Информационные процессы, Том 20, № 3, 2020, стр. 231–253

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Вопросы обеспечения безопасности интернета транспортных средств. Обзор исследований[1]

О.Д. Соколова, В.В. Шахов

Институт вычислительной математики и математической геофизики СО РАН, Новосибирск

Поступила в редколлегию 01.09.2020

Аннотация—Развитие и распространение технологий Интернета транспортных средств несут не только огромную выгоду пользователям, но и серьезные риски, обусловленные угрозами информационной безопасности. Проблема обеспечения безопасности Интернета в интеллектуальных транспортных системах является очень актуальной, исследования проводятся во всем мире. В данной статье представлен обзор результатов, опубликованных в последние два десятилетия, рассмотрены угрозы нарушения конфиденциальности, целостности, доступности информации. Показано, что используемые средства защиты применяются на каждом из трех уровней периметра безопасности: предотвращение атак, обнаружение атак и противодействие атакам. Основная цель обзора — дать представление о типовых подходах, используемых при решении задачи обеспечения безопасности Интернета транспортных средств (кластеризация узлов, использование придорожного оборудования и др.).

КЛЮЧЕВЫЕ СЛОВА: интернет транспортных средств, информационная безопасность, стандарт IEEE 802.11p, системы обнаружение вторжений.

1. ВВЕДЕНИЕ

В настоящее время тематике Интернета вещей (Internet of Things, IoT) уделяется огромное внимание во всем мире, технологии IoT проникают во все сферы человеческой жизнедеятельности. Воплощение парадигмы Интернета вещей (IoT) на транспорте привело к эволюции сетей VANET(Vehicle ad hoc networks) в Интернет транспортных средств (Internet of Vehicles, IoV) [1]. В рамках концепции IoV автомобиль рассматривается как интеллектуальный объект, оснащенный разнообразными устройствами, которые обмениваются данными друг с другом, с устройствами других автомобилей, а также с любыми другими объектами, включая придорожную инфраструктуру. Внедрение интеллектуальных транспортных сетей значительно повысит безопасность дорожного движения и качество информационно-развлекательных услуг, предоставляемых автовладельцам, а также поспособствует мониторингу окружающей среды и решению ряда экологических проблем. Рынок технологий IoV имеет огромный потенциал. По оценкам консалтинговой компании NavigantResearch, количество транспортных средств во всем мире уже превышает 1 миллиард, а к 2035 году достигнет 2 миллиардов. При этом проблемы надежности и защиты передачи данных в сетях IoV становятся критически важными, поскольку IoV наследует уязвимости VANET (Vehicle ad hoc networks) и беспроводных сетей в целом. В IoV присутствуют коммуникации не только между транспортными средствами (vehicle-to-vehicle, V2V), автомобиль может взаимодействовать с любыми объектами, способными оказать на него влияние, что расширяет возможности как нарушения, так и

[1] Работа выполнена при поддержке гранта РФФИ № 19-17-50144 Экспансия. The reported study was funded by RFBR, project number 19-17-50144.

обеспечения информационной безопасности. Исследования в области безопасности интеллектуальных транспортных систем проводятся во всем мире [2–6], актуальность их несомненна, и данная статья посвящена обзору публикаций на эту тему.

В обзоре рассматриваются угрозы IoV, соответствующие трем основным категориям информационной безопасности — конфиденциальность, целостность, доступность. В отличие от недавно опубликованных обзоров по безопасности IoV [7–8], в статье угрозы характеризуются в соответствии с моделью информационной безопасности, называемой триадой CIA (Confidentiality, Integrity, Availability), поскольку она является наиболее признанной международным профессиональным сообществом [9–11]. При подготовке обзора авторы стремились не только проанализировать публикации, имеющие отношение к той или иной проблеме информационной безопасности, но и дать представление об инструментарии, используемом при решении задачи обеспечения безопасности IoV, в частности, рассмотреть некоторые математические модели. В обзоре показано, что средства защиты, используемые в сетях IoV, применяются на каждом из трех уровней периметра безопасности: предотвращение атак, обнаружение атак и противодействие атакам. В настоящее время многие исследователи, занимающиеся проблемами безопасности IoT, подчеркивают важность второй линии защиты, поскольку невозможно предотвратить постоянно совершенствующиеся методы информационных разрушающих воздействий и появление принципиально новых атак. От успеха систем обнаружения вторжений (IDS, Intrusion Detection System) зависит выбор и эффективность средств подавления атак. Аналогичная ситуация наблюдается и в IoV. В обзоре рассматриваются идеи, лежащие в основе разработки таких систем, предназначенных для IoV. При выборе публикаций, где рассматриваются вопросы организации превентивных мер и противодействия атакам, предпочтения также отдавались тем статьям, где присутствуют характерные особенности IoV. Например, кластеризация сетевых узлов и использование придорожного оборудования при распространении сообщений позволяют не только повысить производительность сети, но и смягчить последствия некоторых атак.

Оставшаяся часть статьи организована следующим образом. В разделе 2 приводится описание атак в сетях IoV. В разделе 3 рассматриваются методы обнаружения атак. В разделе 4 излагаются меры, принимаемые для предотвращения атак или затруднения их реализации, а также подходы, используемые для противодействия атакам. Краткие выводы сделаны в разделе 5.

2. ОБЗОР АТАК В СЕТЯХ

2.1. Преднамеренное создание помех

Описание атаки преднамеренное создание помех

DoS атака, осуществляемая путем генерации помех, является типовой для любых беспроводных сетей, в том числе и для технологий IoV [12]. Преднамеренно созданные помехи (ПСП, jamming) могут использоваться и для воздействия на приемник, т.е. искажается принимаемый радиосигнал, и для воздействия на передатчик, т.е. предотвращается передача сигнала. В публикациях обычно выделяют следующие профили атакующего с применением ПСП:

– Постановщик постоянных помех (constant jammer) непрерывно генерирует радиосигналы, не соблюдая какой-либо MAC-протокол. Сигналы являются случайным набором бит. Помехи используются для поддержания занятости беспроводных каналов, тем самым создаются препятствие и для доступа к ним, и для повреждения уже передаваемых пакетов. Злоумышленник может использовать как специализированное оборудование для атаки, генераторы сигналов, так и обычные беспроводные устройства.

– Ложный передатчик (deceptive jammer) следует протоколам множественного доступа к среде и использует их уязвимость для реализации атаки, побуждая узлы оставаться в состоянии приема, даже если у них есть свои пакеты для отправки. Вместо случайных бит без остановки отправляются обычные пакеты с корректными заголовками. Либо непрерывно транслируется преамбула, извещающая узлы о намерении начать передачу пакетов. В соответствии с некоторыми протоколами (например, B-MAC, S-MAK [13]), если узел обнаружил преамбулу, то он ожидает начала передачи данных, и не может переключиться в состояние отправки пакетов. Таким образом, фальшивая преамбула может побуждать атакуемые узлы оставаться в режиме приема сколь угодно долго.
– Постановщик случайных помех (random jammer) после осуществления атаки перестает передавать радиосигналы, переходит в "спящий" режим на некоторое случайное время, после чего повторяет атаку, продолжительность которой может быть также случайна. При этом атакующий может действовать в соответствии с любым из рассмотренных выше профилей. При данном виде ПСП злоумышленник может использовать различные стратегии энергосбережения, что важно при использовании атакующим автономного источника энергии. Когда промежутки между атакующими воздействиями детерминированы, говорят о периодических ПСП (periodic jamming).
– Оперативно реагирующий постановщик помех (reactive jammer) прослушивает радиоканал и остается пассивным, если радиоканал не используется. Генерация помех осуществляется только при обнаружении передачи пакетов. В этом принципиальное отличие данного способа атаки от рассмотренных выше случаев, когда генерация помех (ниже будем называть их реактивными) не зависит от сетевого трафика. Данный вид ПСП обнаружить наиболее трудно, кроме того, атака может быть очень эффективной при весьма скромных энергозатратах атакующего.

Применительно к сетям VANET обычно рассматривают все перечисленные выше способы ПСП, однако в основном усилия исследователей фокусируются на реактивных помехах, поскольку они наиболее предпочтительны для злоумышленника по указанным выше причинам. Учет специфики данных сетей отражается следующим образом. Исследователи рассматривают мобильные постановщики помех (mobile jammer), а также воздействие ПСП на служебные сигналы обеспечения безопасного движения. В статье [14] рассматривается транспортное средство, оснащенное генератором постоянных помех, в качестве которого может выступать, например, устройство Bluetooth. Злоумышленник может перемещаться случайным образом или по определенному шаблону, атакуя мобильные сетевые узлы в непосредственной близости. В статье [15] рассматривается атака с использование ПСП, когда злоумышленник целенаправленно атакует головной узел, управляющий информационным обменом организованной группы машин. В [16] постановщик помех смонтирован на беспилотном летательном аппарате, целью разрушающего воздействия является нарушение работы системы адаптивного круиз-контроля автомобиля.

Математические модели атаки ПСП

В качестве оценки ущерба атаки ПСП авторы часто рассматривают отношение числа успешно доставленных пакетов к общему числу отправленных пакетов, т.е. доля доставленных пакетов (PDR, packets delivery ratio [17–19]).

Авторы статьи [17] используют двумерную Марковскую цепь с непрерывным временем для моделирования приема и передачи пакетов одним мобильным сетевым узлом в условиях атаки Jamming. Состояния цепи описываются двумя неотрицательными целыми числами: количество неповрежденных пакетов (i) и количество поврежденных пакетов (j). Пакеты поступают в буфер ограниченного объема размера K. Таким образом, $0 \leq i + j \leq K$. Рассматривается

атака, когда на узлы одновременно оказывают воздействие два типа атакующих: постановщик постоянных помех и оперативно-реагирующий постановщик помех. Потоки событий, ведущих к изменению состояний (i, j), предполагаются пуассоновскими. Приведем обозначения для интенсивностей указанных потоков. Новые пакеты поступают в буфер с интенсивностью λ, они предполагается неповрежденными. Обслуживаются неповрежденные и поврежденные пакеты с интенсивностями μ и β соответственно. Предполагается, что постоянные помехи воздействуют на узел с интенсивностью α, переводя неповрежденные пакеты в поврежденные. Реактивные помехи уменьшают количество неповрежденных пакетов с интенсивностью ε, не затрагивая поврежденные пакеты. На рисунке 1 указан фрагмент диаграммы состояний соответствующей Марковской цепи, при условии, что $i > 0$, $j > 0$, $i + j < K$.

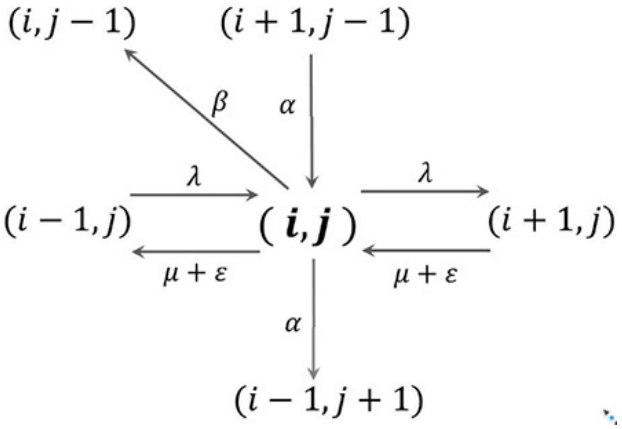

Рис. 1. Фрагмент диаграммы состояний Марковской цепи, используемой для моделирования атаки Jamming.

Систему линейных уравнений для вероятностей состояний в установившемся режиме авторы решают численно, с использованием метода Гаусса–Зейделя. Далее, указано, что полученное решение используются для оценки математического ожидания показателей эффективности атаки. Несмотря на то, что аппарат Марковских процессов часто используется для количественного анализа сетей в различных ситуациях, включая вопросы обеспечения безопасности [20], предоставляя разумную идеализацию исследуемых объектов, в данном случае, на наш взгляд, предложенная модель содержит следующие неоправданные предположения. ПСП действуют на пакеты в буфере, независимо от сеансов приема-передачи. Реактивные помехи используются при передаче данных атакованным узлом, но не используются при приеме. Кроме того, отсутствует описание использования вероятностей состояний для оценки ущерба — не ясно, каким образом можно раздельно учитывать корректно обслуженные пакеты и пакеты, утраченные под воздействием реактивных помех.

Функция плотности распределения PDR для атакованного узла выводится в [18]. Рассматриваются постоянные, случайные и реактивные ПСП. Авторы отмечают, что принимают во внимание особенности физического и канального уровней стандартов IEEE 802.11p [21] и IEEE 1609 [22, 23]. Так, в качестве показателя качества приема сигнала выступает отношению мощности полезного сигнала к мощности шума, включающего интерференцию, $SINR$ (signal-to-interference-plus-noise ratio). Для сигнала, передаваемого автомобилем i, авторы определяют $SINR_i$ следующим образом:

$$SINR_i = \frac{P_{r_i}}{\sum_{j \in TX,\, j \neq i} P_{r_j} + I + Noise + \delta P_A},$$

где P_{r_i} — мощность принимаемого сигнала от передатчика автомобиля i, P_A — мощность ПСП, $\delta \in \{0,1\}$ — индикатор наличия атаки, TX — множество автомобилей с параллельно работающими передатчиками, $\sum_{j \in TX,\, j \neq i} P_{r_j} + I$ — мощность других (мешающих) сигналов, $Noise$ — случайный шум.

Показатель $SINR$ сравнивается с некоторым пороговым значением $SINR_{th}$, величину которого предлагается вычислять экспериментально [24] или аналитически [25]. Если $SINR \geq SINR_{th}$, то сигнал от машины i считается успешно принятым. Вероятность соответствующего события учитывается при выводе функции плотности распределения PDR. Для того чтобы более детально учесть особенности рассматриваемой системы, предлагается использовать подходящие модели потерь при распространении радиосигнала и вероятностные законы распределения транспортных средств. В статье приводится пример следующей модели, активно используемой в исследованиях атаки ПСП [26–28]:

$$P_{r_i} = d_i^{-z} P_{t_i},$$

где P_{t_i} — мощность передатчика, d_i — расстояние до передатчика, z — коэффициент, затухания сигнала, зависящий от среды. Также предполагается, что количество потенциально интерферирующих передатчиков распределено по закону Пуассона.

Принимая во внимание особенности уровня управления доступом к среде (MAC, Medium Access Control) авторы рассматривают не только атакующее воздействие ПСП на контрольный канал, но и коллизии легитимных сигнальных пакетов (beacon). При этом используют следующие предположения. Каждое из n соседних транспортных средств в каждом окне связи, разделенном на w слотов, с равной вероятностью выбирает один слот для передачи одного сигнального пакета. Слот успешно использован для передачи, если он выбран ровно одним автомобилем. Если два и более пакета передается в одном слоте, то возникает коллизия, и пакеты теряются. Таким образом, в отсутствии ПСП каждый из w слотов может быть незанятым, успешным или неудачным. Атакующий с заданной вероятностью повреждает каждый слот, и если помехи приходятся на слот, в котором возникли коллизии, то они вреда не наносят. Далее авторы предлагают рекурсивный способ вычисления функции плотности распределения для показателя PDR. При этом используется вероятность события, состоящего в том, что отдельный слот выбран ровно x автомобилями:

$$P(w,n,x) = \binom{n}{x} \left(\frac{1}{w}\right)^x \left(1 - \frac{1}{w}\right)^{n-x}.$$

К сожалению, при вычислении статистики по всем w слотам, авторы ошибочно используют указанное биноминальное распределение, что имело бы место, если бы каждый из n автомобилей передавал в каждом слоте сигнальный пакет с вероятностью $w-1$ независимо от других обстоятельств, с теоретической возможностью передачи в рассматриваемом окне w пакетов (или ни одного). В случае схемы, указанной авторами, необходимо вести речь о векторе размещения сигнальных пакетов по w слотам, $(x_1, x_2, \ldots, x_w)$, элементы которого связаны соотношением:

$$\sum_{i=0}^{w} x_i = n.$$

Вероятность реализации набора $(x_1, x_2, \ldots, x_w)$ следующая:

$$P(w,n,x_1,x_2,\ldots,x_w) = \frac{n!}{w^n x_1! x_2! \ldots x_w!}.$$

Результаты экспериментального исследования и моделирования атак с использованием радиопомех в автомобильных сетях приводятся в серии работ [19, 29–30]. Авторы выполнили тщательную экспериментальную оценку производительности устройств IEEE 802.11p под воздействием ПСП, рассматривая постоянные, периодические и реактивные помехи. В результате идентифицированы процессы, на которые преднамеренные помехи влияют в большей степени, а именно: обнаружение ложного сигнала, инициируемого преамбулой, и переполнение динамического диапазона на аналого-цифровом преобразователе. Предложена методика использования характеристик производительности в лабораторных условиях атакуемого приемо-передатчика для прогнозирования качества связи двух автомобилей. Отмечено высокое соответствие между прогнозируемыми и измеренными характеристиками в полевых условиях. Также авторы оценивали влияние различных радиочастотных помех на организованную группу транспортных средств. Показано, что любая из рассмотренных атак ПСП может эффективно нарушить передачу внутри группы на большой территории. Особую тревогу вызывают размеры зоны каскадных отключений связи, вызванной постоянными и периодическими помехами, которые могут охватывать более 400 м в условиях открытой местности. Авторы выполнили подробное исследование влияния постоянных, периодических и реактивных помех на устройства, поддерживающие стандарт IEEE 802.11p. В качестве приемника и передатчика использовались устройства NEC Link bird 802.11p [31], которые являются эталонными реализациями стандарта и часто используются в экспериментах с технологиями IoV [32–36]. Для реализации различных профилей постановщика помех использовалась платформа WARP (Wireless Open-Access Research Platform), находящаяся в свободном доступе [37], используемая рядом университетов для организации лабораторных работ в курсах по технологиям беспроводной связи. В результате идентифицированы наиболее уязвимые для ПСП элементы протокола, к которым, например, относится преамбула, используемая для обнаружения сигнала, оценки смещения частоты, синхронизации часов отправителей и получателей, оценки состояния канала и т.д. Показано, что периодические ПСП могут серьезно нарушить связь, даже если мощность полезного сигнала значительно выше мощности помех (до 56 дБ). Для оценки влияния ПСП на связь VANET в общих условиях предложен метод, где в качестве входных данных используются результаты лабораторных экспериментов для определения зависимости PDR от SINR, а также положения передатчика, приемника и постановщика помех, модели распространения радиосигнала, зависящие от конкретной среды. Метод включает следующие шаги:

1. Определение расстояний от легитимного передатчика и постановщика помех до приемника.
2. Вычисление значений мощности получаемого сигнала от передатчика (P_T) и постановщика помех (P_J) по формуле:

$$P_i = \frac{P_{i,T} G_T G_R}{z}, \quad i \in \{T, J\},$$

   где G_T и G_R — коэффициенты усиления антенны передатчика (или постановщика помех) и приемника, z — коэффициент затухания сигнала, значение которого определяется согласно заданной модели распространения сигнала, $P_{i,T}$ — мощность передаваемого сигнала.
3. Вычисление $SINR$:

$$10 \log_{10} \frac{P_T}{P_J + Noise}.$$

4. Оценка PDR в соответствии с результатами лабораторных экспериментов.

Для противодействия атакам ПСП на канал управления в интеллектуальных автомобильных сетях предложен механизм кооперативной ретрансляции сигналов, использующий пространственное разнесение транспортных средств для повышения отказоустойчивости связи

[38]. Авторы рассматривают сегмент дороги, часть которого подвержена атаке ПСП. Согласно сделанным предположениям, количество атакованных машин и количество ретранслирующих узлов распределены в соответствии с законом Пуассона. Сформулирована оптимизационная задача выбора ретранслятора реле max-min, которая пытается максимизировать отношение сигнал / шум, минимальное для атакованных транспортных средств при ограничении на количество ретрансляторов.

$$\max \min_{v_j \in V} \sum_{v_i \in R} x_i \widehat{P}_i H_{i,j}$$
$$\sum_{v_i \in R} x_i \leq K, \quad \forall v_j \in V,$$
$$x_i \in \{0, 1\}, \forall v_i \in R,$$

где $\widehat{P}_i$ — нормализованная мощность передачи ретранслятора v_i, $H_{i,j}$ — коэффициенты усиления канала между ретранслятором i и атакованным узлом j, x_i — индикатор, показывающий, выбрано транспортное средство в качестве ретранслятора или нет, K — максимально разрешенное количество транзитных узлов, V — множество атакованных узлов, R — множество ретрансляторов. Для решения задачи предложен эвристический алгоритм с трудоемкостью, линейно зависящей от числа кандидатов в транзитные узлы.

2.2. Атака Blackhole

Атака Blackhole представляет серьезную угрозу для IoV [39]. Обычно протоколы маршрутизации, используемые в VANET, реагируют на изменения в сети и оперативно изменяют маршруты продвижения пакетов в соответствии с некоторыми критериями (уменьшается время задержки, увеличивается пропускная способность и т.п.). Злоумышленник использует данную уязвимость и информирует окружение о том, что его выбор в качестве промежуточного узла улучшает критерий, используемый для построения маршрутов. Например, если в качестве критерия используется число хопов (т.е. промежуточных узлов) от отправителя к получателю, то атакующий представляет себя как узел с кратчайшим путем к узлу назначения. В результате весь трафик от узлов в некоторой области попадает к злоумышленнику и отбраковывается.

Проиллюстрируем данную ситуацию на примере (рис. 2). Узлом назначения для пакетов, передаваемых транспортными средствами, является модуль придорожной инфраструктуры (Road Side Unit, RSU). Сплошным черным цветом отмечен организатор атаки, который информирует соседние транспортные средства (узлы 1 и 2) о том, что им установлено непосредственное соединение с RSU. Узлы 1 и 2 полагают, что теперь между ними и узлом назначения находится всего один узел, о чем они информируют свое окружение, и передают пакеты напрямую злоумышленнику, который их отбраковывает. Сплошными стрелками показаны маршруты при наличии атаки, пунктирными — изменения, которые были бы в отсутствии атаки. Некоторые узлы не попали под воздействие атаки. Например, изначально узел 3 находился в двух хопах от RSU. Переключение на узел 2 не улучшит ситуацию, маршрут для данного узла не изменился. Узел 4, как и раньше, передает пакеты через узел 1, однако теперь они не доходят до получателя. Также под действие атаки попал узел 5, переключившись на узел 2, полагая, что теперь находится в двух хопах от RSU.

Для маскировки атаки могут отбраковываться не все пакеты, случайно выбранные пакеты будут доставлены по назначению, кроме того, атакующий, используя мощный передатчик, может передавать их непосредственно в узел назначения. Такая разновидность атаки называется GreyHoles. Отметим, что некоторые авторы отождествляют атаку Sinkhole (воронка) и атаку

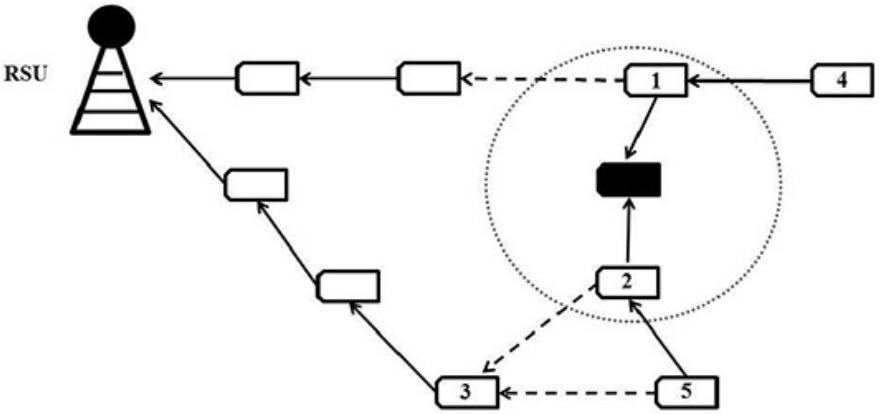

Рис. 2. Пример действия атаки Blackhole.

Blackhole, называют указанные термины синонимами [40]. Другие отмечают, что при атаке Sinkhole атакующий узел также замыкает трафик на себя, но в отличие от атаки Blackhole в данном случае пакеты не отбраковываются [41].

Атаке Blackhole подвержены как проактивные протоколы маршрутизации (когда маршруты выбираются на основе периодически обновляемых таблиц, содержащих информацию о соседних узлах, достижимых узлах, и количестве транзитных узлов до них), так и реактивные протоколы маршрутизации (т.е. процесс построения маршрута до адресата пакета запускается по требованию отправителя). В атаке может быть задействовано несколько узлов как для расширения атакуемого сегмента сети, так и с целью кооперативного противодействия механизмам защиты [42].

В статье [43] авторы исследуют уязвимость двух протоколов маршрутизации, разработанных с учетом требований обеспечения безопасности SAODV (Secure Ad hoc On-Demand Distance Vector) [44] и ARAN (Authenticated Routing for Ad hoc Network) [45]. Протоколы содержат механизмы аутентификации и целостности сообщений, основанные на криптографии с открытым ключом. В общем виде схема маршрутизации предполагается следующей. Когда узел должен отправить пакет другому узлу, он инициирует процесс, начинает процесс поиска маршрута к узлу назначения, отправляя соседним узлам сообщение RREQ (route request message) с запросом маршрута. Соседние узлы получают запрос, увеличивают счетчик транзитных узлов и пересылают сообщение своим соседям, т.е. фактически пакеты RREQ передаются с использованием широковещательного подхода. В конечном итоге сообщение RREQ достигнет узла назначения, который отреагирует ответным сообщением RREP (route reply message), содержащим построенный маршрут. Для сообщений RREP используется однонаправленная передача, в соответствии с путем до отправителя, установленным в соответствующем сообщении RREQ. Таким образом, промежуточные узлы получают информацию как о маршруте к источнику пакетов, так и к получателю.

По сценарию атакующий узел манипулирует сообщениями RREQ и RREP, так, чтобы он был включен в маршрут, и затем отбраковывает все поступающие пакеты с данными. С использованием имитационного моделирования авторы показали, что в условиях атаки Blackhole, проводимой одним узлом, PDR может падать до 55% в случае протокола SAODV и 23% в случае ARAN (при постоянной скорости транспортных средств равной 20м/с). Показатели эффективности протоколов ожидаемо снижаются при увеличении скорости автомобилей, протокол ARAN зависит от нее в большей степени.

2.3. Нарушение конфиденциальности в сетях IoV

Одним из ключевых условий успешного развития и распространения технологий IoV является разработка решений для противодействия угрозам нарушения конфиденциальности. Подробный обзор по данной проблематике приводится в статье [46], где указано, что соответствующие задачи, решаемые для автомобильных сетей, во многом схожи с задачами, решаемыми в обычных сетях. Соответственно, хорошо зарекомендовавшие себя подходы, разработанные ранее, целесообразно применять и в сетях VANET. Так, для обеспечения приватности пользователей используются псевдонимы [47], аутентификация осуществляется с использованием асимметричных криптоалгоритмов [48] и цифровой подписи [49], против пассивного прослушивания канала (eavesdropping) применяются как криптографические методы [50], так и не криптографические, основанные на выборе мощности передатчика с целью обеспечения целевого значения разности между пропускными способностями каналов (с аддитивным белым гауссовским шумом) легитимного транспортного средства и злоумышленника [51]. Для противодействия атаке eavesdropping в беспроводных сетях с ретрансляторами активно применяют кооперативную постановку “дружественных” помех, что находит применение и в автомобильных сетях [52].

Применительно к IoV имеется особый вид угроз конфиденциальности, связанный с раскрытием текущего местоположения автомобиля или отслеживанием его траектории. Следовательно, существует угроза несанкционированного доступа к персональным данным автовладельца. Некоторые перспективные приложения для автомобильных сетей, например, предназначенные для обеспечения безопасности дорожного движения, запрашивают разнообразную информацию об автомобиле, такую как GPS координаты, скорость, угол поворота руля, которая позволяет достаточно точно прогнозировать местоположение автомобиля [46, 53]. Для разработки соответствующих методов предсказания использовались фильтр Калмана и нейронные сети [53].

В настоящее время стремительно набирают популярность технологии оказания информационных и развлекательных услуг, основанных на определении текущего местоположения мобильного пользователя (local-based services, LBSs). Технологии LBSs являются неотъемлемой частью концепции “Умный город” [54]. Поставщик LBSs использует данные конкретного пользователя для предоставления запрашиваемой им информации, например, ближайшая АЗС, ресторан, больница. Несмотря на очевидную пользу, LBSs также создает серьезную угрозу конфиденциальности пользователей, поскольку сервера LBSs уязвимы к взлому [55]. Злоумышленника может интересовать информация о местоположении пользователя, история его передвижений, личность пользователя, характер запроса. Например, перехват запроса о местоположении клиники, специализирующейся на определенном виде услуг, нарушает неприкосновенность частной жизни клиента. Таким образом, при разработке безопасных LBSs систем необходимо принимать во внимание возможности злоумышленника получать доступ к последовательности запросов пользователя, анализировать их, атаковать алгоритм обеспечения конфиденциальности на стороне клиента.

2.4. Прочие атаки в сетях IoV

В различных обзорах по безопасностям в сетях VANET [56–58] упоминается множество атак, действие которых направлено на распространение заведомо ложных сообщений, искажение данных о местоположении транспортных средств, задержку передачи информации. В статье [59] утверждается, что вредоносное программное обеспечение (malware) может использоваться для поражения VANET сетей теми же способами (вирусы, черви и др.), как и в случае обычных сетей. Для защиты предложено использовать типовой подход к решению проблем обеспечения безопасности облачных вычислений. Известен тип атак, распространяющий

заведомо ложную информацию о местоположении транспортных средств — Position attack. Информация о координатах поддерживается спутником GPS, и злоумышленник может манипулировать этими показаниями. В [60] был предложен набор проверок достоверности, которые могут нивелировать последствия Position attack. Атака Illusion искажает данные, получаемые от датчиков автомобилей. Распространение такой неверной информации о скорости автомобилей, о пробках может привести к автомобильным авариям. В статье [61] предложен метод защиты от такой атаки, при котором собираются два типа входных данных — от антенн и от датчиков.

Распространенная атака, действие которой осуществляется на узлы сети — Sybil-атака. Злоумышленник намеренно запрашивает или крадет несколько идентификаторов и с их помощью распространяет ложные сообщения, нарушая функциональность сети. Как отмечено в [62], упоминание о таких атаках на одноранговые сети впервые появилось в статье [63]. Сообщения в транспортных сетях передаются через общую беспроводную среду, а значит, атакующий узел может легко получить идентификационные данные для запуска атаки. В результате один вредоносный узел, расположенный на автомобиле или придорожном оборудовании, может представлять несколько идентификаторов. Этот узел может отправлять заведомо ложные сообщения о ситуациях, связанных с дорожным движением. Сети VANET предназначены для распространения информации о ситуациях на дорогах среди участников движения, следовательно, реагирование на полученную информацию всегда должно приниматься мгновенно. С учетом недостатка времени на проверку истинности отправителя, появляется возможность передавать ложные данные от вредоносного узла, что может существенно повлиять на основную цель сетей VANET — обеспечение безопасного движения. В работах [64–65] рассматривается, как атака Sybil использует уязвимости в транспортных сетях специального назначения — например, в сети организованной группы транспортных средств, движущихся в одном направлении и обменивающихся необходимой информацией о скорости движения, ускорении и пр. В статье [65] описаны различные возможные сценарии атаки — например, фальсификация сообщений во время экстренного торможения. В то время, когда лидер колонны транспортных средств начинает сильно замедляться, атакованные узлы начинают фальсифицировать свое положение, чтобы побудить членов взвода к ускорению. Такая атака может привести к столкновению транспортных средств на высокой скорости.

3. МЕТОДЫ ОБНАРУЖЕНИЯ АТАК

3.1. Обнаружение преднамеренных помех

Для обнаружения преднамеренных помех существуют различные методы. В статье [17] авторы предлагают обратить внимание на изменение доли доставленных пакетов (Packet Delivery Ratio, PDR) от времени, и вводят показатель

$$Down_{PDR} = \frac{PDR(t_1) - PDR(t_0)}{t_1 - t_0},$$

где t_1 и t_0 — соответственно текущий и некоторый прошлый моменты времени. Делается вывод о наличии атаки ПСП, если выполнено хотя бы одно из двух следующих условий:

- Значение $Down_{PDR}$ достигает или превышает некоторое пороговое значение.
- Значение PDR меньше или равно порогу для PDR, и доля доставленных пакетов строго монотонно убывает до нулевого значения.

С помощью имитационного моделирования, применяя дискретно-событийный сетевой симулятор ns-3, авторы подбирают параметры процедуры обнаружения атаки и делают вывод

о ее пригодности. При этом оценки качества обнаружения (частота ложной тревоги, доля ложноотрицательных результатов и т.п.) не приводятся.

В [18] процесс обнаружения ПСП состоит из трех фаз: инициализация, наблюдение и собственно обнаружение. В ходе первой фазы выполняется оценка количества соседних узлов n (конкурирующих за канал). Далее, в ходе второй фазы, оценивается количество успешно полученных сигнальных пакетов l_s и количество коллизий l_c, а также уточняется n. В статье выводится решающее правило для обнаружения ПСП, которое проверяется на третьем этапе:

$$\frac{n - l_s}{l_c} < 2.$$

Если неравенство верно, то генерируется сигнал, информирующий о ПСП.

В [66] для обнаружения реактивных помех предлагается использовать следующее предположение: в случае ПСП наблюдается сильная отрицательная корреляция между интервалами времени успешного и неуспешного приема. Соответственно, авторы предлагают делать вывод о наличие ПСП на основе наблюдений выборочной оценки соответствующего коэффициента корреляции. Здесь следует отметить, что к схожему эффекту может привести группирование случайных ошибок в канале [67] или наличие скрытого терминала (hidden terminal) [68]. Кроме того, эффективность обнаружения зависит от условий формирования выборки и ее размера. Данные вопросы в статье не затрагиваются, показатели качества метода обнаружения не приводятся.

В статье [69] представлен метод для обнаружения преднамеренных помех, примененных с целью атаки на организованную группу машин. Система обнаружения вторжений анализирует сигнальные пакеты. Группа автомобилей разделяется на подгруппы так, чтобы сигнальные пакеты разных подгрупп не вступали в коллизии. В статье приводится процедура для такого группирования. Таким образом, в случае коллизии, обусловленной случайными причинами, будут потеряны сигнальные пакеты от двух или более узлов подгруппы. Сигнал о наличии атаки подается, если потерян ровно один сигнальный пакет.

3.2. Методы обнаружения атаки Black hole

Для повышения эффективности обнаружения, в особенности, для снижения количества ложно-положительных результатов, в [70] предлагается использовать специальные сторожевые устройства (watchdog), которые проводят мониторинг трафика на физическом и канальном уровнях, комбинируют данные для принятия решения о наличие атаки Black hole. В процессе обнаружения атаки на физическом уровне каждое легитимное транспортное средство получает свой уникальный ключ, в соответствии с которым модифицирует отправляемые служебные сигналы. Для назначения ключей авторы предлагают использовать придорожное оборудование (базовые станции), что имеет как преимущества, обусловленные локализацией обработки данных, так и недостатки, например, потребуются дополнительные усилия для обеспечения связи транспортных средств, обслуживаемых соседними станциями. Предполагается, что злоумышленник не модифицирует сигналы. Сторожевое устройство перехватывает копию сигнала, искаженного аддитивным белым гауссовским шумом, после чего проверяет гипотезу “сигнал не модифицирован” против альтернативы “сигнал модифицирован” используя критерий логарифма отношения правдоподобия.

На MAC-уровне сторожевое устройство имеет возможность отслеживать отправку и подтверждение приема сообщений, а также адресатов сообщений. Если узел A послал сообщение узлу C через узел B, узел B успешно получил сообщение, и не поступило подтверждение успешного приема данного сообщения от узла C, то узел B помечается как вредоносный узел.

Ложноположительный результат имеет место, если узел B пересылал пакет узлу C, но последний не получил данные из-за коллизии. Функции сторожевых устройств назначаются случайно выбранным узлам. Решения, принимаемые узлами, имеют одинаковый вес. Окончательное решение о наличие атаки основывается на агрегировании решений нескольких сторожевых узлов.

Для верификации подхода авторы использовали имитационное моделирование. Моделировалось движение автомобилей по скоростной автостраде, показано, что количество ложноположительных решений не превысило 15%. Однако для того, чтобы добиться 5% ложноотрицательных решений, необходимо задействовать в качестве сторожевых устройств не менее 60% узлов сети. Следует отметить, что подход может применяться, только если в атаку не вовлечены взломанные авторизированные узлы. Кроме того, злоумышленник, обладающий возможностями прослушивания канала и простого статистического анализа, может достаточно просто нейтрализовать метод обнаружения Black hole на физическом уровне.

Возможность организации атак Black hole и Grey hole с вовлечением авторизованных узлов рассмотрена в [71]. Авторами предполагается существование абсолютно надежного способа назначать каждому сетевому узлу уникальный идентификатор и пару открытых и закрытых ключей. Таким образом, узлы знают открытые ключи друг друга, могут безошибочно аутентифицировать сообщения, подписанные любыми другими узлами. Узел сохраняет историю обмена пакетами с другими узлами в своем собственном хранилище, соответствующие записи содержат временные метки и другие поля, позволяющие идентифицировать несанкционированное удаление записи. Предлагается хранить лишь некоторое количество последних записей во избежание проблем с переполнением памяти. При встрече узлы обмениваются списками отправленных и полученных пакетов для проверки благонадежности друг друга. Авторы отмечают, что атакующий узел в основном принимает и отбраковывает пакеты, не пересылая их, и предлагают использовать для обнаружения атаки следующую статистику:

$$RR = \frac{N_{RS}}{N_{RNS}},$$

где N_{RS} — количество пакетов, которые узел получил и переправил, N_{RNS} — количество пакетов, которые узел получил для ретрансляции, но не отправил.

Авторы отмечают, что злоумышленники могут сотрудничать, чтобы повысить показатель RR путем создания поддельных записей встреч друг с другом, что затруднит их обнаружение. Поэтому предлагается использовать для обнаружения атаки в условиях возможного сговора злоумышленников следующую статистику:

$$SFR = \frac{N_{self\_send}}{N_{send}},$$

где N_{self_send} — количество пакетов, которые узел самостоятельно сгенерировал и отправил, N_{send} — общее количество отправленных пакетов, независимо от источника. Узлы, вовлеченные в атаку Black hole, будут имеет большие значения показателя RR и меньшие для SFR по сравнению с легитимными узлами. Решение об атаке принимается на основе сравнения величин RR и SFR с заданными пороговыми значениями. Каждый узел ведет свой локальный “черный список” неблагонадежных узлов.

Исследование параметров предложенного метода и оценка его эффективности проводится с помощью среды имитационного моделирования ONE [72]. Моделировалось движение автомобилей по городским улицам со скоростью 10–50 км/ч. Для сети из 40 автомобилей получена высокая эффективность подхода в экспериментах не только с атакой Black hole, но и с Grey hole.

Хотя похожие способы обнаружения и противодействия атаке Black hole, основанные на использовании записей встреч, предлагаются и в других работах [73–75], на наш взгляд предположение о неспособности злоумышленника манипулировать записями встреч представляется неоправданно оптимистичным. Более того, атакующий может по выбору компрометировать любое количество смежных узлов, например, используя ПСП, добиваясь их внесения в "черные списки" остальными узлами. Следует также отметить, что предложенный подход не работает в случае, когда атака Black hole комбинируется с атакой Worm hole [76]. В этом случае злоумышленник может пересылать каждый отбракованный в дальнейшем пакет, фабрикуя произвольную статистику, используемую для обнаружения атаки. Также серьезным недостатком подхода являются противоречия с некоторыми технологиями IoV, например, кластеризацией. Так, если восходящий трафик от транспортных средств идет через головной узел кластера или RSU, а нисходящий обеспечивается широковещательной рассылкой базовыми станциями или RSU[77], то рядовые узлы кластера будут заподозрены в манипулировании показателем SFR.

В статье [78] предложено использовать квитанции с двумя звеньями (Two-hop ACK) для обнаружения Black hole следующим образом. Узел A посылает пакет узлу C через узел B и ожидает уведомление о получении от узла C. Для того чтобы узел B не подделал соответствующий ACK пакет, используется асимметричное шифрование с открытым ключом. ACK пакет может быть не доставлен не только в результате атаки, проводимой узлом B, но и по причинам, не связанным с атакой (коллизии, случайные помехи, экранирование и т. д.). Различать указанные случаи предлагается с использованием метода Байесса [79]. Данный подход не предусматривает наличия двух или более сотрудничающих злоумышленников. Кроме того, атакующий (узел B в схеме выше) может пересылать все пакеты узла A, отбраковывать все пакеты, пересылаемые через A, и не высылать ACK пакеты. Получится вариант атаки Grey hole, при котором рассматриваемый метод обнаружения в качестве злоумышленника объявит узел A.

В статье [80] предлагается использовать несколько обособленных распределенных узлов, на которых развернуты системы обнаружения вторжений. Идея обнаружения атаки Black hole основана на предположении, что злоумышленник не рассылает пакеты RREQ при построении некоторого маршрута, но отправляет соответствующий пакет RREP. Узлы, участвующие в защите, отслеживают указанные действия и начисляют штрафные баллы для каждого подозрительно ведущего себя узла. Если количество штрафных баллов превышает заданное пороговое значение (настраиваемый параметр), то соответствующий узел считается вредоносным. Остальные узлы в его окрестности информируются путем широковещательной рассылки о необходимости исключить данный узел из информационного обмена. Данный метод обнаружения и противодействия атаке Black hole может быть эффективным при том условии, что атакующий не подозревает о мониторинге служебных пакетов, поскольку для обхода защиты достаточно организовать генерацию фальшивых пакетов RREQ.

3.3. Методы обнаружения атаки Sybil

Множество публикаций посвящено поиску решений для защиты узлов сети VANET от атаки Sybil. В статье [81] автор замечает, что выбор метода для обнаружения атаки зависит от дорожной архитектуры, количества транспортных средств. При этом успешный метода должен отвечать следующим требованиям: обнаружение большого процента узлов Sybil; минимальное время для их обнаружения и удаления; обмен сообщениями в сети не должен увеличиваться. В [82] описаны два механизма сертификации узлов: с использованием серии временных меток и с временными сертификатами. При этом рассматривается ситуация, когда узлами, выдающими сертификаты, являются придорожные базовые станции. Предполагается, что два

транспортных средства крайне редко проходят через ряд базовых станций в одно и то же время. Каждое транспортное средство, проезжающее через несколько подряд стоящих станций, получает серию сертификатов, с указанием времени проезда. Проверив сходство таких временных отметок, можно обнаружить атаку. Подход, основанный на временных сертификатах, позволяет предотвратить атаку: RSU выдает временные сертификаты, которые действуют только в определенной области в течение ограниченного времени. При выдаче первого сертификата требуется, чтобы RSU физически идентифицировал транспортное средство, то есть гарантируется, что транспортное средство получит только один сертификат. Таким образом, атака предотвращается.

Автор работы [62] считает, что для предотвращения атаки узел, получивший сообщение, должен установить его подлинность, прежде чем реагировать на него. В статье предполагается, что каждый узел в сети VANET оснащен системой доверия для принятия решений. Описано два варианта установления доверия: на основе статической инфраструктуры и на динамическом установлении доверия самоорганизующимся образом. Доверие на основе статической инфраструктуры авторы считают более эффективным. Если все узлы устанавливают доверие с другими узлами, вероятность возникновения атаки Sybil может быть уменьшена.

В статье [83] авторы предлагают новый подход для обнаружения атаки Sybil — на основе кластеризации временных рядов. Sybil-узлы обнаруживаются как узлы, которые движутся близко друг к другу в кластере в течение долгого времени. Результаты моделирования, приведенные в статье, показывают, что этот подход позволяет идентифицировать Sybil-узлы при различной интенсивности атаки. В статье [84] сравниваются модели для обнаружения Sybil-узлов в двух расположениях: около источника и около места назначения отправки пакета данных. Авторы показывают, что наиболее серьезная угроза исходит от Sybil-узлов, которые распространяют сообщения рядом с источником отправки пакетов.

4. ПРЕВЕНТИВНЫЕ МЕРЫ И ПРОТИВОДЕЙСТВИЕ УГРОЗАМ В СЕТЯХ IOV

4.1. Применение кластеризации узлов для повышения надежности и живучести сетей IoV

Одна из эффективных мер, применяемых для повышения надежности функционирования сетей передачи данных — кластеризация множества узлов. Разбиение узлов на подгруппы полезно для решения различных задач функционирования сети, главные из которых — оптимальное управление сетью, балансировка нагрузки, повышение безопасности передачи данных. Алгоритмы кластеризации объединяют элементы множества в группы (кластеры) согласно некоторому набору правил, при этом в каждом кластере выбирается головной узел (cluster head, CH) для взаимодействия между кластерами. Функции головного узла различаются в зависимости от целей кластеризации, а также от метода, которым он выбран. Формирование иерархических структур в сетях путем объединения нескольких узлов в одну группу используется не только для эффективной маршрутизации при передаче данных, но и для противодействия ряду атак. В некоторых алгоритмах кластеризация применяется для улучшения маршрутизации.

Методы разбиения множества узлов на кластеры и организация связей между кластерами основываются, как правило, на мониторинге каналов, прогнозировании мобильности узлов, оценке безопасности функционирования сети. Наиболее полный обзор по применению технологий кластеризации в современных сетях [85] рассматривает различные способы разбиения множества узлов на подмножества, применяемые в сетях MANET и известные еще с 1980-х годов. Авторы отмечают, что, как правило, такие подходы направлены на решение отдельных проблем и часто используют простые модели каналов, которые не отражают среду современных транспортных сетей VANET. Проанализировав эффективность различных методов кластеризации, авторы отметили недостаток — отсутствие реалистичного моделирования каналов

передачи данных. Обзор представляет таксономию известных алгоритмов, а также выделяет новые направления и тенденции в разработке методов кластеризации узлов в транспортных сетях.

При разбиении множества узлов сети VANET на кластеры существует ряд проблем, характерных для сетей с меняющейся топологией: стабильность кластеров, выбор членов кластера, выбор головного узла CH. Критерии для выбора CH могут включать различные показатели, например, мобильность узла, качество сигнала и способность обеспечивать определенные функции трафика. Как утверждают авторы обзора [85], наиболее распространенный подход для выбора CH основан на том, что каждый узел вычисляет свой индекс, определяющий его пригодность для работы в качестве CH для своих соседей, и рекламирует этот индекс своим ближайшим узлам-соседям. Индекс, как правило, представляет собой взвешенную сумму различных сетевых показателей, таких как степень связности, стабильность соединения, время работы и др. Узлы, желающие присоединиться к этому CH, затем ранжируют всех соседей и запрашивают связь с наиболее ранжируемым узлом-кандидатом. Также авторы замечают, что для выбора CH могут использоваться параметры мобильности узла, показатели качества сигнала, класс транспортного средства, надежность и намерение водителя.

Большая подвижность узлов может приводить к изменению состава кластера, поэтому учет мобильности должен быть включен в процесс кластеризации. В одной из первых работ, посвященных этой проблеме [86], авторы указывают, что узел не может быть выбран в качестве CH, если он очень мобилен по отношению к своим соседям, поскольку в этой ситуации высока вероятность того, что организация кластера будет быстро нарушена. Авторы вводят метрику мобильности для одноранговых сетей, основанную на соотношении между уровнями принимаемой мощности последовательных передач, измеренными в каждом узле от всех соседних узлов. Введенная метрика мобильности используется для выбора головных узлов в алгоритме кластеризации MOBIC. Авторы показывают, что с помощью этого алгоритма можно сформировать более стабильные кластеры, чем, например, с помощью известного алгоритма для кластеризации узлов сетей MANET, описанного в статье [87].

Авторы работы [88] предлагают модель распространения сообщений в сетях VANET с использованием метода для обнаружения атак Ensemble SVM, описанного в [89]. Выбор узла CH в каждом кластере выполняется с помощью алгоритма муравьиной колонии, после этого идет обмен данными. Разработанный на основе метода опорных векторов, Ensemble SVM отслеживает сетевую активность, чтобы обнаружить любое аномальное поведение во время процесса связи. Целевая функция классификатора Ensemble of Ada Booster SVM используется для точного различения аномального и нормального поведения узлов, что повышает точность обнаружения аномальных вторжений.

Максимизировать стабильность кластера при учете высокой мобильности транспортных средств — сложная задача. Авторы статьи [90] предлагают алгоритм кластеризации Affinity Propagation, основанный на передаче сообщений между узлами. Для каждого узла анализируются параметры движения, связности, и на основании этого транспортные средства с низкой относительной мобильностью и хорошими коммуникационными характеристиками могут быть выбраны в качестве CH. Авторами разработан взвешенный механизм для количественной оценки устойчивости кластера в случае, когда некоторое транспортное средство присоединяется к нему. На основании этой оценки происходит выбор оптимального кластера из нескольких кластеров-кандидатов. Преимущество этого метода — нет необходимости указывать количество кластеров заранее, и вычисляемые оценки используются для улучшения стабильности кластера.

Часто в алгоритмах разбиения множества узлов на кластеры сначала выявляют множество транспортных средств, имеющих одинаковую модель мобильности, чтобы обеспечить устойчи-

вость кластеров. В [91] авторы представляют разработанный алгоритм для выделения устойчивых кластеров и определения головных узлов. Метод основан на выборе в качестве CH узла с наименьшей мобильностью (параметр вычисляется как функция разности скоростей между соседними узлами). Моделирование, проведенное с использованием ns-3 и SUMO, показало, что применение алгоритма уменьшает количество смен головных узлов кластеров на 10%.

4.2. Использование придорожного оборудования для повышения безопасности сети

В ситуации, когда транспортный поток является разреженным, то есть узлы сети находятся на большом расстоянии друг от друга, могут возникать задержки при передаче данных, что противоречит основной задаче сетей VANET — мгновенное распространение информации о чрезвычайных ситуациях на дорогах. Кроме того, большое количество транзитных узлов увеличивает задержку пакетов, повышает вероятность их отбраковки, затрудняет обеспечение требуемого качества обслуживания и безопасности. Все это служит мотивацией для развертывания придорожных модулей (например, базовых станций, расположенных вдоль трассы). Эти станции, являющиеся узлами сети VANET, как правило, оснащены более совершенным оборудованием, чем устройства, используемые в транспортных средствах, и могут повышать производительность сети и выполнять функции обеспечения безопасность связи.

Использование придорожного оборудования для улучшения качества связи в сетях VANET обсуждается во многих публикациях. В статье [92] приведен обзор статей в ведущих отечественных и зарубежных изданиях по проектированию беспроводных сетей вдоль протяженных транспортных магистралей. Один из основных вопросов в этом обзоре — оптимальное размещение базовых станций. Авторы проанализировали различные методы расположения базовых станций вдоль транспортных магистралей, с помощью которых максимизируется область покрытия при некоторых ограничениях — например, на суммарную стоимость и на время задержки передачи пакетов данных.

Задача размещения придорожного оборудования для рассылки информации при таких условиях обсуждается в статьях [93, 94]. В статье [95] исследуется ситуация, когда каждое транспортное средство может получить доступ к RSU двумя способами: прямая доставка в случае, когда транспортное средство находится в диапазоне передачи RSU, и многошаговая передача, когда транспортное средство находится вне зоны покрытия RSU. Авторы формулируют задачу размещения придорожного оборудования с помощью модели целочисленного линейного программирования, чтобы максимизировать совокупную пропускную способность в сети. Эффективность предложенной стратегии размещения оценивается с помощью моделирования в системе ns-2.

4.3. Противодействие атаке Black hole

Для противодействия атаке Black hole в [96] предлагается использовать несколько независимых маршрутов. Источник начинает отправлять ответные сообщения только после того, когда указанные маршруты сформированы. Эффективность, и, более того, целесообразность применения данного подхода во многом зависит от топологии сети. Делегировать придорожному оборудованию функции обнаружения как одиночных, так и совместных атак Black hole предлагается в статье [97]. Автомагистрали делятся на кластеры, контролируемые RSU, которые проводят мониторинг подозрительных действий по установлению маршрута, фиксируют атаки на протоколы аутентификации, а также выступают в качестве центров сертификации. Авторы отмечают возможный резкий рост вычислительной нагрузки на RSU, и предлагают, для решения этой проблемы использовать технологии туманных вычислений, в настоящее время активно применяемых для управления ограниченными ресурсами, в том числе и в автомобильных сетях [98]. Привлечь все транспортные средства сети для отслеживания узлов,

помеченные как Black hole, с использованием технологии блокчейн (Blockchain) предлагается в [99]. Заметим, что применение технологии блокчейн в решении разнообразных задач IoV, в том числе, имеющих отношение к обеспечению безопасности, является современным трендом [100].

4.4. Защита конфиденциальности

Популярный подход к обеспечению конфиденциальности владельцев транспортных средств при использовании LBSs основан на концепции k-анонимности. В соответствии с данным подходом, пользователи, отправляющие запросы к ненадежным серверам LBSs,объединяются в группы размера k, так, что по своему местоположению конкретный пользователь не отличим от остальных $k-1$ пользователей группы. Однако, злоумышленник, располагая информацией об атрибутах профиля пользователя (например, пол или возраст), может значительно сократить количество потенциально интересных ему пользователей. Если атрибуты профиля целевого пользователя заметно отличаются от атрибутов профиля других участников группы, то можно даже с высокой достоверностью идентифицировать его. Для того, чтобы гарантировать k-анонимность необходимо создавать группы, в которых все пользователи имеют схожие атрибуты профиля. С этой целью авторы статьи [101] предлагают анализировать семантику запросов, выявлять атрибуты, восприимчивые к де-анонимизации, и для каждого такого атрибута использовать как минимум p носителей при формировании групп. В статье [102] предлагается учитывать не только семантику запросов мобильных пользователей, но и характер перемещений: траектория движения, скорость, время пребывания в локации и т.п.

В статье [103] авторы предложили протокол, названный “Passand Run”, для затруднения предсказаний траекторий транспортных средств, в основе которого лежит следующая идея. Вместо того, чтоб передавать запрос от автомобиля к серверу LBSs по кратчайшему пути через RSU, используется маршрут из нескольких автомобилей, в том числе движущихся, возможно, в направлении противоположном отправителю. Основным недостатком протокола является чрезмерное увеличение задержки пакетов [46]. Идея смешанных зон предложена в [104]. Смешанная зона определяется как пространственная зона, где личность пользователя не может быть идентифицирована. Все пользователи, пребывающие в смешанную зону, изменяют свой псевдоним на новый неиспользованный ими ранее псевдоним, что затруднит идентификацию пользователей злоумышленниками. Серьезным допущением подхода является наличие доверенных центров, которые выполняют процесс анонимизации перед передачей данных в сторонние приложения. Кроме того, возможна утечка данных и де-анонимизация при обновлении глобальных баз данных, ассоциированных с пользователями.

Обеспечение конфиденциальности в автомобильных сетях с использованием алгоритмов генерации фиктивных локаций (dummy) является весьма перспективным в настоящее время, поскольку при этом не требуется развертывания доверительных центров. При запросе услуги пользователь отправляет множество фиктивных местоположений, помимо своего реального местоположения [105]. Все местоположения используют один и тот же идентификатор, соответствующий пользователю, и, следовательно, злоумышленники не располагают точным местоположением пользователя. Однако на эффективность метода влияют физические ограничения, обусловленные окружающей средой. Очевидно, что локации, сгенерированные вокруг единственной горной дороги или в море, являются фиктивными. В статье [106] предложена процедура, позволяющая обойти указанное затруднение.

5. ЗАКЛЮЧЕНИЕ

В заключении обзора приведем некоторые краткие выводы. Особенности IoV активно эксплуатируются при исследовании атак Jamming, Black hole, Sybil, а также атак с целью рас-

крытия текущего местоположения автомобиля или отслеживания его траектории. Ожидаемо, что основные усилия исследователей сфокусированы на разработке методов обнаружения атак в IoV, что в целом характерно для исследований в области обеспечения безопасности новых информационных технологий. В то же время одной из основных проблем IoT является уязвимость устройств к угрозам преднамеренного быстрого истощения батарей (например, атака Depletion of Battery). Особенно актуальны проблемы энергобезопасности для технологий Edge Computing. В повестке исследований безопасности IoV данная проблема практически не присутствует. Кластеризация сетевых узлов, использование придорожного оборудования, являются как превентивными мерами для ряда атак (например, Jamming, Black hole), так и средствами для противодействия атакам. Необходимо отметить, что при всем многообразии публикаций по проблематике безопасности IoV, существует дефицит соответствующих математических моделей и методов. Проверка качества средств обеспечения безопасности IoV, в основном, проводится с использованием имитационного моделирования.

СПИСОК ЛИТЕРАТУРЫ

1. Shen X., Fantacci R., Chen S. Internet of Vehicles // Proc. of the IEEE. – 2020. – Vol. 108, no. 2. P. 242–245.

2. Desnitsky V., Kotenko I., Zakoldaev D. Evaluation of Resource Exhaustion Attacks against Wireless Mobile Devices // Electronics. – 2019. Vol. 8, no. 5. P. 500.

3. Malhi A. K., Batra S., Pannu H. S. Security of vehicular ad-hoc networks: A comprehensive survey // Comput. Secur. – 2020.– Vol. 89.

4. Зегжда П.Д., Иванов Д.В. , Москвин Д.А., Кубрин Г.С. Актуальные угрозы безопасности VANET/MANET-сетей // Проблемы инф. безоп. Комп.сист. – 2018. № 2. С. 41–47.

5. Byahatti P., Saboji S. Review of Security in VANET // Int. J. of Engineering Research & Techn. – 2016. –Vol. 4, no. 29.

6. Овасапян Т.Д., Москвин Д.А., Калинин М.О. Применение нейронных сетей для выявления внутренних нарушителей в VANET-сетях // Проблемы инф. безопасности. Комп. сист. – 2018. Том 1., С. 68?73.

7. Sharma S., Kaushik B. A survey on internet of vehicles: applications, security issues & solutions // Vehicular Communications. – 2019.– Vol. 20.

8. Malhi A.K., Batra S., Pannu H.S. Security of Vehicular Ad-hoc Networks: Comprehensive Survey. // Computers & Security. – 2020.– Vol. 89.

9. Shoufan A., Damiani E. On inter-Rater reliability of information security experts // Journal of Information Security and Applications. – 2017.– Vol. 37. P. 101–111.

10. Weber R.H., Studer E. Cybersecurity in the internet of things: legal aspects // Computer Law & Security Review. – 2016.– Vol. 32, no.5. P. 715–728.

11. Berger S., Burger O., Roglingerac M. Attacks on the Industrial Internet of Things — Development of a multi-layer Taxonomy // Computers & Security. – 2020. – Vol. 93.

12. Makhdoom M., Abolhasan J., Lipman R., Liu P., Ni W. Anatomy of Threats to the Internet of Things // IEEE Comm. Surv.& Tutorials. – 2019. –Vol. 21, no. 2, P. 1636–1675.

13. Raymond D. R., Marchany R. C., Brownfield M. I., Midkiff S. F. Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols // IEEE Transactions on Vehicular Technology. – 2009.– Vol. 58, no. 1, P. 367–380.

14. Mustafa H., Zhang X., Liu Z., Xu W., Perrig A. Jamming-Resilient Multipath Routing // IEEE Trans. on Dependable and Secure Computing. – 2012. –Vol. 9, no. 6. P. 852–864.

15. Patounas G., Zhang Y., Gjessing S. Evaluating Defence Schemes Against Jamming in Vehicle Platoon Networks // IEEE 18th Intern. Conf. on Intelligent Transportation Systems, Las Palmas. – 2015. P. 2153–2158.

16. Alipour-Fanid A., Dabaghchian M., Zhang H., Zeng K. String Stability Analysis of Cooperative Adaptive Cruise Control under Jamming Attacks // IEEE 18th Intern. Symposium on High Assurance Systems Engineering, Singapore. – 2017. P. 157–162.

17. Lynda Mokdad, Jalel Ben-Othman, Anh Tuan Nguyen. DJAVAN: Detecting jamming attacks in Vehicle Ad hoc Networks // Perform. Evaluation. – 2015. –Vol. 87. P. 47–59.

18. Benslimane A., Nguyen-Minh H. Jamming Attack Model and Detection Method for Beacons Under Multichannel Operation in Vehicular Networks // IEEE Transactions on Vehicular Technology. – 2017. –Vol. 66, no. 7. P. 6475–6488.

19. Gummadi R., Wetherall D., Greenstein B., Seshan S. Understanding and mitigating the impact of RF interference on 802.11 networks // ACM SIG COMM Comput. Commun. Rev. – 2007. – Vol. 37, no. 4. P. 386–396, 2007.

20. Shakhov V., Insoo Koo Depletion-of-Battery Attack: Specificity, Modeling and Analysis // Sensors. – 2018. – Vol. 18, no. 6.

21. 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 Amendment 6: Wireless Access in Vehicular Environments, IEEE Std. 802.11p-2010, 2010, P. 1–51.

22. IEEE Standard for Wireless Access in Vehicular Environments(WAVE)–Networking Services, IEEE Std. 1609.3-2010 (Revision of IEEE Std. 1609.3-2007), 2010, P. 1–144.

23. IEEE Standard for Wireless Access in Vehicular Environments (WAVE)–Multi-channel Operation, IEEE Std. 1609.4-2010 (Revision of IEEE Std. 1609.4–2006), 2011, P. 1–89

24. Jiang D., Chen Q., Delgrossi L. Optimal data rate selection for vehicle safety communications // Proc. 5th ACM Int. Workshop VANET, New York, 2008, P. 30–38.

25. Schulze H., Lders C. Basics of Digital Communications // Hoboken, NJ, USA: Wiley, 2006. P. 1–49.

26. An N., Weber S. Efficiency and Detectability of Random Reactive Jamming in Carrier Sense Wireless Networks // IEEE Trans. on Comm. – 2019.– Vol. 67, no. 10. P. 6925–6938.

27. Vilela J. P., Pinto P. C., Barros J. Position-Based Jamming for Enhanced Wireless Secrecy // IEEE Trans. on Inform. Forensics and Security. 2011.– Vol. 6. P. 616–627.

28. Benslimane A., El Yakoubi A., Bouhorma M. Analysis of jamming effects on IEEE 802.11 wireless networks // Proc. IEEE Int. Conf. on Commun.– 2011. P. 1–5.

29. Puñal O., Pereira C., Aguiar A., Gross J. Experimental Characterization and Modeling of RF Jamming Attacks on VANETs // IEEE Transactions on Vehicular Technology. – 2015.– Vol. 64, no. 2. P. 524–540.

30. Puñal O., Aguiar A., Gross J. In VANETs We Trust?: Characterizing RF jamming in vehicular networks // Proc. 9th Int. ACM Workshop on Veh. Inter-Networking, Systems and Applications. – 2012. P. 83–92.

31. Festag A., Baldessari R., Zhang W., Le L. CAR-2-X communication SDK– A software toolkit for rapid application development and experimentations // Proc. IEEE Int. Conference on Communications Workshops. – 2009. P. 1–5.

32. Nourkhiz Mahjoub H., Tahmasbi-Sarvestani A., Osman Gani S. M., Fallah Y. P. Composite $\alpha-\mu$ Based DSRC Channel Model Using Large Data Set of RSSI Measurements // IEEE Trans. on Intelligent Transp. Syst. – 2019.– Vol. 20, no.1, P. 205–217.

33. Librino F., Renda M. E., Santi P. Multihop Beaconing Forwarding Strategies in Congested IEEE 802.11p Vehicular Networks // IEEE Trans. on Vehicular Technology. – 2016. – Vol. 65, no. 9. P. 7515–7528.

34. Hofer M., Zemen T., Bernado L. Evaluation of Vehicle-in-the-Loop Tests for Wireless V2X Communication // IEEE 90th Vehicular Technology Conf. – 2019. Honolulu. P. 1–5.

35. Renda M. E., Resta G., Santi P., Martelli F., Franchini A. IEEE 802.11p VANets: Experimental evaluation of packet inter-reception time // Computer Communications. – 2016. – Vol. 75. P. 26–38.

36. Mangel T., Klemp O., Hartenstein H. 5.9 GHz inter-vehicle communication at intersections: A validated non-line-of-sight path-loss and fading model // EURASIP J. on Wireless Communications and Networking. – 2011.– Vol. 2011, no. 1. P. 1–11.

37. Rice University: The WARP Project, Nov. 29, 2013. [Online]. http://warp.rice.edu

38. Gu P., Hua C., Khatoun R., Wu Y., Serhrouchni A. Cooperative Anti jamming Relaying for Control Channel Jamming in Vehicular Networks // IEEE Trans. on Vehicular Technology. – 2018. – Vol. 67, no. 8. P. 7033–7046.

39. Bibhu, V., Roshan, K., Singh, K.B., Singh, D. Performance analysis of black hole attack in VANET // Inter. J. of Comp. Net. and Inform. Security. – 2012. – Vol. 4, no. 11, P. 47–54.

40. Abduvaliyev A., Pathan A. K., Zhou J., Roman R., Wong W. On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks // IEEE Communications Surveys & Tutorials. – 2013. – Vol. 15, no. 3. P. 1223–1237.

41. Butun I., Osterberg P., Song H. Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures // IEEE Comm. Surveys & Tutorials. – 2020.– Vol. 22, no. 1. P. 616–644.

42. Tseng, F., Chou, L., Chao, H. A survey of black hole attacks in wireless mobile ad hoc networks // Hum. Cent. Comput. Inf. Sci. – 2011.– Vol.1. P. 1–16.

43. Nugraha M. A., Sudiharto D. W., Herutomo A. Performance comparative analysis between ARAN and SAODV on VANET facing the black hole // Intern. Conf. on Electrical Engineering and Informatics. – 2017. Banda Aceh. P. 1–6.

44. CerriD., Ghioni A. Securing AODV: The A-SAODV secure routing prototype // IEEE Communication Magazine. – 2008. P. 120–125.

45. Sanzgiri K., La Flamme D., Dahill B., Levine B. N., Shields C., Belding-Royer E. M. Authenticated routing for ad hoc networks //IEEE Journal on Selected Areas in Communications. – 2005.– Vol. 23. P. 598–610.

46. Lu Z., Qu G., Liu Z. A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy // IEEE Trans. on Intell. Transp. Syst. – 2019.– Vol. 20, no. 2. P. 760–776.

47. Petit J., Schaub F., Feiri M., KarglF. Pseudonym schemes in vehicular networks: A survey // IEEE Commun. Surveys and Tutorials. – 2015.– Vol. 17, no. 1. P. 228–255.

48. Azees M., Vijayakumar P., Deboarh L. J.EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks // IEEE Trans. on Intelligent Transportation Systems. – 2017.– Vol. 18, no. 9. P. 2467–2476.

49. Zhang L., Wu Q., Domingo-Ferrer J., Qin B., and Hu C. Distributed aggregate privacy-preserving authentication in VANETs // IEEE Trans. on Intelligent Transportation Systems. – 2017. –Vol. 18, no. 3. P. 516–526.

50. Li K., Lu L., Ni W., Tovar E., Guizani M. Secret Key Agreement for Data Dissemination in Vehicular Platoons // IEEE Trans. on Vehicular Techn. – 2019. – Vol. 68, no. 9. P. 9060–9073.

51. Yin Z., Jia M., Wang W., Cheng N., Lyu F., Shen X. Max-Min Secrecy Rate for NOMA-Based UAV-Assisted Communications with Protected Zone // IEEE Global Communications Conference (GLOBECOM), 2019, Waikoloa, USA. P. 1–6.

52. Wang D., Ren P., Du Q., Sun L., Wang Y. Security Provisioning for MISO Vehicular Relay Networks via Cooperative Jamming and Signal Superposition // IEEE Trans. on Vehicular Technology. – 2017. – Vol. 66, no. 12. P. 10732–10747.

53. Feng, H., Liu, C., Shu, Y. et al. Location Prediction of Vehicles in VANETs Using A Kalman Filter // Wireless Personal Communications. – 2015. –Vol. 80. P. 543–559.

54. Wang, C., David, B., Chalon, R., Yin, C. Dynamic road lane management study // Transport. Research Part E: Logistics and Transport. Review. – 2015. – Vol. 89.P. 272–287.

55. Wu Z., Wang R., Li Q., Lian X., Xu G., Chen E., Liu X.A Location Privacy-Preserving System Based on Query Range Cover-Up or Location-Based Services // IEEE Trans. on Veh. Techn. – 2020. – Vol. 69, no. 5, P. 5244–5254.

56. Zeadally S., Hunt R., Chen Y., Irwin A., Hassan, A. Vehicular ad hoc networks (VANETS): status, results, and challenges // Telecomm. Syst. – 2012.– Vol. 50. P. 217–241.

57. Kariuki G. A Survey on Possible Attacks in Vehicular Ad Hoc Network // J. of Telecomm. and Information Technology. 2019.

58. Junaid M., Syed A.A., Warip M., Azir K.N., Romli N.H. Classification of Security Attacks in VANET: A Review of Requirements and Perspectives // MATEC Web of Conf. – 2018. – Vol. 150.

59. Zhang T., Antunes H., Aggarwal S. Defending Connected Vehicles Against Malware: Challenges and a Solution Framework // IEEE Internet of Things Journal. – 2014.– Vol. 1, no. 1, P. 10–21.

60. Alsharif, N., Wasef, A., Shen, X. ESPR: Efficient Security Scheme for Position-Based Routing in Vehicular Ad Hoc Networks // IEEE Global Telecomm. Conf. – 2010 P. 1–5.

61. Lo N., Tsai H.—C. Illusion Attack on VANET Applications — A Message Plausibility Problem // IEEE Globecom Workshops. – 2007. P. 1–8.

62. Grover J. Sybil Attack in VANETs: Detection and Prevention // In book: Security of Self organizing networks: MANET, WSN,WMN, VANET (Chapter 12)Publisher: CRC Press, Taylor & Francis Group, USA. Editors: Al Sakib khan Pathhan. 2011.

63. Douceur J. R.The Sybil Attack //Intern. Workshop on Peer-to-Peer Systems. LNCS. – 2002.– Vol. 2429. P. 251–260.

64. Boeira F., Barcellos M. P., de Freitas E. P., Vinel A., Asplund M. On the impact of sybil attacks in cooperative driving scenarios // IFIP Networking Conference and Workshops. – 2017. Stockholm. P. 1–2.

65. Boeira F., Barcellos M. P., de Freitas E. P., Vinel A., Asplund M. Effects of colluding Sybil nodes in message falsification attacks for vehicular platooning // IEEE Vehicular Networking Conference. 2017. Torino. P. 53–60.

66. Hamieh A., Ben-Othman J., Mokdad L. Detection of Radio Interference Attacks in VANET // IEEE Global Telecommunications Conference. Honolulu. 2009. P. 1–5.

67. Melent'ev, O.G., Kleiko, D.V. Computing the parameters of the discrete channel resulting under frequency hopping in the general case// Autom. and Remote Control. – 2013.– Vol. 74. P. 1128–1131.

68. Akimoto K., Kameda S., Suematsu N. Optimum Allocation Scheme for User Fairness of Location-Based Virtual Sector Method Solving Hidden Terminal Problem in WLAN // IEEE Transactions on Vehicular Technology. – 2018.– Vol. 67, no. 9. P. 8363–8371.

69. N. Lyamin, A.Vinel, M. Jonsson, J. Loo Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11p Vehicular Networks // IEEE Comm. Letters. – 2014.– Vol. 18, no. 1. P. 110–113.

70. Baiad R., Alhussein O., Otrok H, Muhaidat S. Novel cross layer detection schemes to detect black hole attack against QoS-OLSR protocol in VANET // Veh. Commun. 2016.– Vol. 5. P. 9–17.

71. Pham T. N. D., Yeo C. K. Detecting Colluding Black hole and Grey hole Attacks in Delay Tolerant Networks // IEEE Trans. on Mobile Comput. – 2016.– Vol. 15, no. 5. P. 1116–1129.

72. Keranen A., Ott J., Karkkainen T. The one simulator for DTN protocol evaluation // Proc. 2nd Int. Conf. Simul. Tools Tech. 2009. Rome, Italy. P. 55:1–55:10.

73. Li F., Wu J., Srinivasan A. Thwarting black hole attacks in disrupt-tolerant networks using encounter tickets // Proc. INFOCOMM, 2009. P. 2428–2436.

74. Guo Y., Schildt S., Wolf L. Detecting blackhole and greyhole attacks in vehicular delay tolerant networks // Proc. IEEE 5thInt. Conf. Commun. Syst. Netw. 2013, P. 1–7.

75. Li Q., Cao G. Mitigating routing misbehaviors in disruption tolerant networks // IEEE Trans. Inf. Forensics Securityю – 2012.– Vol. 7, no. 2. P. 664–675.

76. Jamali S., Fotohi R. DAWA: Defending against wormhole attack in MANETs by using fuzzy logic and artificial immune system // J. Super comput. – 2017. –Vol. 73. P. 5173–5196.

77. Evdokimova E., Vinel A., Lyamin N., Fiems, D. Internet Provisioning in VANETs: Performance Modeling of Drive-Thru Scenarios // IEEE Transactions on Intelligent Transportation Systems. – 2020. –Vol. 21, no. 7. P. 2801–2815.

78. Djenouri D, Badache N. Struggling Against Selfishness and Black Hole Attacks in MANETs // Wireless Communications & Mobile Comput. – 2008.– Vol. 8(6). P. 689–704.

79. Davison A. Bayesian Models // In book: Statistical Models (chupter 11). Springer, 2000. P. 565-644

80. Su M.-Y. Prevention of Selective Black Hole Attacks on Mobile Ad Hoc Networks Through Intrusion Detection Systems // IEEE Comp. Comm. – 2011. –Vol. 34. P. 107–117.

81. Mane A. Sybil attack in VANET // International J. of Computational Engineering Researchю – 2016.– Vol. 06, no. 12. P. 60–65.

82. Park, S., Aslam, B., Turgut, D., Zou, C.C. Defense against Sybil attack in the initial deployment stage of vehicular ad hoc network based on roadside unit support. // Security and Communication Networks. – 2013. – Vol. 6, no 4. P. 523–538.

83. Dutta N., Chellappan S. A Time-series Clustering Approach for Sybil Attack Detection in Vehicular Ad hoc Networks // Computer Science 2013.

84. Kafil P., Fathy M., Lighvan M. Z. Modeling Sybil attacker behavior in VANETs // 9th Intern. Conf. on Information Security and Cryptology. 2012. P. 162–168.

85. Cooper C., Franklin D., Ros M., Safaei F., Abolhasan M. A Comparative Survey of VANET Clustering Techniques // IEEE Comm. Surveys & Tutorialsю – 2017. – Vol. 19, no. 1. P. 657–681.

86. Basu P., Khan N., Little T. D. A mobility based metric for clustering in Mobile Ad Hoc. Networks // Proc. Int. Conf. Distrib. Comput. Syst. Workshop, Mesa, 2001. P. 413–418.

87. Chiang C.-C., Wu H.-K., Liu W., Gerla M. Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel // Proceedings of SICON 1997. P. 197–212.

88. Mythili A., Magendran S. K. Clustering algorithm and ensemble SVM for attack detection in VANET // Int. J. of Pure and Applied Math. – 2018. –Vol. 119, no.12. P.15407–15418

89. Murugan K., Suresh P. Ensemble of Ada Booster with SVM Classifier for Anomaly Intrusion Detection in Wireless Ad Hoc Network //Indian J. of Science and Tech. – 2017.– Vol. 10, no 23. P. 1–10.

90. Bi X., Guo B., Shi L., Lu Y., Feng L., Lyu Z. A New Affinity Propagation Clustering Algorithm for V2V-Supported VANETs // IEEE Access. – 2020. – Vol. 8. P. 71405–71421.

91. Ucar S., Ergenand S. C., Ozkasap O. VmaSC: Vehicular multi-hop algorithm for stable clustering in Vehicular Ad Hoc Networks //IEEE Wireless Communications and Networking Conference, Shanghai, 2013, P. 2381–2386.

92. Вишневский В.М., Кришнамурти А., Козырев Д.В., Ларионов А.А., Иванов Р.Е. Методы исследования и проектирования широкополосных беспроводных сетей вдоль протяженных транспортных магистралей // T-Comm: Телекоммуникации и транспорт. — 2015. — Том 9. — №5. — С. 9–15.

93. Reddy K., Tamizhazhagan V. An Innovative Selection of Road Side Unit Emplacement in VANETs // Int. Conf. Sustainable Comm. Networks and Appl. ICSCN – 2019. – Vol. 39.

94. Mehar S., Senouci S., Kies A., Maaza, Z. An Optimized Roadside Units (RSU) placement for delay-sensitive applications in vehicular networks // 12th Annual IEEE Consumer Communications and Networking Conference, 2015. P. 121–127.

95. Wu T.-J., Liao W., Chang C.-J. A Cost-Effective Strategy for Road-Side Unit Placement in Vehicular Networks // IEEE Trans. on Comm. – 2012. – Vol. 60, no 8, P. 2295-2303

96. Al-Shurman M., Yoo S-M, Park S. Black Hole Attack in Mobile Ad Hoc Networks // 42nd Annual ACM Southeast Regional Conference, 2004. Huntsville, Alabama.

97. Albouq S. S., Fredericks E. M. Lightweight Detection and Isolation of Black Hole Attacks in Connected Vehicles // IEEE 37th Int. Conf. on Distributed Computing Systems Workshops. – 2017. Atlanta. P. 97–104.

98. Chen X., Leng S., Zhang K., Xiong K. A machine-learning based time constrained resource allocation scheme for vehicular fog computing // China Comm. – 2019. – Vol. 16, no. 11. P. 29–41.

99. Tobin J., Thorpe C., Murphy L. An Approach to Mitigate Black Hole Attacks on Vehicular Wireless Networks // IEEE 85th Vehicular Technology Conf. 2017. Sydney. P. 1–7

100. Wang S., Ye D., Huang X., Yu R., Wang Y., Zhang Y. Consortium Blockchain for Secure Resource Sharing in Vehicular Edge Computing: A Contract-based Approach // IEEE Transactions on Network Science and Engineering. – 2020.

101. Dargahi T., Ambrosin M., Conti M., Asokan N. ABAKA: A novel attribute-based k-anonymous collaborative solution for LBSs // Comp. Commun. – 2016. –Vol. 85. P. 1–13.

102. Tan R., Tao Y., Si W., Zhang Y.-Y. Privacy preserving semantic trajectory data publishing for mobile location-based services // Wireless Networks. – 2019.

103. Dunbar C., Qu G.A DTN routing protocol for vehicle location information protection // Proc. IEEE Military Commun. Conf. 2014. P. 94–100.

104. Beresford A. R., Stajano F. Location privacy in pervasive computing // IEEE Pervasive computing. 2003.– Vol.2, no. 1. P. 46–55.

105. Niu B., Li Q., Zhu X., Cao G., Li H. Achieving k-anonymity in privacy-aware location-based services // Proceedings IEEE, INFOCOM, 2014,. P. 754–762.

106. Song D., Song M., Shakhov V., Park K. Efficient dummy generation for considering obstacles and protecting user location. // Concurrency and Computation: Practice and Experience. 2019.

A Survey on Security Issues in Internet of Vehicles

Sokolova O.D., Shakhov V.V.

The Internet of Vehicles (IoV) offers tremendous opportunities for the global community. However, there are concerns that IoV security risks outweigh the benefits. There are many research works aimed at reducing the aforementioned risks. This paper conducts a comprehensive survey on corresponding results. We consider threats to confidentiality, integrity and availability. It has been shown that security solutions involve three main security layers: prevention, detection, mitigation. The main goal of the survey is to provide insight into technique for ensuring IoV security.

KEYWORDS: Internet of vehicles, information security, IEEE 802.11p standard, intrusion detection systems.