УДК 004.057.4:004.738

**Е.В. Щерба, В.И. Никонов, Г.А. Литвинов**

# Обеспечение безопасности протоколов маршрутизации для телекоммуникационных сетей с динамической топологией

Дан сравнительный обзор актуальных угроз безопасности и применяемых подходов к защите протоколов маршрутизации для телекоммуникационных сетей с динамической топологией, включая сети MANET, WSN и др. Рассматриваются более 20 значимых и перспективных протоколов маршрутизации, безопасность в рамках которых обеспечивается посредством двух базовых подходов – криптографической защиты и защиты на основе концепции доверия и кооперации узлов. Выделены достоинства, недостатки и уязвимости рассмотренных протоколов, а также определены перспективные направления для дальнейших исследований.

**Ключевые слова:** беспроводные самоорганизующиеся сети, MANET, VANET, FANET, WSN, уязвимости маршрутизации, сетевая безопасность.

**doi:** 10.21293/1818-0442-2018-21-3-19-29

Увеличение количества мобильных сетевых устройств по всему миру спровоцировало интенсивные исследования по различным аспектам взаимодействия данных устройств. Среди большого количества зарубежных и отечественных работ в данной области можно выделить несколько основных направлений исследований, которые охватывают технологии самоорганизующихся сетей мобильных устройств (MANET), беспроводных сенсорных сетей (WSN), самоорганизующихся сетей беспилотных летательных аппаратов (FANET), самоорганизующихся сетей интеллектуальной транспортной системы (VANET) и др. Таким образом, широкий спектр оборудования гражданского и военного назначения может объединяться в сети посредством сетевой архитектуры беспроводных динамически организуемых децентрализованных сетей [1, 2].

Ключевые особенности рассматриваемой архитектуры по сравнению с традиционной фиксированной архитектурой телекоммуникационных сетей состоят в следующем. Во-первых, каждое устройство может выступать в качестве маршрутизатора, т.е. принимать сетевые пакеты, адресованные другим узлам, производить выбор направления для дальнейшей передачи пакетов и осуществлять эту передачу. Во-вторых, подвижность узлов влечет за собой постоянные изменения в сетевой топологии, т.е. топология сети является динамической. Данные особенности обусловливают разработку специализированных протоколов маршрутизации для данных сетей. Кроме того, указанные особенности являются источником уязвимостей безопасности самого процесса маршрутизации сетевых пакетов в данных сетях, что порождает целый класс атак на протоколы маршрутизации, специфичный для рассматриваемой архитектуры.

Таким образом, основная цель данной работы заключается в аналитическом исследовании разработанных протоколов маршрутизации, уязвимостей их безопасности и предусмотренных методов и механизмов защиты.

**Протоколы маршрутизации для сетей с динамической топологией**

Благодаря широкому спектру приложений указанной архитектуры в сетях различного назначения к настоящему моменту разработано несколько десятков протоколов маршрутизации для данных сетей, которые можно условно классифицировать на несколько групп: проактивные, реактивные, гибридные.

Проактивные (табличные) протоколы маршрутизации основаны на постоянном обмене служебными пакетами для регулярной актуализации таблицы маршрутов и обладают чертами традиционной табличной маршрутизации. Такой принцип эффективен в сравнительно небольших сетях, но может оказаться слишком затратным при значительном увеличении числа подключенных к сети устройств. Для эффективной работы проактивных протоколов в больших сетях требуется отсутствие существенных ограничений по пропускной способности и вычислительным ресурсам для обработки огромных таблиц маршрутизации. Рядовые сценарии, такие как добавление нового узла, изменение его расположения или удаление, могут вызывать задержки в сетях с проактивной маршрутизацией.

Протокол DSDV (Destination Sequenced Distance Vector) [3] стал одним из первых проактивных протоколов маршрутизации, предложенных для динамически организуемых сетей. Данный табличный протокол основан на алгоритме Беллмана–Форда и для каждой записи маршрутизации помимо метрики маршрута предусматривает наличие возрастающего порядкового номера, что позволяет избегать маршрутизации пакетов по замкнутому кругу.

Наиболее распространенным и перспективным проактивным протоколом маршрутизации в сетях с динамической топологией является протокол OLSR (Optimized Link State Routing) [4]. Учитывая спецификации OLSRv2 [5], выпущенные Инженерным советом Интернета (IETF) в 2014 г., протокол является первым обновленным протоколом среди всех стандартизированных протоколов маршрутизации, применяемых в динамически организуемых сетях. Каждый узел в рамках указанного протокола регулярно производит обнаружение соседних узлов, доступных за один и за два перехода, на основе широковещательных сообщений приветствия (HELLO). Среди всех узлов, доступных за один переход, осу-

ществляется оптимальный выбор подмножества шлюзов MPR (Multipoint Relay), обеспечивающих связь со всеми узлами, доступными за два перехода. Каждый узел, выбранный в качестве шлюза MPR, производит рассылку широковещательных сообщений TC (Topology Control), которые в обязательном порядке содержат объявления маршрутов к узлам-селекторам, выбравшим данный узел в качестве шлюза MPR. Данные сообщения принимаются и обрабатываются всеми соседними узлами, но ретранслируются далее по сети только узлами, выбранными в качестве шлюзов MPR. На основе полученных сообщений TC каждый узел производит построение сетевой топологии и определяет оптимальные маршруты до всех получателей в соответствии с числом переходов для OLSRv1 либо в соответствии с установленной метрикой для OLSRv2. В результате в пересылке пакетов данных могут участвовать только узлы, выбранные в качестве шлюза MPR каким-либо другим узлом.

В рамках реактивных протоколов узел инициирует поиск маршрута только при возникновении необходимости передачи им информации (т.е. по требованию или по запросу). В больших сетях такой алгоритм позволяет сократить как размеры таблиц маршрутизации, так и объем рассылаемой информации. При этом очевидными проблемами реактивных протоколов являются высокие задержки при прокладке маршрута и отсутствие поддержки устаревающих маршрутов.

Обнаружение маршрутов в рамках реактивного протокола пошаговой маршрутизации AODV (Ad Hoc On-demand Distance Vector) [6] осуществляется посредством рекурсивной широковещательной рассылки управляющего пакета RREQ (Route Request). Если требуемый маршрут найден в таблице маршрутизации промежуточного узла либо пакет RREQ достигает узла назначения, ответный управляющий пакет RREP (Route Reply) высылается соответствующим узлом источнику в целях прокладки маршрута. Для поддержания связности с соседними узлами каждый узел регулярно производит отправку сообщений HELLO. Уведомление об ошибке маршрутизации осуществляется при помощи отправки управляющего пакета RRER (Route Error). Протоколом предусмотрена процедура обслуживания маршрутов (для удаления устаревших и потерявших актуальность маршрутов), которая также подразумевает рассылку управляющего пакета RERR.

Основное отличие реактивного протокола маршрутизации DSR (Dynamic Source Routing) [7] от протокола AODV заключается в применении концепции построения пути от источника передачи вместо пошаговой маршрутизации. Данный подход позволяет отказаться от периодической рассылки сообщений для проверки маршрутов, что в свою очередь ведет к снижению нагрузки на сеть и экономии ресурсов узлов. С другой стороны, эффективность протокола быстро ухудшается с увеличивающейся подвижностью узлов.

Сочетание проактивной и реактивной маршрутизации положено в основу так называемых гибридных протоколов. Один из способов такого комбинирования подходов, предлагаемый в рамках протокола ZRP (Zone Routing Protocol) [8], подразумевает зонирование сети. При этом внутри зон функционирует проактивная маршрутизация IARP (Intra-zone Routing Protocol), а взаимодействие между зонами организовано на основе реактивной маршрутизации IERP (Inter-zone Routing Protocol).

**Анализ существующих уязвимостей протоколов маршрутизации**

Изначально протоколы маршрутизации, разрабатываемые для динамически организуемых телекоммуникационных сетей, не обладали какими-либо защитными механизмами, учитывающими специфику данных сетей. Указанное обстоятельство способствовало возникновению множества пассивных и активных атак на эти протоколы. Наибольшее распространение получили традиционные атаки типа «человек посередине» и «отказ в обслуживании», а также класс атак, позволяющих перенаправлять сетевые пакеты по ложному маршруту [9, 10]. Далее перечислены основные виды сетевых атак на протоколы маршрутизации для телекоммуникационных сетей с динамической топологией.

Классическим примером атаки типа «отказ в обслуживании» является переполнение таблиц маршрутизации (Routing Table Overflow) соседних узлов путём объявления множества маршрутов к несуществующим узлам. В случае переполнения таблицы маршрутизации добавление в нее легитимных маршрутов станет невозможным.

Атаку типа «блекхол» (Black Hole Attack) также можно отнести к атакам типа «отказ в обслуживании». В примере (рис. 1), иллюстрирующем атаку, сетевые пакеты, проходящие от отправителя $V_1$ через узел нарушителя $M$, отбрасываются и не передаются далее к получателю $V_4$.

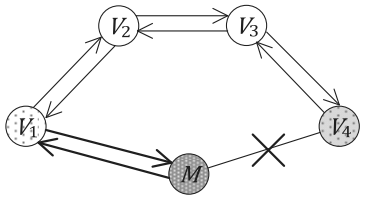


Рис. 1. Схема атак типа «блекхол» и «грейхол»

Существует множество разновидностей указанной атаки, включая выборочное блокирование управляющих пакетов протокола маршрутизации, выборочное блокирование отдельных пакетов данных (атака типа «грейхол») и полное блокирование всех пакетов.

В ходе атаки типа «синкхол» (Sink Hole Attack) нарушитель $M$ распространяет ложный оптимальный маршрут до узла получателя $V_4$ и тем самым направляет через себя сетевые пакеты, отправленные соседними узлами $V_1$ и $V_2$ (рис. 2).

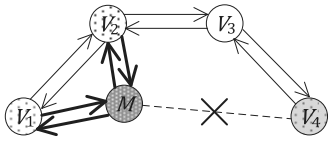


Рис. 2. Схема атаки типа «синкхол»

В результате кооперации нарушителей осуществляется атака типа «вормхол» (Worm Hole Attack), суть которой заключается в несанкционированном доступе к пакетам соседних устройств, передаваемых до получателя по реально существующему высококачественному каналу, созданному нарушителями. В примере (рис. 3), иллюстрирующем атаку, высокие характеристики создаваемого канала позволяют нарушителям $M_1$ и $M_2$ предложить оптимальный маршрут от узла $V_1$ к узлу $V_5$ и в обратном направлении. В результате сетевые пакеты, доставляемые ранее через узлы $V_2$, $V_3$ и $V_4$, будут перенаправлены через узлы нарушителей.

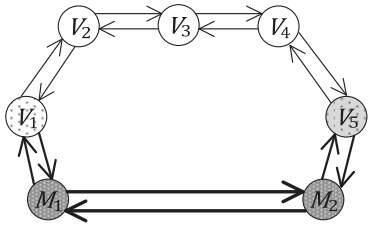


Рис. 3. Схема атаки типа «вормхол»

Помимо вышеназванных атак, отдельно можно отметить актуальность проблемы эгоистичности узлов (Selfish Attack), скрывающих маршруты в целях экономии ресурсов, и атаки сговора на механизм репутации, используемый в ряде протоколов маршрутизации для обеспечения их защиты (разновидность Sybil Attack). Реализация указанной атаки позволяет завысить либо занизить значение репутации узла, что также может привести к изменению маршрута доставки пакета.

Подробный анализ известных уязвимостей для протокола OLSRv2, многие из которых актуальны и для других протоколов маршрутизации, был выпущен в 2017 г. Инженерным советом Интернета (IETF) в документе RFC 8116 [11].

**Криптографические расширения безопасности протоколов маршрутизации**

В ходе исследований по вопросам обеспечения безопасности протоколов маршрутизации было предложено множество решений, что привело к разработке ряда новых защищенных протоколов. Следует отметить, что большинство разработанных протоколов опираются на механизмы криптографических преобразований и были представлены как защищенные версии (расширения) существующих протоколов.

Учитывая доминирующий статус реактивных протоколов маршрутизации, основное внимание исследователей и разработчиков уделяется обеспечению безопасности данных протоколов. Так, протокол SAODV (Secure AODV) был предложен для защиты управляющих пакетов протокола AODV на основе асимметричной криптосистемы [12]. Аутентификация пакетов RREQ и RREP производится посредством электронных подписей. Каждый управляющий пакет подписывается секретным ключом отправителя этого пакета. Промежуточные узлы и конечные получатели пакетов производят проверку подписи и осуществляют обработку и передачу пакетов только в случае её валидности.

Поскольку пакеты RREQ и RREP содержат изменяемое в процессе передачи поле Hop_Count (число переходов), аутентификация этого поля производится отдельно на основе цепочки хэшей. Узел-источник выбирает случайное значение (seed) в начале процесса обнаружения маршрута и устанавливает максимальное количество переходов (MHC). Далее источник вычисляет значение Hash как хэш исходного числа h(seed) и значение Top_Hash, как $h^{MHC}$(seed). Промежуточные узлы при получении управляющего пакета производят проверку корректности значения Top_Hash, учитывая текущее значение поля Hop_Count, после чего увеличивают значение поля Hop_Count и вычисляют новое значение Hash как h(Hash) перед дальнейшей рассылкой управляющего пакета RREQ. Одна из главных проблем протокола SAODV связана со сложностью безопасного распределения ключей (протокол подвержен атакам типа «человек посередине»).

Для решения данной проблемы реактивный протокол маршрутизации ARAN (Authenticated routing for ad hoc networks) [13] предусматривает наличие в самоорганизующейся сети удостоверяющего центра и применение криптографических сертификатов, что позволяет обеспечить аутентификацию сторон, целостность данных и неотказуемость. В ходе первой предварительной стадии протокола каждый подключаемый к сети узел должен инициировать создание сертификата открытого ключа, подписанного удостоверяющим центром. Далее в ходе реактивного обнаружения маршрутов для всех передаваемых сообщений на основе сгенерированных сертификатов выполняется обязательная аутентификация источника и получателя, что позволяет построить безопасный маршрут.

Кроме того, для повышения безопасности в рамках протокола также предусмотрены проверка подписи отправителя сообщения и формирование новой подписи каждым промежуточным передающим узлом. Вместе с тем ввиду сложности и ресурсоёмкости процедуры аутентификации протокол ARAN не получил широкого распространения. Среди других недостатков протокола можно выделить проблему выбора удостоверяющего центра и уязвимость к атакам типа «вормхол».

Схема защиты проактивного протокола OLSR, предложенная в работе [14], также предусматривает применение инфраструктуры открытых ключей в целях формирования и проверки подписи каждого управляющего сообщения протокола. Формируемая подпись включает временную метку и используется

для предотвращения модификации или фальсификации данных о топологии сети в передаваемых сообщениях. Однако, как было отмечено ранее, необходимость развертывания инфраструктуры открытых ключей является ограничивающим фактором в сетях с динамической топологией.

Альтернативный подход к защите OLSRv1 на основе асимметричной криптографии предложен разработчиками протокола SLSP (Secure Link State Routing Protocol) [15]. Протокол не предусматривает создание выделенного центра распределения ключей, вместо этого каждый узел самостоятельно генерирует ключевую пару и передаёт свой открытый ключ всем соседним узлам. Распространяемые сообщения приветствия и обновления маршрутизации подписываются секретным ключом отправителя. Защита изменяемого поля «Hop Count» производится на основе рассмотренного ранее механизма цепочки хэшей; кроме того, каждое обновление содержит поле «Sequence Number» (порядковый номер) для защиты от атаки воспроизведением.

Таким образом, протокол обеспечивает защищенное обнаружение соседних узлов и распространение маршрутной информации по сети. Кроме того, протокол SLSP устойчив к атакам, выполняемым в целях переполнения таблицы маршрутизации. Каждому из соседних узлов присваивается значение приоритета. Узлы, генерирующие максимальное число обновлений маршрутизации, имеют минимальный приоритет, что позволяет снизить эффективность атаки на отказ в обслуживании. Несмотря на то, что данный протокол не подвержен внешним атакам типа «блекхол» и «синкхол», он не позволяет противостоять различным атакам сговора нескольких нарушителей.

Протокол SRP (Secure Routing Protocol) [16], применяемый для защиты DSR и реактивной составляющей IERP гибридного протокола ZRP, предусматривает наличие общего ключа, используемого узлом источника и узлом назначения при организации защищенной связи SA (Security Association). Узел источника производит обнаружение маршрута до узла назначения посредством широковещательной рассылки управляющего пакета запроса маршрута RREQ, включающего пару идентификаторов (порядковый номер запроса и произвольный идентификатор запроса) и код аутентичности – значение ключевой хэш-функции, рассчитываемое на основе параметров запроса (адрес узла-источника, адрес узла назначения, идентификаторы). Промежуточные узлы, участвующие в пересылке пакета RREQ, добавляют в пакет свои адреса, а узел назначения осуществляет аутентификацию запроса посредством проверки кода аутентичности и формирует ответный пакет RREP, включающий использованные идентификаторы и новый код аутентичности. Доставка пакета RREP производится полностью в соответствии с маршрутом доставки пакета RREQ, а узел источника осуществляет его аутентификацию при получении.

Применение концепции маршрутизации от источника позволяет исключить необходимость осуществления криптографических преобразований промежуточными узлами, обеспечивающими пересылку пакетов между сторонами защищенной связи, что особенно актуально в рамках рассматриваемой архитектуры в целях повышения производительности и экономии ресурсов. Несмотря на все преимущества SRP, в рамках протокола не рассматривается проблема безопасного распределения ключей в динамически организуемой сети. Кроме того, протокол SRP, как и многие другие, также подвержен атакам типа «вормхол».

Протокол SEAD (Secure Efficient Ad hoc Distance-Vector), предложенный в работе [17], базируется на принципах работы проактивного дистанционно-векторного протокола DSDV. Особенностью протокола можно считать нестандартный механизм аутентификации записей обновлений маршрутизации, основанный на цепочке хэшей и дереве Меркла [18]. В соответствии со спецификациями протокола DSDV каждая запись маршрутизации помимо метрики маршрута включает порядковый номер. Произвольный узел при получении обновления маршрута заменяет запись в таблице маршрутизации, только если порядковый номер обновления выше текущего либо значение метрики обновления меньше текущего значения при условии совпадения порядковых номеров. Каждое обновление также включает идентификатор источника маршрута и значение $h_{n-i*m+j}$ из цепочки хэшей, где $m$ – диаметр сети, $i$ – порядковый номер записи маршрута, а $j$ – значение метрики маршрута.

Таким образом, перехваченные значения цепочки хэшей не позволяют нарушителю сгенерировать обновление с более высоким порядковым номером либо с меньшей метрикой (при условии совпадения порядковых номеров). Вместе с тем данный подход не обеспечивает защиты от модификации других важных полей протокола, а процедура генерации дерева Меркла, привязанного к идентификаторам узлов сети, ограничивает применение протокола в сетях с динамической топологией.

Протокол SDSDV (Secure DSDV) [19] пересматривает подход, заложенный в протоколе SEAD. В отличие от SEAD протокол SDSDV не предусматривает построение дерева Меркла, в то время как каждый узел генерирует $2*n$ цепочек хэшей, где $n$ – количество узлов сети. Аутентификация обновлений маршрутизации производится на основе дополнительных полей AL (Alteration Field) и AC (Accumulation Field), которые используются для защиты от понижения значения метрики и повышения номера последовательности соответственно. Следует отметить, что протоколы SEAD и SDSDV обладают типичными недостатками и подвержены всем уязвимостям, характерным для протоколов данного класса.

Разработчиками реактивного протокола SAR (Security-Aware Ad-hoc Routing) [20] был предложен перспективный подход, позволяющий обеспечить

высокую степень безопасности маршрутизации. Ключевой особенностью протокола является присваивание каждому узлу некоторого уровня безопасности. Прохождение пакетов через узлы с уровнем безопасности ниже требуемого не является безопасным. При этом главной метрикой маршрута становится уровень его безопасности, а его значение определяется как наименьшее среди уровней безопасности всех узлов, входящих в маршрут до узла назначения. Обнаружение маршрутов в рамках протокола производится по запросу узла отправителя, поскольку изначально SAR был предложен как расширение безопасности протокола маршрутизации AODV. В служебный пакет запроса маршрута RREQ помещается требуемое отправителем пакетов значение метрики безопасности маршрута. В результате узлы, получившие RREQ, но не обладающие необходимым уровнем безопасности, не имеют возможности объявлять маршрут и не участвуют в дальнейшей трансляции управляющего пакета. Узел, обладающий маршрутом до узла назначения с требуемым значением метрики безопасности, отправляет узлу источника расширенный в соответствии с протоколом SAR служебный пакет RREP.

Дополнительно протокол предусматривает криптографическую защиту всех передаваемых пакетов (аутентификация и шифрование). В ситуации, когда найдено несколько маршрутов, отвечающих требованиям безопасности, передача пакетов осуществляется по маршруту с минимальным значением метрики расстояния. С другой стороны, даже для полносвязной телекоммуникационной сети вероятны случаи, когда безопасный в понимании протокола маршрут не может быть предложен.

Гибкость протокола SAR может быть расширена в рамках ролевого подхода [21], что позволяет учитывать тип информационного потока при определении безопасного маршрута. Одна из основных проблем протокола заключается в отсутствии регламентированного механизма установления уровней безопасности взаимодействующих узлов, что затрудняет его практическое применение.

Эффективный подход для противодействия атакам «блекхол», «синкхол» и «вормхол» был предложен в рамках протокола SPREAD [22]. Идея протокола заключается в применении пороговой ($k$, $n$) схемы разделения секрета [23] к передаваемым сообщениям и последующей доставке всех частей секрета до получателя по различным маршрутам на базе многопутевой маршрутизации. Поскольку для восстановления секрета потребуется $k$ частей, реализация атак типа «блекхол» или «синкхол» может быть успешной только при кооперации ($n - k$) нарушителей. Вместе с тем избыточность, образуемая при применении указанной схемы, может быть существенным ограничением во многих динамически организуемых сетях.

В целом можно отметить, что криптографические преобразования позволяют обеспечить полную аутентификацию взаимодействующих сторон и шифрование данных, передаваемых в том числе в рамках протоколов маршрутизации. Но в условиях ограниченности ресурсов в беспроводных самоорганизующихся сетях данные механизмы (особенно криптосистемы с открытым ключом) являются чересчур затратными, что вынуждает искать вспомогательные решения.

Кроме того, рассмотренные подходы не позволяют решить проблему эгоистичности узлов, а правильность информации, предоставляемой аутентифицированными узлами, не может быть гарантирована в рамках схем защиты, основанных исключительно на криптографических преобразованиях. Таким образом, все протоколы маршрутизации, безопасность которых обеспечивается по данным схемам (с определенными оговорками, за исключением протоколов SAR и SPREAD), уязвимы к атакам внутренних нарушителей и зараженных узлов, поскольку предполагается, что любой аутентифицированный узел является доверенным узлом без какой-либо дополнительной проверки.

**Расширения безопасности протоколов маршрутизации на основе концепции доверия**

Существует тесная взаимосвязь между понятиями «доверие» и «безопасность». Опираясь на концепцию доверия, можно существенно повысить уровень сетевой безопасности. Репутация является основной характеристикой узлов сети в рамках протоколов маршрутизации, базирующихся на установлении доверительных отношений между узлами и их кооперации. В результате кооперации в отношении узлов с плохой репутацией могут быть приняты специальные меры, включая их изоляцию.

Основные принципы концепции доверия в сетях MANET были сформированы в работе [24].

1. Метод определения доверия к взаимодействующему узлу должен быть полностью распределенным ввиду отсутствия третьей доверенной стороны (по типу удостоверяющего центра).

2. Определение доверия должно производиться гибким настраиваемым способом без излишней вычислительной и коммуникационной нагрузки, с учётом всей сложности и полноты доверительных отношений.

3. Определение доверия в MANET не должно строиться на готовности к сотрудничеству всех узлов. В условиях ограниченных ресурсов эгоизм сторон может преобладать над готовностью к сотрудничеству, например для экономии вычислительной мощности или расхода заряда батареи.

4. Доверие является динамическим, а не статическим.

5. Доверие носит субъективный характер.

6. Доверие не обязательно транзитивно. Тот факт, что $A$ доверяет $B$ и $B$ доверяет $C$, не означает, что $A$ доверяет $C$.

7. Доверие асимметрично и не обязательно является взаимным.

8. Доверие зависит от контекста. $A$ может доверять $B$ в одном качестве и не доверять в другом. Например, для решения трудоёмкой вычислительной

задачи в MANET узел с высокой вычислительной мощностью будет рассматриваться как доверенный, в то время как узел, который имеет низкую вычислительную мощность, но не является вредоносным, будет рассматриваться как недоверенный.

В качестве одного из первых протоколов маршрутизации, основанных на установлении доверия и кооперации, был разработан протокол CORE [25]. Указанный протокол базируется на механизмах реактивного протокола маршрутизации DSR и предполагает определение каждым узлом прямой (на основе собственных наблюдений) и косвенной (на основе сообщений от других узлов) репутации других узлов. Кроме того, протокол вводит понятие функциональной репутации как репутации, связанной с одной определенной задачей (например, пересылка пакетов), и глобальной репутации, которая вычисляется с учётом всех функциональных репутаций и их весовых коэффициентов. Протокол разработан для принятия решений о сотрудничестве или постепенной изоляции узла. Уникальной особенностью протокола CORE является то, что он предусматривает обмен только позитивной информацией о репутации, что, с одной стороны, позволяет обеспечить защиту от атак на «отказ в обслуживании», но, с другой стороны, оставляет возможность для кооперации злоумышленников в целях завышения своей репутации.

Другим расширением протокола DSR, построенным на основе концепции доверия и кооперации узлов, является протокол безопасной маршрутизации CONFIDANT [26]. Его реализация на каждом узле включает подсистему репутации, монитор, диспетчер маршрутов и менеджер доверия. Узлы, передающие пакеты, могут обнаруживать отклонения в поведении следующих по маршруту узлов с помощью механизма пассивного подтверждения или путем наблюдения за поведением протокола маршрутизации. Монитор каждого узла регистрирует отклонения от нормального поведения, и в тех случаях, когда регистрируется плохое поведение, вызывается подсистема репутации. В рамках доверительных отношений узлы также могут делиться этой информацией с соседними узлами, что подразумевает комбинированное определение уровня доверия узлов. Диспетчер доверия работает с таблицей аварийных сигналов, таблицей доверия и таблицей узлов.

Таблица аварийных сигналов включает информацию о принятых тревожных сигналах. В таблице доверия содержатся уровни доверия узлов, позволяющие определить достоверность принимаемых тревожных сигналов. В таблице узлов перечислены все узлы, отправляющие сигналы тревоги. Подсистема репутации управляет таблицей узлов, участвующих в передаче пакетов, и их уровнем доверия. Уровень доверия к узлу изменяется только тогда, когда злонамеренное поведение этого узла было зафиксировано несколько раз (выше некоторого порогового значения), чтобы исключить совпадения. Если уровень доверия к узлу ухудшится настолько, что выйдет из допустимого диапазона, будет вызван диспетчер маршрутов, который выполнит пересчёт маршрута в соответствии с базовой метрикой безопасности (например, уровнем доверия).

Значительное количество расширений безопасности, построенных на основе концепции доверия, предложено для реактивного протокола AODV. Например, в работе [27] предложен адаптивный протокол, предусматривающий определение коэффициента доверия для каждого узла и требуемого уровня безопасности данных. В рамках указанного протокола предлагается определять уровень доверия к узлам и использовать различную длину ключа шифрования для различных сообщений протокола AODV в зависимости от уровня доверия к узлам и требуемого уровня безопасности для передаваемых данных, что позволит снизить накладные расходы на криптографические преобразования. Вместе с тем в рамках указанного подхода не рассматривается методика определения самого коэффициента доверия.

Протокол TAODV (Trusted AODV) [28] также является модификацией протокола AODV, его главное отличие – установление доверительных отношений между всеми узлами сети. Текущий узел выбирает для последующей передачи только те узлы, с которыми установлены доверительные отношения. Узлы, преднамеренно выполняющие неправомерные действия, после обнаружения будут изолированы.

Модель доверия, реализуемая в рамках протокола TAODV, основывается на трехмерной метрике:

$$\omega_B^A = (b_B^A, d_B^A, u_B^A),$$

где $\omega_B^A$ – мнение узла $A$ об узле $B$; $b$ – степень доверия; $d$ – степень недоверия; $u$ – степень неуверенности. Причем

$$b_B^A + d_B^A + u_B^A = 1.$$

В этом выражении степень доверия характеризует вероятность, с которой узел $A$ может доверять узлу $B$, а степень недоверия характеризует вероятность, с которой узел $A$ не может доверять узлу $B$. Тогда степень неуверенности определяет случаи, в которых отсутствуют как доверие, так и недоверие, причем сумма этих трех элементов равняется 1.

Пусть $p$ – количество успешных взаимодействий, а $n$ – количество безрезультатных взаимодействий узла $A$ с узлом $B$. Тогда мнение узла $A$ об узле $B$ вычисляется следующим образом:

$$\begin{cases} b_B^A = \dfrac{p}{p+n+2}, \\ d_B^A = \dfrac{n}{p+n+2}, \\ u_B^A = \dfrac{2}{p+n+2}. \end{cases}$$

Модель при этом является динамической, поскольку мнения узлов со временем изменяются. Протокол предполагает сотрудничество узлов при вычислении каждым узлом указанной трехмерной метрики. Данное сотрудничество реализуется посредством специальных служебных сообщений:

TREQ – широковещательный запрос мнения, TREP – предоставление мнения. В рамках предложенной модели каждый раз при получении управляющих пакетов базового протокола от узла *B*, узел *A* посредством запросов TREQ и ответов TREP собирает мнения всех соседних узлов об узле *B* и объединяет их все, включая уже имеющееся мнение узла *A* об узле *B*, на базе операций дисконтирования и согласования.

Дисконтирование мнения узла *B* об узле *C* при определении мнения узла *A* об узле *C* производится по следующим правилам:

$$\begin{cases} b_C^{AB} = b_B^A b_C^B, \\ d_C^{AB} = b_B^A d_C^B, \\ u_C^{AB} = d_B^A + u_B^A + b_B^A u_C^B. \end{cases}$$

Согласование мнений узлов *A* и *B* об узле *C* производится по следующим правилам:

$$\begin{cases} b_C^{A,B} = (b_C^A u_C^B + b_C^B u_C^A)/k, \\ d_C^{A,B} = (d_C^A u_C^B + d_C^B u_C^A)/k, \\ u_C^{A,B} = (u_C^A u_C^B)/k \ , \end{cases}$$

$$k = u_C^A + u_C^B - 2u_C^A u_C^B.$$

Дальнейшие действия узла *A* зависят от сформированного мнения об узле *B*. Причем решение принимается на основе предложенных в рамках протокола критериев (таблица).

**Критерии для оценки доверия**

| Степень доверия | Степень недоверия | Степень неуверенности | Действие |
|---|---|---|---|
| | | >0,5 | Запросить и проверить цифровую подпись |
| | >0,5 | | Изолировать узел на определенный период |
| >0,5 | | | Доверять узлу и осуществлять маршрутизацию |
| <0,5 | <0,5 | <0,5 | Запросить и проверить цифровую подпись |

Протокол также предусматривает модификацию управляющих пакетов запроса и предоставления маршрутов (TRREQ и TRREP) исходного протокола AODV за счёт включения дополнительных полей для реализации модели и расширение таблицы маршрутизации за счёт трех дополнительных полей для каждой записи узла: количество успешных взаимодействий, количество безрезультатных взаимодействий, значение метрики (мнение).

Аналогичный, но значительно упрощенный подход использован в рамках протокола GradeTrust [29]. Протокол не предполагает кооперации узлов при вычислении уровня доверия, но предусматривает классификацию всех узлов сети в соответствии с уровнем доверия к ним на три равные группы для того, чтобы минимизировать количество маршрутизируемых пакетов через узлы с низким уровнем доверия. Несмотря на минимальные накладные расходы, такой подход не может гарантировать достаточный уровень защиты даже от атак типа «грейхол».

Применение концепции доверия возможно не только в рамках реактивных протоколов маршрутизации, но также для обеспечения защиты проактивных и гибридных протоколов маршрутизации. В частности, в работе [30] предлагается комбинированное обеспечение защиты проактивного протокола маршрутизации OLSR на основе криптографических механизмов и концепции доверия. Аутентификация всех сообщений протокола производится на основе электронной подписи, генерируемой отправителем. Каждый узел предоставляет свой открытый ключ при установлении соседских отношений с другими узлами. Кроме того, обеспечение защиты указанного протокола строится на валидации сообщений HELLO и TC всех узлов и пакетов данных, маршрутизируемых шлюзами MPR. Каждый узел устанавливает доверительные отношения со всеми симметричными соседями, предоставляющими корректную информацию. В рамках обеспечения безопасности протокола OLSR любой узел, во-первых, контролирует поведение соседних узлов на его соответствие спецификациям протокола, а во-вторых, производит контроль поведения выбранных шлюзов MPR. Выбор шлюзов MPR является критичной операцией, поскольку именно шлюзы MPR осуществляют маршрутизацию пакетов для каждого узла и обеспечивают доступность узла для удаленных узлов. Контроль поведения соседних узлов производится исходя из следующих свойств протокола:

1. Узлы-селекторы некоторого шлюза MPR, объявляемые в сообщении TC, должны являться симметричными соседями этого шлюза.

2. Каждый шлюз MPR, объявляющий некоторый узел-селектор в сообщении TC, должен быть объявлен как соседний шлюз MPR в сообщении HELLO указанного узла-селектора.

3. При пересылке шлюзом MPR сообщений TC или пакетов данных некоторого узла перенаправленное сообщение должно быть идентично сообщению, сгенерированному самим узлом.

Контроль поведения выбранных шлюзов MPR производится исходя из следующих свойств протокола.

1. Каждый выбранный шлюз MPR должен генерировать сообщения TC, правильно объявляющие его узлы-селекторы.

2. Каждый выбранный шлюз MPR должен осуществлять маршрутизацию пакетов данных и управляющих сообщений TC, отправленных его селекторами.

Корреляция между полученными сообщениями позволяет узлам проверять указанные свойства. В случае обнаружения нарушений некоторым соседним узлом указанных свойств доверительные и соседские отношения с этим узлом могут быть разорваны. В случае обнаружения нарушений выбранным шлюзом MPR указанных свойств узел теряет соответствующий статус и доверительные отноше-

ния с этим узлом также разрываются. Кроме того, при обнаружении нарушений узлы генерируют широковещательные оповещения, прилагая в качестве доказательства подписанные сообщения, свидетельствующие о нарушении. Кооперация узлов позволяет распространять по сети указанные оповещения и использовать их для изоляции эгоистичных узлов и узлов-нарушителей.

Альтернативный подход к обеспечению безопасности OLSR на основе концепции доверия представлен в работе [31]. В предложенной модели оценка уровня доверия узлов производится на основе нечетких сетей Петри. Кроме того, авторами предложен алгоритм выбора пути с максимальным уровнем доверия среди всех возможных путей. Для организации сотрудничества узлов в целях реализации указанной модели в работе предложена расширенная версия исходного протокола FPNT-OLSR.

Перспективный подход к защите протоколов маршрутизации от атак типа «блекхол» и «синкхол» предложен в рамках схемы ActiveTrust [32]. Суть подхода заключается в активном выявлении нарушителей в ходе предварительного установления множества маршрутов до получателя. Выявление нарушителей происходит в результате расчёта уровня доверия к маршрутизирующим узлам на основе полученных от других узлов рекомендаций и сравнения рассчитанного уровня доверия с некоторым пороговым значением.

Основные положения концепции доверия также широко используются в целом ряде других работ, предназначенных для обнаружения атак на протоколы маршрутизации в телекоммуникационных сетях с динамической топологией [33–36].

**Выводы и анализ направлений для дальнейших исследований**

Исходя из представленного анализа, можно сделать вывод, что для обеспечения безопасности протоколов маршрутизации в телекоммуникационных сетях с динамической топологией требуется комбинированное применение рассмотренных подходов, включая механизмы криптографической защиты и применение подхода, основанного на концепции доверия и кооперации узлов. Выбор безопасного маршрута для доставки пакетов может основываться на уровне безопасности узлов, обоснованным также выглядит применение многопутевой маршрутизации. Для минимизации накладных расходов степень применяемых криптографических преобразований может зависеть от уровня репутации узлов и общей безопасности маршрута. При этом ряд проблем, связанных с применением концепции доверия, остаются открытыми и требуют дальнейших исследований.

1. Большинство уже разработанных протоколов и моделей обеспечения безопасности маршрутизации в рамках применения концепции доверия в основном полагаются на отслеживание сброшенных пакетов в результате реализации рассмотренных сетевых атак. Такой подход не позволяет отслеживать сетевые атаки, связанные со злонамеренным ухудшением качества маршрутов, включая необоснованную мобильность и внесение дополнительных задержек при передаче пакетов. Также редко учитываются социальные характеристики узлов сети, что позволяет внутренним нарушителям игнорировать сотрудничество с другими узлами (проблема эгоистичности) либо злонамеренно распространять ошибочные сигналы или рекомендации. Решение указанных проблем возможно в результате обеспечения маршрутизации с множественными ограничениями, включая ограничения по качеству каналов связи и социальным свойствам узлов сети, что является вычислительно сложной задачей. Альтернативный вариант решения требует разработки комплексной метрики маршрутизации, объединяющей в себе критерии качества маршрутов, специализированные для сетей с динамической топологией, а также социальные характеристики узлов сети, формирующих маршруты доставки пакетов.

2. Необходимы методы определения оптимального порогового значения уровня репутации или комплексной метрики маршрутов в различных сценариях. Очевидно, что указанное пороговое значение будет определять эффективность реализации концепции доверия и безопасность маршрутизации в целом. Правильный выбор порогового значения позволит минимизировать количество ошибок первого и второго рода и тем самым обеспечить эффективность и безопасность маршрутизации. Решение указанной проблемы требует определения перечня факторов, влияющих на доверительный порог.

3. Трудно оценить влияние доверия на эффективность маршрутизации. Очевидно, что недостаточный уровень доверия к некоторым узлам сети может приводить к выбору менее производительных маршрутов в целях обеспечения безопасности маршрутизации. Для решения указанной проблемы требуется определить, как можно минимизировать негативный эффект концепции доверия на производительность сетевого взаимодействия.

4. Эффективность применяемой модели обеспечения безопасности маршрутизации во многом может зависеть от архитектуры, назначения и свойств рассматриваемой динамически организуемой сети. Выбор адекватного решения в каждом конкретном сценарии также представляет серьёзную задачу.

Работа выполнена при финансовой поддержке гранта Президента Российской Федерации для государственной поддержки молодых российских ученых – кандидатов наук МК-2592.2018.9.

*Литература*

1. Cunha F. Data communication in VANETs: Protocols, applications and challenges / F. Cunha, Villas L., Boukerche A. et al. // Ad Hoc Networks. – 2016. – Vol. 44. – P. 90–103.

2. Bekmezci I. Flying Ad-Hoc Networks (FANETs): A survey / I. Bekmezci, O.K. Sahingoz, S. Temel // Ad Hoc Networks. – 2013. – Vol. 11, No. 3. – P. 1254–1270.

3. Perkins C.E. Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers / C.E. Perkins, P. Bhagwat // Proc. of SIGCOMM’94 Conf. on

Communications Architectures, Protocols and Applications. – 1994. – P. 234–244.

4. Optimized link state routing protocol for ad hoc networks / P. Jacquet et al. // Proc. of IEEE INMIC 2001 Multi Topic Conf. – 2001. – P. 62–68.

5. RFC7181: The Optimized Link State Routing Protocol Version 2 / T. Clausen, C. Dearlove, P. Jacquet, U. Herberg. – 2014. – URL: https://tools.ietf.org/html/rfc7181 (дата обращения: 01.06.2018).

6. Perkins C.E. Ad hoc on-demand distance vector (AODV) routing. No. RFC 3561 / C.E. Perkins, E. Belding-Royer, S. Das. – 2003. – URL: https://www.ietf.org/rfc/rfc3561 (дата обращения: 01.06.2018).

7. Johnson D.B. Dynamic Source Routing in Ad Hoc Wireless Networks / D.B. Johnson, D.A. Maltz // Mobile Computing. – 1996. – Vol. 353. – P. 153–181.

8. Haas Z.J. The Routing Algorithm for the Reconfigurable Wireless Networks // Proc. of IEEE ICUPC 1997 Conf. – 1997. – Vol. 2. – P. 562–566.

9. Karlof C. Secure routing in wireless sensor networks: Attacks and countermeasures / C. Karlof, D. Wagner // Ad Hoc Networks. – 2003. – Vol. 1, No. 2-3. – P. 293–315.

10. Pathan A.S.K. Security of self-organizing networks: MANET, WSN, WMN, VANET. – New York: CRC Press, 2016. – 638 p.

11. Clausen T. Security Threats to the Optimized Link State Routing Protocol Version 2 (OLSRv2). No. RFC 8116 / T. Clausen, U. Herberg, J. Yi. – 2017. – URL: https://tools.ietf.org/html/rfc8116 (дата обращения: 01.06.2018).

12. Zapata M.G. Secure ad hoc on-demand distance vector routing / M.G. Zapata, N. Asokan // ACM Mobile Computing and Communications Review. – 2002. – Vol. 6, No. 3. – P. 106–107.

13. A secure routing protocol for ad hoc networks / K. Sanzgiri et al. // Proc. of 10th IEEE International Conference on Network Protocols. – 2002. – P. 78–87.

14. Securing the OLSR protocol / C. Adjih et al. // Proc. of Med-Hoc-Net. – 2003. – P. 25–27.

15. Papadimitratos P. Secure link state routing for mobile ad hoc networks / P. Papadimitratos, Z.J. Haas // Proc. of Symposium on Applications and the Internet Workshops. – 2003. – P. 379–383.

16. Papadimitratos P. Secure routing for mobile ad hoc networks / P. Papadimitratos, Z.J. Haas // Proc. of SCS Communication Networks and Distributed Systems Modeling and Simulation Conf. (CNDS 2002). – 2002. – P. 1–12.

17. Hu Y.C. SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks / Y.C. Hu, D.B. Johnson, A. Perrig // Ad Hoc Networks. – 2003. – Vol. 1(1). – P. 175–192.

18. Merkle R.C. A digital signature based on a conventional encryption function // Conf. on the Theory and Application of Cryptographic Techniques. – 1987. – P. 369–378.

19. Wang J.W. A secure DSDV routing protocol for ad hoc mobile networks / J.W. Wang, H.C. Chen, Y.P. Lin // Proc. of Fifth International Joint Conference on INC, IMS and IDC, 2009 (NCM'09). – 2009. – P. 2079–2084.

20. Yi S. Security-aware ad hoc routing for wireless networks / S. Yi, P. Naldurg, R. Kravets // Proc. of the 2nd ACM international symposium on Mobile ad hoc networking & computing. – 2001. – P. 299–302.

21. Shcherba E.V. A role-based approach to secure routing in wireless ad-hoc networks / E.V. Shcherba, V.I. Nikonov // Proc. of 2016 International Siberian Conference on Control and Communications (SIBCON), IEEE. – 2016. – P. 1–5.

22. Lou W. SPREAD: Improving network security by multipath routing / W. Lou, W. Liu, Y. Fang // Military Communications Conf., 2003 (MILCOM'03). – 2003. – Vol. 2. – P. 808–813.

23. Shamir A. How to share a secret // Communications of the ACM. – 1979. – Vol. 22(11). – P. 612–613.

24. Cho J.H. A survey on trust management for mobile ad hoc networks / J.H. Cho, A. Swami, R. Chen // IEEE Communications Surveys & Tutorials. – 2011. – Vol. 13, No. 4. – P. 562–583.

25. Michiardi P. CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks / P. Michiardi, R. Molva // Advanced communications and multimedia security. – 2002. – P. 107–121.

26. Buchegger S. Performance analysis of the CONFIDANT protocol / S. Buchegger, J.Y. Le Boudec // Proc. of the 3rd ACM international symposium on Mobile ad hoc networking & computing. – 2002. – P. 226–236.

27. Nekkanti R.K. Trust based adaptive on demand ad hoc routing protocol / R.K. Nekkanti, C.W. Lee // Proc. of the 42nd annual Southeast regional conference. – 2004. – P. 88–93.

28. Li X. A trust model based routing protocol for secure ad hoc networks / X. Li, M.R. Lyu, J. Liu // Proc. of Aerospace Conference, 2004, IEEE. – 2004. – Vol. 2. – P. 1286–1295.

29. Airehrour D. GradeTrust: A secure trust based routing protocol for MANETs / D. Airehrour, J. Gutierrez, S.K. Ray // Proc. of 2015 International Telecommunication Networks and Applications Conf. (ITNAC), IEEE. – 2015. – P. 65–70.

30. Adnane A. Trust-based security for the OLSR routing protocol / A. Adnane, C. Bidan, R.T. de Sousa Júnior // Computer Communications. – 2013. – Vol. 36(10-11). – P. 1159–1171.

31. Tan S. Trust based routing mechanism for securing OSLR-based MANET / S. Tan, X. Li, Q. Dong // Computer Communications. – 2015. – Vol. 30. – P. 84–98.

32. ActiveTrust: Secure and trustable routing in wireless sensor networks / Y. Liu, M. Dong, K. Ota, A. Liu // IEEE Transactions on Information Forensics and Security. – 2016. – Vol. 11, No. 9. – P. 2013–2027.

33. Enhanced trust aware routing against wormhole attacks in wireless sensor networks / R.W. Anwar et al. // Proc. of 2015 International Conference on Smart Sensors and Application (ICSSA), IEEE. – 2015. – P. 56–59.

34. Naderi O. A trust based routing protocol for mitigation of sinkhole attacks in wireless sensor networks / O. Naderi, M. Shahedi, S.M. Mazinani // International Journal of Information and Education Technology. – 2015. – Vol. 5, No. 7. – P. 520–526.

35. Poongodi M. A novel intrusion detection system based on trust evaluation to defend against DDoS attack in MANET / M. Poongodi, S. Bose // Arabian Journal for Science and Engineering. – 2015. – Vol. 40, No. 12. – P. 3583–3594.

36. Ishmanov F. Trust Mechanisms to Secure Routing in Wireless Sensor Networks: Current State of the Research and Open Research Issues / F. Ishmanov, Y. Bin Zikria // Journal of Sensors. – 2017. – Vol. 2017. – P. 1–16.

**Щерба Евгений Викторович**
Канд. техн. наук, доцент каф.
комплексной защиты информации (КЗИ)
Омского государственного технического ун-та (ОмГТУ)
Мира пр-т, д. 11, г. Омск, Россия, 644050
ORCID 0000-0003-4401-4343
Тел.: +7 (381-2) 21-77-02
Эл. почта: evscherba@gmail.com

**Никонов Вячеслав Игоревич**
Канд. техн. наук, доцент каф. средств связи
и информационной безопасности (ССИБ) ОмГТУ
Мира пр-т, д. 11, г. Омск, Россия, 644050
Тел.: +7 (381-2) 65-85-60
Эл. почта: vi.nikonov@gmail.com

**Литвинов Георгий Александрович**
Магистрант каф. ССИБ ОмГТУ
Мира пр-т, д. 11, г. Омск, Россия, 644050
Тел.: +7 (381-2) 65-85-60
Эл. почта: georgyfunds@gmail.com

Shcherba E.V., Nikonov V.I., Litvinov G.A.
**Securing Routing Protocols for Wireless Networks with Dynamic Topology**

The presented paper contains a comparative survey of current security threats and approaches applied to the protection of routing protocols for telecommunication networks with dynamic topology, including MANET, WSN, and other types of networks. More than 20 significant and promising routing protocols are considered in the paper. Cryptographic protection and protection based on the concept of trust are the basic approaches to ensure the security of these protocols. The authors highlight the advantages, disadvantages and vulnerabilities of the protocols examined, and also identify promising areas for further research.
**Keywords:** wireless ad-hoc networks, MANET, VANET, FANET, WSN, routing vulnerabilities, network security.
**doi:** 10.21293/1818-0442-2018-21-3-19-29

*References*

1. Cunha F., Villas L., Boukerche A., Maia G., Viana A., Mini R.A., Loureiro A.A. Data communication in VANETs: Protocols, applications and challenges. *Ad Hoc Networks*, 2016, vol. 44, pp. 90–103.

2. Bekmezci I., Sahingoz O.K., Temel S. Flying Ad-Hoc Networks (FANETs): A survey. *Ad Hoc Networks*, 2013, vol. 11, no. 3, pp. 1254–1270.

3. Perkins C.E., Bhagwat P. Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. *Proc. of SIGCOMM'94 Conf. on Communications Architectures, Protocols and Applications*, 1994, pp. 234–244.

4. Jacquet P., Muhlethaler P., Clausen T., Laouiti A., Qayyum A., Viennot L. Optimized link state routing protocol for ad hoc networks. *Proc. of IEEE INMIC 2001 Multi Topic Conf.*, 2001, pp. 62–68.

5. Clausen T., Dearlove C., Jacquet P., Herberg U. RFC7181: The Optimized Link State Routing Protocol Version 2. 2014. Available at: https://tools.ietf.org/html/rfc7181 (accessed: 01.06.2018).

6. Perkins C.E, Belding-Royer E., Das S. Ad hoc on-demand distance vector (AODV) routing. No. RFC 3561, 2003. Available at: https://www.ietf.org/rfc/rfc3561 (accessed: 01.06.2018).

7. Johnson D.B., Maltz D.A. Dynamic Source Routing in Ad Hoc Wireless Networks. *Mobile Computing*, 1996, vol. 353, pp. 153–181.

8. Haas Z.J. The Routing Algorithm for the Reconfigurable Wireless Networks. *Proc. of IEEE ICUPC 1997 Conf.*, 1997, vol. 2, pp. 562–566.

9. Karlof C., Wagner D. Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad Hoc Networks*, 2003, vol. 1, no. 2-3, pp. 293–315.

10. Pathan A.S.K. *Security of self-organizing networks: MANET, WSN, WMN, VANET*. New York, CRC Press, 2016, 638 p.

11. Clausen T., Herberg U., Yi J. Security Threats to the Optimized Link State Routing Protocol Version 2. No. RFC 8116, 2017. Available at: https://tools.ietf.org/html/rfc8116 (accessed: 01.06.2018).

12. Zapata M.G., Asokan N. Secure ad hoc on-demand distance vector routing. *ACM Mobile Computing and Communications Review*, 2002, vol. 6, no. 3, pp. 106–107.

13. Sanzgiri K., Dahill B., Levine B.N., Shields C., Belding-Royer E.M. A secure routing protocol for ad hoc networks. *Proc. of 10th IEEE International Conference on Network Protocols*, 2002, pp. 78–87.

14. Adjih C., Clausen T., Jacquet P., Laouiti A., Muhlethaler P., Raffo D. Securing the OLSR protocol. *Proc. of Med-Hoc-Net*, 2003, pp. 25–27.

15. Papadimitratos P., Haas Z.J. Secure link state routing for mobile ad hoc networks. *Proc. of Symposium on Applications and the Internet Workshops*, 2003, pp. 379–383.

16. Papadimitratos P., Haas Z.J. Secure routing for mobile ad hoc networks. *Proc. of SCS Communication Networks and Distributed Systems Modeling and Simulation Conf. (CNDS 2002)*, 2002, pp. 1–12.

17. Hu Y.C., Johnson D.B., Perrig A. SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. *Ad Hoc Networks*, 2003, vol. 1(1), pp. 175–192.

18. Merkle R.C. A digital signature based on a conventional encryption function. *Proc, of Conf. on the Theory and Application of Cryptographic Techniques*, 1987, pp. 369–378.

19. Wang J.W., Chen H.C., Lin Y.P. A secure DSDV routing protocol for ad hoc mobile networks. *Proc. of Fifth International Joint Conference on INC, IMS and IDC*, 2009 (NCM'09), 2009, pp. 2079–2084.

20. Yi S., Naldurg P., Kravets R. Security-aware ad hoc routing for wireless network. *Proc. of the 2nd ACM international symposium on Mobile ad hoc networking & computing*, 2001, pp. 299–302.

21. Shcherba E.V., Nikonov V.I. A role-based approach to secure routing in wireless ad-hoc networks. *Proc. of 2016 International Siberian Conference on Control and Communications (SIBCON), IEEE*, 2016, pp. 1–5.

22. Lou W., Liu W., Fang Y. SPREAD: Improving network security by multipath routing. *Proc. of Military Communications Conf., 2003 (MILCOM'03)*, 2003, vol. 2, pp. 808–813.

23. Shamir A. How to share a secret. *Communications of the ACM*, 1979, vol. 22(11), pp. 612–613.

24. Cho J.H., Swami A., Chen R. A survey on trust management for mobile ad hoc networks. *IEEE Communications Surveys & Tutorials*, 2011, vol. 13, no. 4, pp. 562–583.

25. Michiardi P., Molva R. CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks. *Advanced communications and multimedia security*, 2002, pp. 107–121.

26. Buchegger S., Le Boudec J.Y. Performance analysis of the CONFIDANT protocol. *Proc. of the 3rd ACM international symposium on Mobile ad hoc networking & computing*, 2002, pp. 226–236.

27. Nekkanti R.K., Lee C.W. Trust based adaptive on demand ad hoc routing protocol. *Proc. of the 42nd annual Southeast regional conference*, 2004, pp. 88–93.

28. Li X., Lyu M.R., Liu J. A trust model based routing protocol for secure ad hoc networks. *Proc. of Aerospace Conference, 2004, IEEE*, 2004, vol. 2, pp. 1286–1295.

29. Airehrour D., Gutierrez J., Ray S.K. GradeTrust: A secure trust based routing protocol for MANETs. *Proc. of 2015 International Telecommunication Networks and Applications Conf. (ITNAC), IEEE*, 2015, pp. 65–70.

30. Adnane A., Bidan C., de Sousa Júnior R.T. Trust-based security for the OLSR routing protocol. *Computer Communications*, 2013, vol. 36 (10-11), pp. 1159–1171.

31. Tan S., Li X., Dong Q. Trust based routing mechanism for securing OSLR-based MANET. *Computer Communications*, 2015, vol. 30, pp. 84–98.

32. Liu Y., Dong M., Ota K., Liu A. ActiveTrust: Secure and trustable routing in wireless sensor networks. *IEEE Transactions on Information Forensics and Security*, 2016, vol. 11, no. 9, pp. 2013–2027.

33. Anwar R.W., Bakhtiari M., Zainal A., Abdullah A.H., Qureshi K.N. Enhanced trust aware routing against wormhole attacks in wireless sensor networks. *Proc. of 2015 International Conference on Smart Sensors and Application (ICSSA), IEEE*, 2015, pp. 56–59.

34. Naderi O., Shahedi M., Mazinani S.M. A trust based routing protocol for mitigation of sinkhole attacks in wireless sensor networks. *International Journal of Information and Education Technology*, 2015, vol. 5, no. 7, pp. 520–526.

35. Poongodi M., Bose S. A novel intrusion detection system based on trust evaluation to defend against DDoS attack in MANET. *Arabian Journal for Science and Engineering*, 2015, vol. 40, no. 12, pp. 3583–3594.

36. Ishmanov F., Bin Zikria Y. Trust Mechanisms to Secure Routing in Wireless Sensor Networks: Current State of the Research and Open Research Issues. *Journal of Sensors*, 2017, vol. 2017, pp. 1–16.

**Evgeny V. Shcherba**
Candidate of Technical Sciences, Associate Professor of Department of Complex Information Security,
Omsk State Technical University (OmSTU)
11, Mira pr., Omsk, Russia, 644050
ORCID 0000-0003-4401-4343
Phone: +7 (381-2) 21-77-02
Email: evscherba@gmail.com

**Vyacheslav I. Nikonov**
Candidate of Technical Sciences, Associate Professor of Department of Communications and Information Security OmSTU
11, Mira pr., Omsk, Russia, 644050
Phone: +7 (381-2) 65-85-60
Email: vi.nikonov@gmail.com

**George A. Litvinov**
Graduate student, Department of Communications and Information Security OmSTU
11, Mira pr., Omsk, Russia, 644050
Phone: +7 (381-2) 65-85-60
Email: georgyfunds@gmail.com