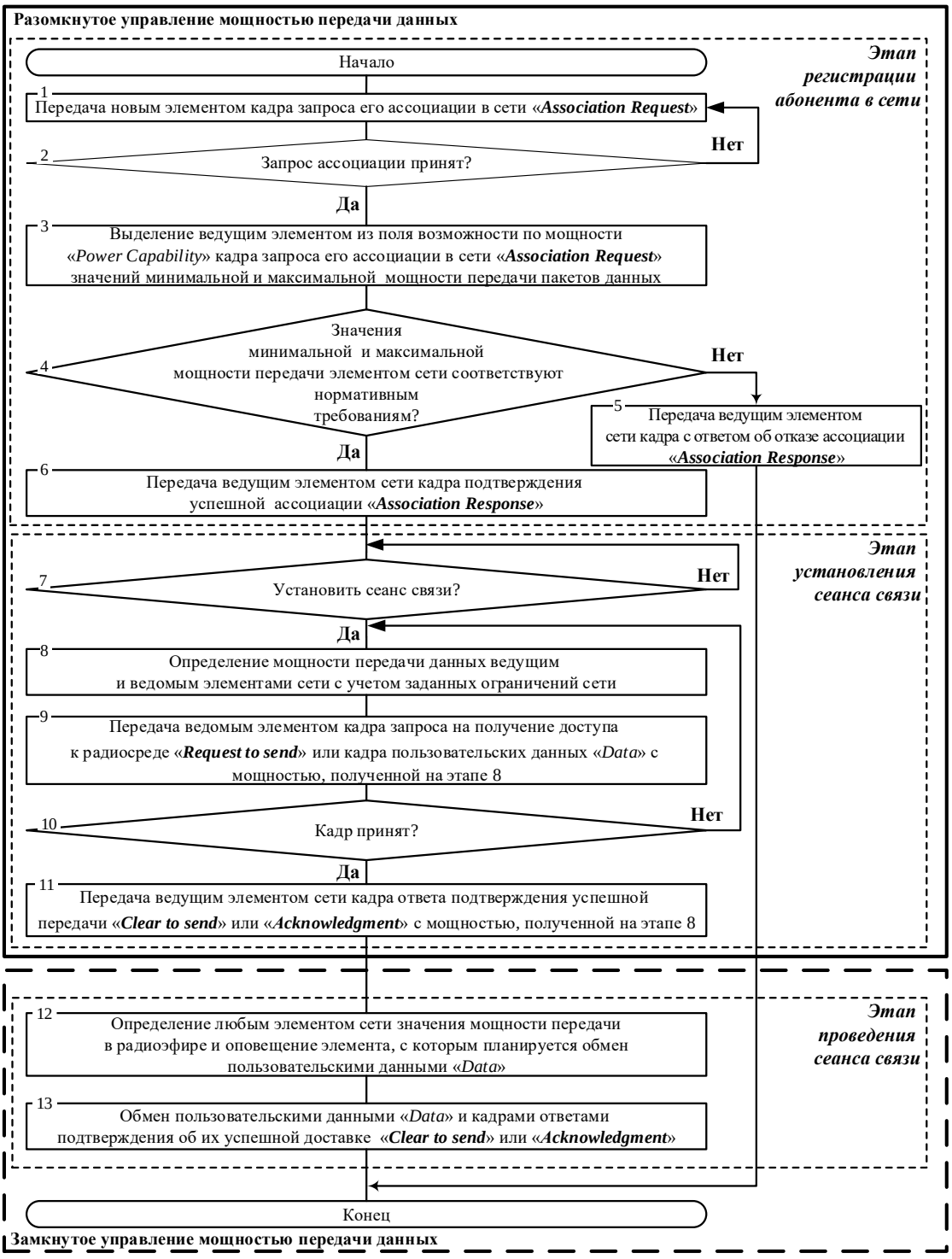

Рис. 1. Обобщенный алгоритм функционирования процедуры распределенного управления мощностью передачи данных в сетях цифровой радиосвязи стандартов IEEE 802.11s и IEEE 802.11p

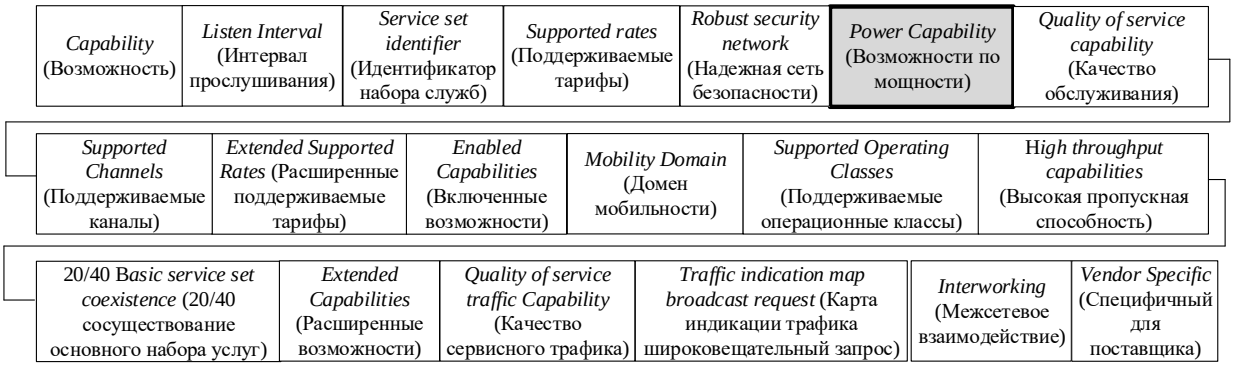

Рис. 2. Обобщенная структура кадра запроса ассоциации «***Association Request***»

Шаг 3. Считывание ведущим элементом в принятом кадре запроса ассоциации «***Association Request***» из поля возможности по мощности «*Power Capability*» значений минимальной и максимальной мощности передачи данных. Структура этого поля представлена на рис. 3.

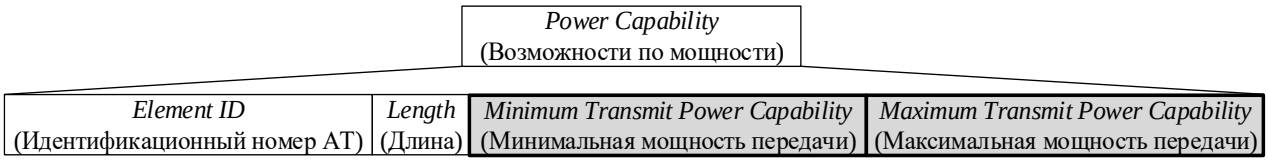

Рис. 3. Структура поля возможности по мощности «*Power Capability*» кадра запроса ассоциации «***Association Request***»

Шаг 4. Если значения минимальной и максимальной мощности передачи данных новым элементом СЦР выходят за границы разрешенных значений в сети, установленных администратором или по умолчанию в соответствии со спецификацией [14], то переходят к шагу 5, в противном случае – к шагу 6.

Шаг 5. Передача ведущим элементом кадра ответа на запрос ассоциации «***Association Response***» с отказом от ассоциации в СЦР.

Шаг 6. Передача ведущим элементом кадра ответа на запрос ассоциации «***Association Response***» с подтверждением успешной ассоциации в СЦР.

Шаг 7. Если требуется установить сеанс связи, то переходят к шагу 8, в противном случае к очередной проверке данного условия (то есть производится зацикливание до востребования).

Шаг 8. Определение ведущим и ведомым элементами СЦР мощности передачи данных с учетом разрешенных значений минимальной и максимальной мощности передачи.

Шаг 9. Передача ведомым элементом СЦР кадра запроса на получение доступа к радиосреде «***Request to send***» или кадра пользовательских данных «*Data*» с мощностью, определенной на предыдущем шаге.

Шаг 10. Если данные успешно приняты ведущим элементом СЦР, то переходят к шагу 11, в противном случае ведомый элемент повторно попытается установить сеанс связи (переходят к шагу 8).

Шаг 11. Передача ведущим элементом СЦР кадра подтверждения успешной передачи «***Clear to send***» или «***Acknowledgment***» с мощностью, полученной на шаге 8.

Шаг 12. Определение любым элементом сети значения мощности передачи данных в радиоэфире и оповещение элемента, с которым планируется обмен пользовательскими данными «*Data*».

Шаг 13. Любые элементы СЦР передают друг другу кадры пользовательских данных «*Data*» и кадры ответов подтверждения об их успешной доставке «***Clear to send***» или «***Acknowledgment***».

Разомкнутое управление мощностью реализуется как на этапе регистрации элемента, так и на этапе установления сеанса связи. Описание разомкнутого управления на этапе регистрации новых элементов приведено в обобщенном алгоритме на рис. 1. Рассмотрим далее разомкнутое управление на этапе установления сеанса связи.

На этапе установления сеанса связи при разомкнутом управлении мощностью передачи данных в СЦР стандартов IEEE 802.11s и IEEE 802.11p ведомые элементы должны осуществлять передачу данных с мощностью, меньшей или равной значению нормативной максимальной мощности передачи ($P \le P_{\max}$), а ведомые элементы – с мощностью, меньшей или равной значению локальной максимальной мощности передачи $L_{\max}$ ($L \le L_{\max}$). Алгоритм определения мощностей передачи данных ведущим и ведомым элементами в СЦР стандартов IEEE 802.11s и IEEE 802.11p на этапе установления сеанса связи показан в виде блок-схемы на рис. 4. Данный алгоритм заключается в следующем.

Шаг 1. Определение мощности передачи данных новым ведущим элементом СЦР осуществляется путем расчета фактической мощности передачи (P_0) по уровню мощности принятого синхронизирующего кадра «***Beacon***» (*RSSI*) от текущего ведущего элемента, сравнения полученного значения со значением нормативной максимальной мощности передачи ($P_{\max}$), содержащейся в данном синхронизирующем кадре «***Beacon***»:

$$P = \begin{cases} P_0, \text{ если } P_0 < P_{\max}; \\ P_{\max} \text{ в противном случае.} \end{cases} \quad (1)$$

Аналитическое выражение для определения мощности передачи данных по уровню принятого радиосигнала приведено в модели процедуры управления питанием СЦР, изложенной в [7].

После этого осуществляется установление вычисленного значения мощности передачи данных P в ведущем элементе.

Шаг 2. Передача ведущим элементом синхронизирующего кадра «***Beacon***» с установленной мощностью P.

Шаг 3. Осуществление приема синхронизирующего кадра «***Beacon***» всеми ведомыми элементами СЦР.

Рис. 4. Алгоритм определения мощностей передачи данных ведущим и ведомым элементами в сетях стандартов IEEE 802.11s и IEEE 802.11p

Шаг 4. Ведомые элементы считывают параметры полей мощность «*Power*» $P_{\max}$ и ограничение по мощности «*Capacity limit*» *S*, содержащиеся в синхронизирующем кадре «**Beacon**». Структура поля ограничение по мощности «*Capacity limit*» представлена на рис. 5.

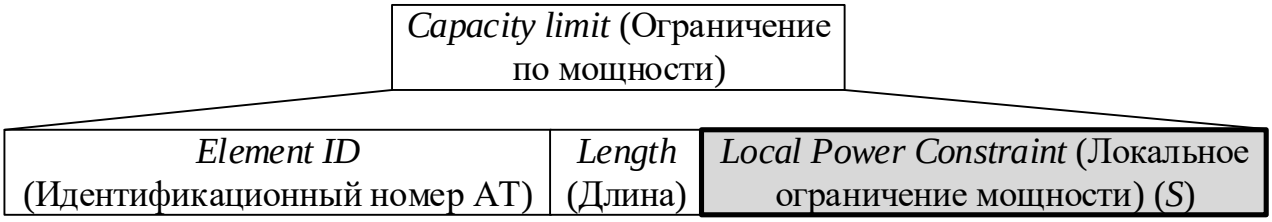

Рис. 5. Структура поля ограничение по мощности «*Capacity limit*» синхронизирующего кадра «**Beacon**»

Шаг 5. Вычисление значения локальной максимальной мощности передачи данных ведомым элементом ($L_{\max}$) по формуле

$$L_{\max} = P_{\max} - S, \tag{2}$$

где *S* – локальное ограничение мощности.

Шаг 6. Определение мощности передачи данных ведомым элементом СЦР осуществляется путем расчета фактической мощности передачи данных ведущим элементом (L_0) по уровню мощности принятого синхронизирующего

кадра «***Beacon***» (*RSSI*) от ведущего элемента, сравнения полученного значения со значением локальной максимальной мощности передачи ($L_{\max}$):

$$L = \begin{cases} L_0, \text{ если } L_0 < L_{\max}; \\ L_{\max} \text{ в противном случае.} \end{cases} \quad (3)$$

После этого осуществляется установление вычисленного значения мощности передачи данных L в ведомом элементе.

При информационном обмене между ведомым и ведущим элементами в соответствии с обобщенным алгоритмом функционирования процедуры распределенного управления мощностью передачи данных в СЦР стандартов IEEE 802.11s и IEEE 802.11p в качестве запроса на получение доступа может выступать либо первый кадр пользовательских данных «*Data*», либо кадр запроса на получение доступа к среде передачи данных «***Request to send***», либо кадр открытия начала передачи данных «***Clear to send***» [14].

Согласно спецификации [14] на этапе проведения сеанса связи при замкнутом управлении мощностью передачи данных все элементы СЦР стандартов IEEE 802.11s и IEEE 802.11p, участвующие в данной передаче, равноправны. Стоит отметить, что данный метод управления питанием заключается в том, чтобы динамически адаптировать мощность передачи данных между элементами СЦР стандартов IEEE 802.11s и IEEE 802.11p, участвующими в радиообмене. При этом алгоритм определения мощности передачи данных между двумя равноправными элементами СЦР стандартов IEEE 802.11s и IEEE 802.11p на этапе проведения сеанса связи представлен в виде блок-схемы, приведенной на рис. 6.

Рис. 6. Алгоритм определения мощности передачи данных между двумя равноправными элементами в сетях стандартов IEEE 802.11s и IEEE 802.11p

Данный алгоритм заключается в следующем.

Шаг 1. Передача кадра запроса уровня мощности передачи «***Transmit power control request***» с указанием в качестве адреса отправителя MAC-адрес элемента 1, а в качестве адреса получателя MAC-адрес элемента 2. Структура кадра запроса уровня мощности передачи «***Transmit power control request***» представлена на рис. 7.

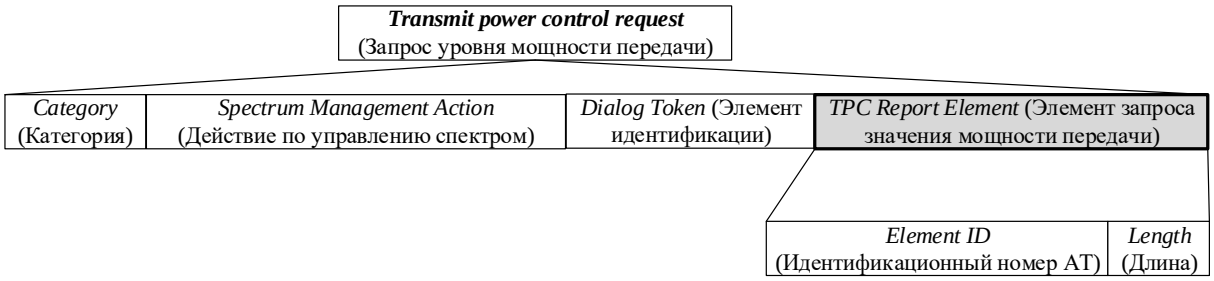

Рис. 7. Структура кадра запроса уровня мощности передачи «***Transmit power control request***»

Шаг 2. Осуществление приема элементом 2 кадра запроса уровня мощности передачи «***Transmit power control request***», отправленного элементом 1.

Шаг 3. Передача кадра ответа на запрос уровня мощности передачи «***Transmission power control report»*** с указанием в качестве адреса отправителя MAC-адрес элемента 2, а в качестве адреса получателя – MAC-адрес элемента 1. Структура кадра ответа на запрос уровня мощности передачи «***Transmission power control report»*** повторяет структуру кадра запроса уровня мощности передачи «***Transmit power control request***», за исключением поля ответа на запрос значения мощности передачи «*Transmission power control report*». Структура данного поля представлена на рис. 8.

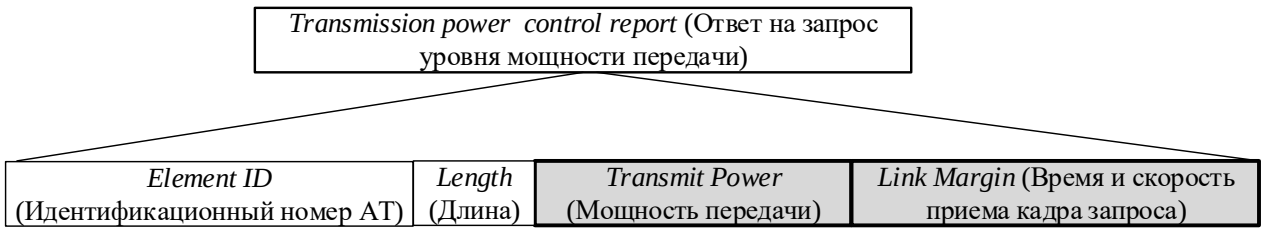

Рис. 8. Структура поля ответа на запрос значения мощности передачи «*Transmission power control report*» кадра ответа на запрос уровня мощности передачи «***Transmission power control report»***

Шаг 4. Осуществление приема элементом 1 кадра ответа на запрос уровня мощности передачи «***Transmission power control report»***, отправленного элементом 2.

Шаг 5. Считывание значения полей мощность передачи «*Transmit Power*», время и скорость приема кадра запроса «*Link Margin*», содержащихся в

кадре ответа на запрос уровня мощности передачи «***Transmission power control report»***.

Шаг 6. Определение в элементе 1 мощности передачи данных с учетом параметров, содержащихся в поле ответа на запрос уровня мощности передачи «*Transmission power control report*» кадра ответа на запрос уровня мощности передачи «***Transmission power control report***».

Таким образом, в СЦР стандартов IEEE 802.11s и IEEE 802.11p на этапах регистрации нового элемента сети и установления сеанса связи применяется разомкнутое управление мощностью передачи данных, согласно которому ведущий и ведомый элементы осуществляют передачу данных с разной мощностью. На этапе проведения сеанса связи применяется замкнутое управление мощностью передачи данных, в котором нет понятия ведущий и ведомый элементы, а все элементы сети, участвующие в радиообмене, равноправны и динамически изменяют мощность передачи данных на основании параметров, содержащихся в кадре ответа на запрос уровня мощности передачи «***Transmission power control report***».

Анализ спецификации стандарта IEEE 802.11 в части распределенного управления мощностью передачи данных позволил выявить следующие уязвимости, определяющие возможность проведения КА:

1) отсутствие шифрования служебных кадров, что определяет доступность к информации, содержащейся в полях таких кадров (MAC-адрес источника, MAC-адрес получателя, наименование радиосети и др.);
2) энергетическая доступность радиосигнала стандартов IEEE 802.11s и IEEE 802.11p при использовании в оборудовании всенаправленных антенн;
3) наличие управляющего воздействия при разомкнутом управлении мощностью передачи в виде команды отказа в ассоциации нового элемента сети (кадр ответа на запрос ассоциации «***Association Response***» с отказом от ассоциации);
4) наличие управляющих воздействий при разомкнутом и замкнутом управлении мощностью передачи данных в виде команд управляющих мощностью передачи данных (поля мощность «*Power*» и ограничение по мощности «*Capacity limit*» синхронизирующего кадра «***Beacon***» при разомкнутом управлении мощности передачи и поля мощность передачи «*Transmit Power*», время и скорость приема кадра запроса «*Link Margin*» кадра ответа на запрос уровня мощности передачи «***Transmission power control report»*** при замкнутом управлении мощностью передачи).

На основе выявленных уязвимостей и с учетом описательной модели распределенного управления мощностью передачи данных определены следующие КА:

1) при разомкнутом управлении мощностью передачи данных на этапе регистрации абонентов в сети – передача от имени ведущего элемента сети кадра ответа на запрос ассоциации «***Association response***» с отказом от ассоциации;

2) при разомкнутом управлении мощностью передачи данных на этапе установления сеанса связи – передача от имени ведущего элемента сети синхронизирующего кадра «***Beacon***» с принудительно установленными значениями параметров полей мощность «*Power*» и ограничение по мощности «*Capacity limit*»;
3) при замкнутом управлении мощностью передачи данных на этапе проведения сеанса связи – передача от имени равноправного элемента сети кадра ответа на запрос уровня мощности передачи «***Transmission power control report***» с принудительно установленными значениями в полях мощность передачи «*Transmit Power*», время и скорость приема кадра запроса «*Link Margin*».

Выводы

Разработана описательная модель процедуры распределенного управления мощностью передачи данных в сетях стандартов IEEE 802.11s и IEEE 802.11p, включающая обобщенный алгоритм функционирования такой процедуры, а также частные алгоритмы определения мощностей передачи данных как при разомкнутом управлении мощностью передачи данных для ведущего и ведомого элементов сети цифровой радиосвязи, так и при замкнутом управлении мощностью для равноправных элементов сети цифровой радиосвязи.

Установлено, что при распределенном управлении мощностью передачи данных в сетях цифровой радиосвязи стандартов IEEE 802.11s и IEEE 802.11p компьютерными атаками, потенциально способными привести к нарушению доступности информации радиосети, являются: на этапе регистрации элементов сети – передача от имени ведущего элемента сети кадра ответа на запрос ассоциации «***Association Response***» с отказом от ассоциации; на этапе установления сеанса связи – передача от имени ведущего элемента сети синхронизирующего кадра «***Beacon***» с принудительно установленными значениями параметров мощности; на этапе проведения сеанса связи – передача от имени равноправного элемента сети кадра с ответом на запрос уровня мощности передачи «***Transmission power control report***» с принудительно установленными значениями параметров мощности.

Предлагаемая описательная модель может найти применение при разработке аналитических и имитационных моделей, применяемых при оценке эффективности и оптимизации функционирования сети цифровой радиосвязи в условиях компьютерных атак со стороны злоумышленника.

Литература

1. Перегудов М. А., Стешковой А. С., Щеглов А. В. Описательная модель канального уровня сетей цифровой радиосвязи семейства стандартов IEEE 802.11 // Системы управления, связи и безопасности. 2020. № 3. С. 203-221.

2. Khorov E., Kiryanov A., Lyakhov A., Safonov A. Analytical Study of Link Management in IEEE 802.11s Mesh Networks // International Symposium on Wireless Communication Systems (ISWCS). 2012. P. 786-790.

3 Фельдман Ш., Рентюк В. В чем разница между Wi-Fi HaLow и традиционным Wi-Fi // Беспроводные технологии. 2021. № 1 (52). С. 10-13.

4. Сандал М. Л., Банков Д. В., Хоров Е. М. Сверхнадежная связь с низкой задержкой в сетях Wi-Fi на основе IEEE 802.11BA // Информационные технологии и системы: сборник трудов 42-й междисциплинарной школы-конференции ИППИ РАН (Казань, 25-30 сентября 2018 г.). – М.: ИППИ РАН, 2018. – С. 326-343.

5. Русаков А. О., Чалый Р. А. Методы защиты от атаки «человек посередине» в Wi-Fi сетях // Актуальные проблемы авиации и космонавтики. 2016. Т. 1. № 12. С. 767-769.

6. Прокопайло А. А., Дьяченко Н. В. Методы взлома и защиты Wi-Fi сетей // Реформирование и развитие естественных и технических наук: сборник материалов XII международной очно-заочной научно-практической конференции. – М.: НИЦ Империя, 2019. – С. 100-103.

7. Росс Д. Wi-Fi. Беспроводная сеть. – М.: НТ Пресс, 2007. – 320 с.

8. Титов К. Д., Липатов А. О., Завалишина О. Н. Оценка помехоустойчивости системы связи стандарта IEEE 802.11n при воздействии помех с учётом структуры пакета передаваемых данных // Теория и техника радиосвязи. 2019. № 4. С. 95-107.

9. Титов К. Д., Завалишина О. Н. Оценка помехоустойчивости системы связи стандарта IEEE 802.11ac при воздействии помех // Успехи современной радиоэлектроники. 2019. № 12. С. 191-196. doi: 10.18127/j20700784-201912-30.

10. Guan Z., Yang Z. J., He M. Energy-efficient analysis of an IEEE 802.11 PCF MAC protocol based on WLAN // Journal of Ambient Intelligence & Humanized Computing.10. 2019. P. 1727–1737.

11. Перегудов М. А., Стешковой А. С. Модель централизованно-зарезервированного доступа к среде в сетях цифровой радиосвязи // Информатика и автоматизация. 2020. Том 19. № 6. С. 1332–1356.

12. Villegas E. G., Afaqui M. S., Aguilera E. L. A novel cheater and jammer detection scheme for IEEE802.11-based wireless LANs // Computer Networks. 2015. Vol. 86. P. 40–56.

13. Перегудов М. А., Стешковой А. С. Модель централизованной синхронизации элементов сетей цифровой радиосвязи со случайным множественным доступом к среде типа CSMA/CA // Труды СПИИРАН. 2020. Том 19. № 1. С. 128–154. doi: 10.15622/sp.2020.19.1.5.

14. IEEE Standard for Information technology – Telecommunications and information exchange between systems Local and metropolitan area networks – Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. – IEEE Std 802.11, 2020. – 4379 с.

15. Перегудов М. А., Уманский А. Я., Стешковой А. С. Оценка эффективности процедуры распределенной синхронизации элементов сети цифровой радиосвязи в условиях деструктивных воздействий // Системы управления, связи и безопасности. 2021. № 1. С. 126-151.

16. Перегудов М. А., Уманский А. Я., Храмов В. Ю., Фокин А. О. Описательная модель распределенной синхронизации элементов сетей

цифровой радиосвязи стандартов IEEE 802.11s и IEEE 802.11p // Успехи современной радиоэлектроники. 2021. Том 75. № 4. С. 21-31.

References

1. Peregudov M. A., Steshkovoy A. S., Shcheglov A. V. Descriptive model of the channel layer of digital radio communication networks of the IEEE 802.11 family of standards. *Systems of Control, Communication and Security*, 2020, no. 3, pp. 203-221 (in Russian).

2. Khorov E., Kiryanov A., Lyakhov A., Safonov A. Analytical Study of Link Management in IEEE 802.11s Mesh Networks. *International Symposium on Wireless Communication Systems (ISWCS)*, 2012, pp. 786-790.

3. Feldman Sh., Rentuok V. V chem raznitsa mezhdu Wi-Fi HaLow i traditsionnym Wi-Fi [What is the difference between Wi-Fi HaLow and traditional Wi-Fi]. *Besprovodnye tekhnologii*, 2021, no 1 (52), pp. 10-13 (in Russian).

4. Sandal M. L., Bankov D. V., Chorov E. M. Sverkhnadezhnaia sviaz' s nizkoi zaderzhkoi v setiakh Wi-Fi na osnove IEEE 802.11BA [Extremely reliable, low latency Wi-Fi connection based on IEEE 802.11BA]. *Informatsionnye tekhnologii i sistemy: sbornik trudov 42-i mezhdistsiplinarnoi shkoly-konferentsii IPPI RAN* [Information Technology and Systems Information Technologies and Systems: Proceedings of the 42nd Interdisciplinary School-Conference IPPI RAN]. Moscow, Institute for Information Transmission Problems of the Russian Academy of Sciences (Kharkevich Institute), 2018, pp. 326-343 (in Russian).

5. Rusakov A. O., Chaly R. A. Methods of protection against «man in the middle» attacks in Wi-Fi networks. *Aktualnye problemy aviatsii i kosmonavtiki*, 2016, vol. 1, no. 12, pp. 767-769 (in Russian).

6. Prokopaylo A. A., Dyachenko N. V. Metody vzloma i zashchity Wi-Fi setei [Methods of hacking and protection of Wi-Fi networks]. *Reformirovanie i razvitie estestvennykh i tekhnicheskikh nauk: sbornik materialov XII mezhdunarodnoi ochno-zaochnoi nauchno-prakticheskoi konferentsii* [Reform and Development of Natural and Technical Sciences: Proceedings of the XII International In-house Scientific and Practical Conference]. Moscow, 2019, pp 100-103 (in Russian).

7. Ross D. *Wi-Fi. Besprovodnaia set'* [Wi-Fi. Wireless network]. Moscow, NT-Press Publ, 2007, 320 p (in Russian).

8. Titov K. D., Lipatov A. O., Zavalishina O. N. Assessment of noise immunity of IEEE 802.11n communication system in cause of intentional interference taking into account the structure of the transmitted data packet. *Radio Communication Theory and Equipment*, 2019, no. 4, pp. 95-107 (in Russian).

9. Titov K. D., Zavalishina O. N. Assessment of the noise immunity of standard data transmissions IEEE 802.11ac under the interference of interference. *Uspekhi sovremennoi radioelektroniki*, 2019, no. 12, pp. 191-196 (in Russian). doi: 10.18127/j20700784-201912-30.

10. Guan Z., Yang Z. J., He M. Energy-efficient analysis of an IEEE 802.11 PCF MAC protocol based on WLAN. *Journal of Ambient Intelligence & Humanized Computing*, 2019, no. 10, pp. 1727–1737.

11. Peregudov M. A., Steshkovoy A. S. Model of centrally reserved access to the environment in digital radio networks of the IEEE 802.11 family of standards. *Computer Science and Automation*, 2020, vol. 19, no. 6, pp. 1332-1356 (in Russian). doi: 10.15622/ia.2020.19.6.8.

12. Villegas E. G., Afaqui M. S., Aguilera E. L. A novel cheater and jammer detection scheme for IEEE802.11-based wireless LANs. *Computer Networks*, 2015, vol. 86, pp. 40–56.

13. Peregudov M. A., Steshkovoy A. S. Digital radio networks centralized elements synchronization model with random multiple access to the CSMA/CA type medium. *SPIIRAS Proceedings*, 2020, vol. 19, no. 1, pp. 128-154 (in Russian). doi: 10.15622/sp.2020.19.1.5.

14. IEEE Standard for Information technology – Telecommunications and information exchange between systems Local and metropolitan area networks – Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Std 802.11, 2020. 4379 p.

15. Peregudov M. A., Umanskiy A. Ya., Steshkovoy A. S. Estimation of the distributed synchronization effectiveness of digital radio network elements in destructive influence conditions. *Systems of Control, Communication and Security*, 2021, no. 1, pp. 126-151 (in Russian). doi: 10.24411/2410-9916-2021-10106.

16. Peregudov M. A., Umanskiy A. Ya., Hramov V. Yu., Fokin A. O. Descriptive model of distributed synchronization of elements of digital radio communication networks of IEEE 802.11s and IEEE 802.11p standards. *Uspekhi sovremennoi radioelektroniki*, 2021, vol. 75, no. 4, pp. 21-31 (in Russian).

Статья поступила 20 июня 2022 г.

Информация об авторах

Перегудов Максим Анатольевич — кандидат технических наук. Докторант. Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж). Область научных интересов: защита информации, моделирование сетей связи. E-mail: maxaperegudov@mail.ru

Уманский Аркадий Янович — старший научный сотрудник. Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж). Область научных интересов: оценка эффективности функционирования сети цифровой радиосвязи. E-mail: smyle2015@mail.ru

Жданова Александра Андреевна — младший научный сотрудник. Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж). Область научных интересов: оценка эффективности функционирования сети цифровой радиосвязи. E-mail: zhdalexandra48@mail.ru

Адрес: 394064, Россия, г. Воронеж, ул. Ст. Большевиков, д. 54А.

The descriptive model of the distributive transmitter power control procedure of digital radio communication networks for IEEE802.11s and IEEE802.11p standards

M. A. Peregudov, A. Ya. Umanskiy, A. A. Zhdanova

Problem Statement *An important practical role in the operation of the digital radio communication networks of IEEE 802.11s and IEEE 802.11p standards is the distributive transmitter power control procedure. The effective functioning of this procedure especially in the context of computer attacks, depends not only on the entry of new subscriber terminals into the network, but also on the organization and conduct of a communication session. Today, however, there is no descriptive model of the distributive transmitter power control procedure of digital radio communication networks of these standards, taking into account possible computer attacks by the attacker.* ***The goal of the paper*** *is to detection of potential computer attacks exploiting the vulnerability of distributed transmitter power control procedure in IEEE 802.11s and IEEE 802.11p digital radio communication networks.* ***Methods.*** *System analysis of a set of interrelated process procedures.* ***Novelty.*** *In contrast to the well-known works in this paper a generalized algorithm of functioning of is the distributive transmitter power control procedure, private rhythms of determination of transmit power as at opened loop, and in the case of closed loop of power control, as well as computer attacks and vulnerabilities of these algorithms used by them.* ***Result.*** *In case of distributive transmitter power control procedure in the digital radio communication networks of IEEE 802.11s and IEEE 802.11p standards, computer attacks with the potential to potentially disrupt the availability of radio network information are: at the stage of registration network element – transmission of the frame response to the «**Association Response**» association's request on behalf of the network's leading element; at the stage of establishing the communication session – transmission of a synchronization frame on behalf of the network's leading element «**Beacon**» with the power parameters set by force; at the stage of the communication session – transfer of a frame on behalf of an equal element of the network with response to the request of the transmission power level «**Transmission power control report**» with power settings enforced.* ***Practical relevance.*** *The results are applicable to the development of analytical and simulation models that allow the assessment of assessment of the effectiveness of digital radio communication networks in the context of computer attacks.*

Key words: *digital radio communication network, procedure, distributed control, opened loop power control, closed loop power control, transmit power, vulnerability, computer attack.*

Information about Authors

Maksim Anatol'evich Peregudov – Ph.D. of Engineering Sciences. Doctoral student. Zhukovsky – Gagarin Military Aviation Academy. Field of research: information security, modeling of radio network. E-mail: maxaperegudov@mail.ru

Arkadiy YAnovich Umanskiy – Senior Research Officer. Zhukovsky – Gagarin Military Aviation Academy. Field of research: digital radio communication networks functioning efficiency evaluation. E-mail: smyle2015@mail.ru

Alexandra Andreevna Zhdanova – Research Assistant. Zhukovsky – Gagarin Military Aviation Academy. Field of research: digital radio communication networks functioning efficiency evaluation. E-mail: zhdalexandra48@mail.ru

Address: Russia, 394064, Voronezh, Old Bolsheviks Street, 54A.