УДК 004.056:004.057.4 Вестник УрФО № 1(59) / 2026, с. 58–67

Сергин Д.А., Щерба Е.В.

DOI: 10.14529/secur260106

ПРОБЛЕМА ВЫБОРА БЕЗОПАСНОГО МНОЖЕСТВА ШЛЮЗОВ ПЕРЕСЫЛКИ В РАМКАХ ПРОТОКОЛА МАРШРУТИЗАЦИИ OLSR[1]

Концепция шлюзов пересылки в рамках протокола маршрутизации OLSR позволяет оптимизировать распространение сетевых пакетов в динамически организуемых сетях. В статье затрагивается проблема нарушения сетевой связности, связанная с некорректным выбором множества шлюзов пересылки. Представлен обзор и выполнен анализ научных работ, направленных на решение указанной проблемы. Определены отличительные особенности, достоинства и недостатки альтернативных подходов к выбору шлюзов пересылки. Обозначены перспективные направления для дальнейших исследований в рамках заданной проблематики.

Ключевые слова: *безопасность маршрутизации, сетевые атаки, задача о покрытии множества, протокол OLSR, выбор MPR.*

Sergin D. A., Shcherba E. V.

THE PROBLEM OF SELECTING A SECURE SET OF MULTIPOINT RELAYS WITHIN THE OLSR ROUTING PROTOCOL

The concept of multipoint relays (MPR) within the OLSR routing protocol enables optimization of network packet propagation in dynamically organized networks. This article addresses the problem of network node availability disruption due to the incorrect selection of multipoint relays. A review and analysis of papers aimed at solving this problem is presented. The distinctive features, advantages, and disadvantages of alternative approaches to multipoint relays selection are identified. Promising directions for further research within the given problems are outlined.

Keywords: *routing security, network attacks, set cover problem, OLSR protocol, MPR elections.*

[1] Исследование выполнено в ОмГТУ в рамках государственного задания Минобрнауки России на 2026–2028 годы НИР № FSGF-2026-0003.

Введение

Проактивный протокол маршрутизации OLSR [1] является одним из наиболее востребованных протоколов маршрутизации для динамически организуемых сетей различных типов. Ключевой особенностью протокола OLSR является процедура выбора подмножества шлюзов пересылки (MPR, Multipoint Relay) среди соседних узлов, которые дают возможность маршрутизации в пределах двушаговых соседних узлов. Узел, выбранный некоторым узлом в качестве шлюза MPR, отправляет служебные сообщения TC (Topology Control) на все доступные ему узлы, тем самым объявляя маршруты до каждого узла-селектора, выбравшего его в качестве шлюза MPR, в этих сообщениях. Все MPR-шлюзы выполняют пересылку полученных сообщений TC своим узлам-селекторам. После формирования базы данных топологии сети, каждый узел вычисляет оптимальные маршруты до всех доступных узлов.

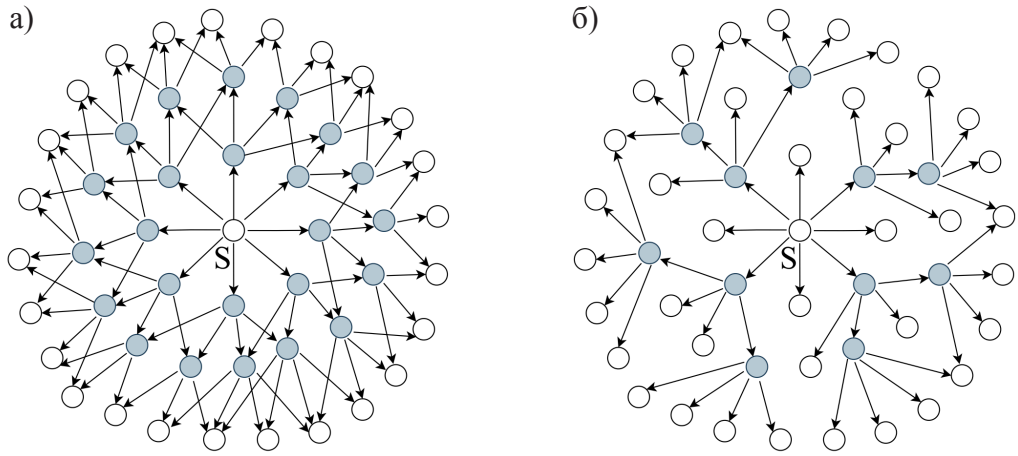

Рис. 1. Схема широковещательной рассылки: лавинная (а) и с использованием MPR (б)

Применение указанной концепции (рисунок 1) позволяет существенно сократить объём широковещательного трафика в сети путем исключения избыточных ретрансляций, производимых узлами в одной и той же физической сети.

Сама процедура выбора множества шлюзов пересылки узлом N предполагает, что узел определяет свой набор шлюзов MPR(N) из узлов, с которыми установлены симметричные отношения соседства. Выбор осуществляется таким образом, чтобы совокупные симметричные отношения соседства узлов, входящих в MPR(N), полностью охватывали все двушаговое окружение узла N (все соседи соседей узла N). То есть каждый узел в строгом симметричном двушаговом окружении узла N должен иметь хотя бы один симметричный канал с каким-нибудь узлом из MPR(N). Таким образом, чем меньше будет мощность множества MPR(N) для каждого узла сети N, тем меньше будет объём широковещательного трафика в сети.

Задача поиска оптимального множества шлюзов пересылки

Задача о покрытии множества (Set Cover Problem) широко известна в дискретной оптимизации [2] и имеет многочисленные приложения. Комбинаторная постановка задачи о покрытии множества состоит в следующем. Пусть даны множество $M = \{1, \ldots, m\}$ и набор его подмножеств $M_1, \ldots, M_n$, таких что $M_1 \cup \cup M_2 \cup \ldots \cup M_n = M$. Совокупность подмножеств M_j, $j \in J \subseteq \{1, \ldots, n\}$, называется покрытием множества M, если $\cup M_j = M$. Каждому M_j приписан вес $c_j \geq 0$. Требуется найти покрытие минимального суммарного веса. Задача называется невзвешенной, если все подмножества M_j имеют единичные веса.

Пусть задано множество вершин графа V, соответствующее множеству взаимодействующих узлов сети, множество дуг графа E, соответствующее множеству каналов связи, в множестве V задана вершина s, соответствующая узлу, для которого необходимо определить оптимальный набор шлюзов MPR. Пусть M представляет множество всех двушаговых симметричных соседей узла s, а для каждой вершины j, соседней к s, множество M_j соответствует множеству симметричных соседних узлов, за исключением самой вершины s. Тогда задача определения оптимального набора шлюзов MPR узлом s сводится к вышеприведенной постановке задачи поиска оптимального покрытия множества M.

В общем случае поиск покрытия минимального веса является NP-трудной задачей. Тем не менее для решения указанной задачи был предложен ряд приближенных алгоритмов, позволяющих осуществлять поиск решений, подходящих с некоторой погрешностью, и несколько эвристических алгоритмов, позволяющих оптимизировать поиск подходящего решения. Один из таких алгоритмов использован в рамках протокола маршрутизации OLSR для выбора оптимального множества шлюзов MPR.

В спецификациях протокола OLSR (RFC3626) [1] для выбора множества MPR предложен жадный эвристический алгоритм, целью которого является покрытие всех двушаговых соседей минимальным количеством шлюзов-ретрансляторов. Алгоритм оперирует двумя ключевыми множествами для каждого узла, выполняющего вычисления, а именно: множество одношаговых соседей (N) и множества двушаговых соседей (N2).

Ключевыми шагами алгоритма являются:

1. Во множество MPR включаются соседи из N, которые объявили готовность к ретрансляции (WILL_ALWAYS).

2. На втором этапе во множество MPR добавляются узлы из N, которые обеспечивают единственно возможный способ достижения узла из N2.

3. На третьем шаге, пока остаются непокрытые узлы из N2, происходит последовательный выбор узлов из N. Выбор происходит с учетом приоритета. В первую очередь оценивается количество узлов из N2, которые станут покрытыми с помощью выбора данного узла, во вторую очередь оценивается степень готовности к пересылке (willingness).

Таким образом, классическая реализация алгоритма позволяет минимизировать объем сетевого трафика при обеспечении полной сетевой связности, но не принимает во внимание аспекты безопасности, включая, например, обеспечение доступности сетевых узлов, что может быть использовано нарушителями для организации сетевых атак.

Модели нарушений безопасности, связанных с выбором множества шлюзов пересылки

К специфичным уязвимостям протокола маршрутизации OLSR можно отнести подверженность сетевым атакам, связанных с выбором множества шлюзов MPR [3]. В ходе подобных атак узел-нарушитель либо выбирает неполное множество шлюзов MPR, либо заставляет другие узлы вычислять некорректное множество MPR. Чтобы инициировать атаку, узел-нарушитель может либо генерировать управляющие пакеты с искажением идентификационной информации, либо сообщать о несуществующих каналах связи к другим узлам. Как следствие, узел-жертва вычисляет ошибочный набор шлюзов MPR, то есть некоторые из его соседей, доступных за два перехода, не охватываются по меньшей мере одним узлом в его множестве MPR.

Атака с подменой узла выполняется нарушителем, выдающим себя за другой узел в сети. В ходе данной атаки распространяется ложная информация об узлах, находящихся на расстоянии одного или двух шагов. Это позволяет повлиять на процесс выбора шлюзов. На рисунке 2(а) вредоносный узел x подменяет узел d и передает широковещательное сообщение HELLO, объявляющее канал связи с узлом c. Затем узел a получает сообщение HELLO от узла x, которое объявляет, что узел d имеет связь с узлами c и f. В этом случае узел a считает узел d единственным элементом в своем наборе MPR, что неверно. Таким образом, узел c становится недоступным и не сможет получить сообщения TC.

На рисунке 2(б) представлен пример, когда нарушитель влияет на выбор MPR узла на расстоянии двух шагов. Вредоносный узел x подменяет узел c. Узлы f и e генерируют сообщения HELLO, в которых указывают узел c в качестве соседа с одним переходом. В результате атаки, узел a может неправильно выбрать узлы f или e в качестве шлюзов MPR. В этом случае узлы b и d не передают TC сообщения узлу c, поскольку они не включены в множество MPR.

Атака подмены канала связи выполняется вредоносным узлом, который сообщает о несуществующем канале другим узлам в сети. Цель нарушителя состоит в том, чтобы манипулировать информацией об узлах, находящихся на расстоянии одного или двух шагов, и быть выбранным в качестве шлюза MPR. После достижения указанной цели, вредоносный узел не генерирует и не пересылает сообщения TC, что приводит к нарушению доступности для узлов-селекторов.

На рисунке 3(а) проиллюстрирована атака с нарушением лавинной рассылки из-за подмены канала. В этом примере узел x объявляет несуществующие каналы к существующим узлам e и c. Узел x отправляет сообщения HELLO и должен быть выбран в качестве шлю-

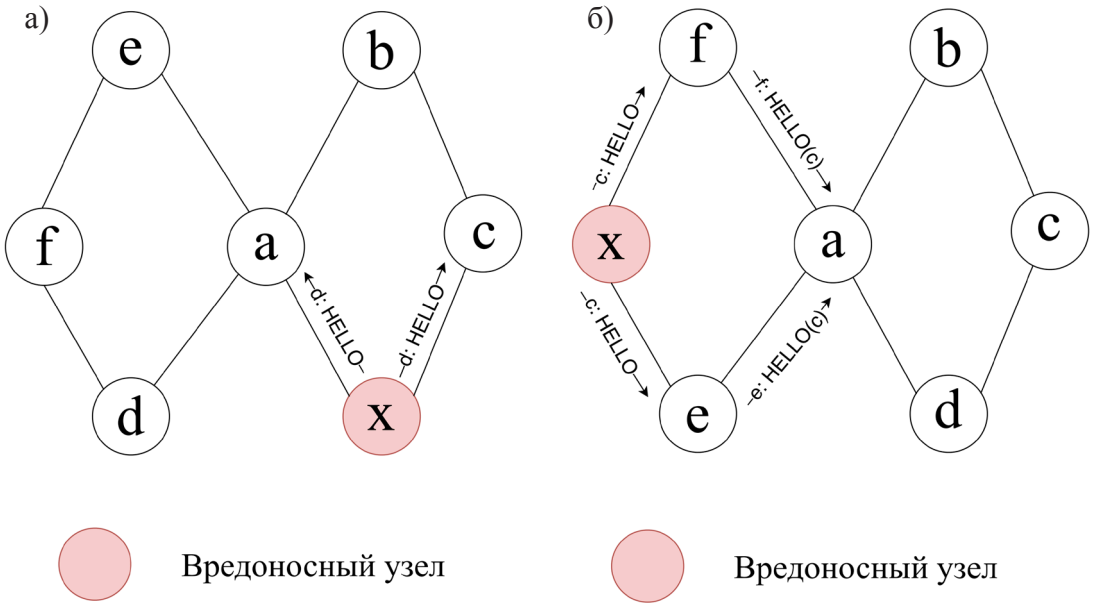

Рис. 2. Схема нарушений безопасности с подменой узла

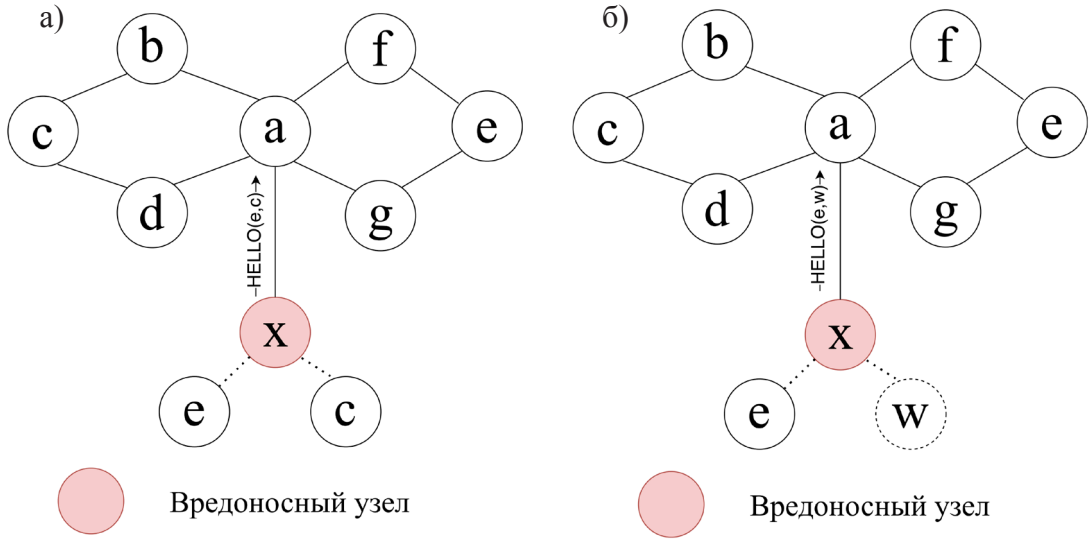

Рис. 3. Схема нарушений безопасности с подменой канала связи

за MPR узлом a. Узел a получает сообщения HELLO от узла x и неправильно вычисляет свое множество MPR, выбирая узел x как единственный узел, обеспечивающий связь с узлами e и c. В результате узел формирует ошибочный набор MPR, который может не обеспечивать покрытие всех его двушаговых соседей.

Альтернативный вариант данной атаки может быть выполнен узлом, который сообщает о канале связи с несуществующим узлом. Например, на рисунке 3(б) узел a вынужден выбрать узел x в качестве MPR, потому что это единственный узел, который обеспечивает связь с несуществующим узлом w. В этом случае вредоносный узел также получает возможность нарушить поток управляющей информации о топологии.

Причина возникновения описанных моделей атак кроется в отсутствии мер безопасности для классического протокола OLSR, где выбор множества шлюзов MPR производится без анализа достоверности полученной информации, а также без учета уровня риска для отдельно взятых узлов сети и каналов связи.

Альтернативные подходы к выбору шлюзов MPR

Для повышения доступности узлов и характеристик сетевого взаимодействия в рам-

ках протокола маршрутизации OLSR был предложен и реализован ряд альтернативных подходов к решению задачи выбора оптимального множества шлюзов MPR.

BW-OLSR

В рамках данного проекта предложен улучшенный алгоритм выбора шлюзов MPR. Особенность модификации заключается в использовании оценки пропускной способности каналов связи в качестве основной маршрутной метрики. Выбор шлюзов MPR осуществляется с помощью графов конфликтов. Согласно результатам тестирования [4], данный подход увеличивает количество шлюзов MPR в сети по сравнению со стандартной реализацией протокола, но при этом увеличивается пропускная способность всей сети.

DF-OLSR

Особенность указанной модификации протокола OLSR [5] заключается в обнаружении вредоносных узлов и их последующей изоляции от выбора в качестве шлюзов MPR. В предложенной версии протокола, узлы обмениваются как стандартными HELLO и TC сообщениями, так и сообщениями новых типов. Авторы работы предложили использовать два новых типа сообщений: VOTEFOR и VOTERPL. Сообщения VOTEFOR отправляются всем соседям на расстоянии одного шага, которые в свою очередь, пересылают эти сообщения далее своим одношаговым соседям. После получения сообщений VOTEFOR, двухшаговые соседи отправляют в ответ сообщения VOTERPL. Данные сообщения предотвращают возможность вредоносных узлов предоставлять ложную информацию о стандартных узлах, т.к. каждый узел записывает информацию, полученную с помощью количества повторов для дальнейшего сравнения, тем самым избегая выбора вредоносного узла в качестве шлюза.

TUE-OLSR

В рамках данной версии OLSR [6] предложен механизм безопасности, основанный на системе доверия между узлами. Представленный алгоритм анализирует поведение устройств и присваивает им рейтинг доверия. Рейтинг напрямую влияет на выбор узла в качестве шлюза MPR. Наиболее надежные узлы становятся шлюзами MPR. Моделирование показало, что данная модификация OLSR позволяет снизить среднюю задержку и повышает коэффициент доставки пакетов по сравнению с классическим протоколом OLSR.

PB-OLSR

Заявленная цель указанного протокола [7] заключается в повышении общей эффективности и живучести сети за счет выбора шлюзов MPR по критериям производительности и динамического уровня доверия.

Для достижения данной цели реализован следующий механизм оценки узлов. Во-первых, оценка производительности узла осуществляется с помощью метода многокритериального анализа принятия решений. Весами являются такие параметры как размер доступной оперативной памяти, уровень загрузки процессора и т.д., тем самым определяется производительность узла. Во-вторых, осуществляется проверка обработки сообщений HELLO и TC узлами сети, при этом используется метод оценки ROC на основе взвешивания критериев.

По результатам моделирования в сетевом симуляторе NS-3, применение указанного подхода позволяет уменьшить влияние вредоносных узлов, поскольку они выбираются в качестве MPR значительно реже. Кроме того, увеличивается длительность жизни маршрутов, поскольку в качестве шлюзов MPR выбираются узлы с высокой производительностью.

EM-OLSR

В данной версии протокола OLSR [8] предложена дополнительная оптимизация для классического алгоритма выбора шлюзов MPR на базе расчёта дополнительного динамического параметра узлов сети, именуемого willingness (готовность к ретрансляции, за счет оценки остаточной энергии узла и его скорости перемещения). Для оценки скорости используется GPS.

Авторы предложили три возможных значения данной характеристики:

1. willingness_high – для узлов с большим запасом энергии и малой скоростью перемещения (данные узлы считаются предпочтительными для выбора в качестве шлюзов MPR);

2. willingness_low – для узлов с высокой мобильностью и низким запасом энергии;

3. willingness_default – для типовых узлов, без выраженных отклонений.

Применение указанного критерия позволило увеличить пропускную способность соединений, уменьшить количество потерь, уменьшить энергопотребление.

W-OLSR

Авторы проекта W-OLSR (Weighted OLSR) [9] в рамках стандартного алгоритма выбора шлюзов MPR предложили использовать но-

вый критерий оценки – Weighted-MPR. Значение указанной метрики зависит от трех характеристик узла – уровень остаточной энергии, уровень сигнала, уровень задержки. Задаваемые коэффициенты определяют вклад каждой характеристики в значение Weighted-MPR. Если рассчитанное значение не превышает заданный порог, то узел может быть выбран в качестве MPR. В ходе моделирования было продемонстрировано увеличение пропускной способности соединений и снижение потерь пакетов.

EOLSR, EOLSR-EC, EOLSR-RE

Цель разработки и применения указанных протоколов [10] заключается в продлении времени функционирования беспроводной сети в условиях разряда аккумуляторов устройств. Для реализации протоколов осуществляется модификация служебных сообщений TC и HELLO. В данные сообщения, в зависимости от реализации добавляются следующие метрики – остаточная энергия (RE) и потраченная энергия (EC).

В случае с EOLSR-RE решение о назначении узла в качестве MPR принимается на основе уровня остаточной энергии. Если значение ниже заданного порога, то узел не будет выбран в качестве MPR. В модификации EOLSR-EC в качестве MPR выбирается узел с наименьшим потреблением энергии. Результаты моделирования показывают, что подход, использованный для протокола EOLSR-RE, является оптимальным, и наблюдается увеличение энергоэффективности сети.

M-OLSR

Протокол M-OLSR [11] предоставляет возможность каждому узлу самостоятельно решить, в какой момент ему обновлять служебные сообщения HELLO и TC. Данный способ позволяет минимизировать стоимость маршрута по критерию количества переходов и энергозатрат. В рамках предложенного протокола осуществляется контроль остаточной энергии узла, и когда он опускается ниже определенного порога, выбирается другой маршрут. Таким образом, для анализа и выбора маршрутов, учитываются сквозная задержка и остаточная энергия узлов.

Результаты моделирования показывают, что при использовании протокола наблюдается уменьшение объема служебного трафика и снижение энергопотребления, что также сопровождается снижением средней пропускной способности относительно классического протокола OLSR.

OLSR-ETX-ML-MD

В исследовании [12] представлен сравнительный анализ трех протоколов, в каждом из которых используется своя метрика:

1. OLSR-ETX предусматривает оценку качества каналов связи на основе успешного обмена сообщениями HELLO. В качестве шлюзов MPR выбираются узлы с наибольшим количеством надежных соседей.

2. OLSR-ML – качество каналов связи оценивается по критерию потерь пакетов.

3. OLSR-MD – в качестве основной характеристики для оценки каналов связи используется задержка.

Моделирование показало, применение протокола OLSR-ETX, из предложенных вариантов, позволяет оптимизировать среднюю задержку и пропускную способность соединений.

MOB-2-OLSR

Целью модификации MOB-2-OLSR [13] является продление времени функционирования сети. При этом ключевым параметром для оценки является мобильность узлов. Предпочтение в выборе в качестве шлюза MPR отдается узлам с наименьшей мобильностью (скоростью перемещения), благодаря чему, увеличивается время жизни сети.

Результаты моделирования показывают, что применение данного протокола вместо OLSR позволяет повысить коэффициент доставки пакетов (PDR), а также увеличить пропускную способность соединений и снизить среднюю задержку.

EDCR-OLSR

В данной работе [14] предложен новый подход к выбору шлюзов MPR. Авторы предложили использовать распределение нагрузки по аналогии с многоядерными процессорами, где нагрузка разделяется на несколько ядер. В данном случае предлагается выбирать некоторое число шлюзов MPR, которые должны функционировать совместно. То есть, в качестве шлюзов MPR выбирается несколько узлов, которые способны разделить нагрузку между собой, что должно значительно повысить отказоустойчивость всей сети.

Результаты моделирования показали, что данный подход уменьшает общее энергопотребление сети, а также увеличивает коэффициент доставки пакетов.

OLSR-AAD

В рамках протокола OLSR-AAD [15] предложено использовать новую метрику при выборе шлюзов MPR – «средний возраст смер-

Таблица 1

Сравнительный анализ модификаций протокола OLSR

Протокол	Основная метрика при выборе MPR	Особенности выбора шлюзов MPR	Новые типы сообщений	Противодействие вредоносным узлам	Ключевая цель модификации
BW-OLSR	Пропускная способность	Граф конфликтов	Нет	Нет	Максимизация пропускной способности соединений
DF-OLSR	Уровень репутации	Изоляция ненадёжных узлов, учет задержки	Да (VOTEFOR, VOTERPL)	Да	Повышение безопасности
TUE-OLSR	Комбинированная репутационная метрика	Стандартный по метрике, с предварительной изоляцией ненадёжных узлов	Нет	Да	Повышение доступности узлов
PB-OLSR	Производительность (RAM, CPU)	Многокрите-риальная оптимизация	Нет	Да	Повышение эффективности маршрутизации
EM-OLSR	Потребление энергии	Стандартный, с расчётом willingness	Нет	Нет	Повышение энергоэффективности
W-OLSR	Комбинированная метрика (энергия, сигнал, задержка)	Стандартный по метрике	Нет	Нет	Повышение доступности и эффективности
EOLSR-RE/EC	Потребление энергии	Пороговые значения	Нет, но изменен формат сообщений	Нет	Увеличение времени жизни сети
M-OLSR	Потребление энергии	Адаптивная стратегия	Нет	Нет	Снижение нагрузки и энергопотребле-ния
OLSR-ETX/ML/MD	Качество связи (ETX) / Задержка (MD)	Стандартный по метрике	Нет	Нет	Повышение качества обслуживания (QoS)
MOB-2-OLSR	Мобильность соседей	Приоритет менее мобильным	Нет	Нет	Снижение потерь пакетов в условиях мобильности
EDCR-OLSR	Комбинированная метрика (энергетический статус, задержка, стабильность)	Многокритериальная оптимизация, распределение нагрузки	Нет	Нет	Повышение энергоэффектив-ности
OLSR-AAD	Прогнозируемое время жизни узла (AAD)	Стандартный по метрике	Нет	Нет	Повышение доступности узлов
DCFM-OLSR	Стандартная	Активное продиводействие атакам	Нет	Да	Повышение безопасности
OPE-OLSR	Энергетический вес (остаточный заряд, стоимость передачи)	Фильтрация неэффективных узлов	Нет	Нет	Увеличение времени жизни сети

ти» (Average Age of Death, AAD). Данная метрика представляет прогнозное время, в течение которого узел сможет выполнять свою роль в качестве шлюза MPR.

Особенность указанного подхода заключается в том, что он позволяет оценить не мгновенное состояние узла, а прогнозируемое. Соответственно, в качестве шлюза MPR выбирается узел, позволяющий обеспечить наибольшее время жизни сетевых соединений.

Результаты моделирования показывают, что применение данного протокола вместо OLSR приводит к увеличению коэффициента доставки пакетов и уменьшению средней задержки.

DCFM-OLSR

Для проекта [16] авторы предложили активный механизм защиты от сетевых атак. Механизм DCFM основан на создании виртуальных узлов, которые имитируют поведение легитимных узлов. Указанные узлы используются для перенаправления или блокировки действий вредоносного узла, что позволяет обеспечить защиту реальных устройств.

Моделирование продемонстрировало, что данный подход позволяет эффективно противодействовать широкому спектру известных атак, что увеличивает безопасность сети.

OPE-OLSR

Разработанный протокол OPE-OLSR [17] направлен на увеличение срока функционирования сети, за счет выбора в качестве шлюзов MPR энергоэффективных узлов. В рамках данного подхода производится оценка остаточной энергии узла у одношаговых соседей. В случае, если несколько одношаговых соседей имеют одинаковый уровень остаточной энергии, то в качестве шлюза MPR выбирается узел с наибольшим количеством двухшаговых соседей. Результаты имитационного моделирования подтверждают достижение целей, заявленных авторами проекта.

Заключение

Сравнительный анализ различных модификаций протокола OLSR (таблица 1) позволил сформулировать следующие выводы:

1. Модификация стандартного эвристического алгоритма для задачи выбора шлюзов MPR, связанной с задачей о покрытии множества, в большинстве случаев действительно позволяет обеспечить более эффективный выбор шлюзов MPR и повысить показатели характеристик сетевого взаимодействия.

2. В настоящее время основные усилия исследователей сосредоточены на оптимизации энергопотребления и увеличении времени жизни сети за счет повышения энергоэффективности. В значительном количестве работ предложены новые метрики для процесса выбора шлюзов MPR, учитывающие остаточный уровень заряда, качество каналов связи и мобильность узлов. При этом, следует отметить, что, как правило, указанные характеристики являются взаимозависимыми, но оценка их взаимного влияния друг на друга не учитывается и не приводится.

3. Проблема безопасного выбора шлюзов MPR в рамках протокола маршрутизации OLSR в условиях наличия вредоносных узлов остаётся актуальной. Определяя и учитывая уровень репутации узлов в процессе выбора шлюзов MPR, можно снизить вероятность выбора вредоносных узлов в качестве шлюзов MPR и, тем самым, повысить безопасность сетевого взаимодействия. При этом, ключевые задачи заключаются в поиске подходящей репутационной модели и разработке эффективного алгоритма выбора шлюзов MPR с учетом репутации узлов (каналов связи).

Литература

1. RFC3626: Optimized Link State Routing Protocol (OLSR)/ T. Clausen, P. Jacquet, 2003. URL: https://tools.ietf.org/html/rfc3626 (дата обращения: 15.02.2026).

2. Еремеев А.В., Заозерская Л.А., Колоколов А.А. Задача о покрытии множества: сложность, алгоритмы, экспериментальные исследования / А.В. Еремеев, Л.А. Заозерская, А.А. Колоколов // Дискретный анализ и исследование операций, сер. 2, 2000. Т. 7, № 2. С. 22–46.

3. Сергин Д.А., Васильев А.А. Моделирование атаки на множество шлюзов пересылки в рамках протокола маршрутизации OLSR // ПЕРСПЕКТИВА-2024: Сборник трудов одиннадцатой всероссийской молодежной школы-семинара по проблемам информационной безопасности. Таганрог, ЮФУ, 2024. С. 140–146.

4. Moad D., Djahel S., Nait-Abdesselam F. Improving the quality of service routing in OLSR protocol // 2012 International Conference on Communications and Information Technology (ICCIT). – IEEE, 2012. – С. 314–319.

5. Malik D., Mahajan K., Rizvi M. A. Security for node isolation attack on OLSR by modifying MPR selection process // 2014 First International Conference on Networks & Soft Computing (ICNSC2014). – IEEE, 2014. – С. 102–106.

6. Wang X. et al. Trust routing protocol based on cloud-based fuzzy petri net and trust entropy for mobile ad hoc network // IEEE Access. – 2020. – Т. 8. – С. 47675–47693.

7. Dyabi M., Hajami A., Allali H. PB-OLSR: Performance Based OLSR // IJCSNS International Journal of Computer Science and Network Security. – 2015. – Т. 15.

8. Fatima L., Najib E. Energy and mobility in OLSR routing protocol // Journal of Selected Areas in Telecommunications (JSAT). – 2012. – Т. 2012. – №. 3. – С. 1–6.

9. Anandrao L. S., Amey J. Y. Comparison of OLSR and Energy Conserved OLSR // International Journal of Technical Research and Applications. – 2014. – Т. 2. – №. 4.

10. Mohit M., Pal S. Stable MPR selection in OLSR for mobile ad-hoc networks // Int. J. Comp. Sci. Inf. Technol. – 2015. – Т. 6. – №. 6. – С. 5121–5125.

11. Jaiswal A. K., Tiwari S. Modified OLSR (MOLSR) Protocol for improving optimal route selection with Dynamic MPR selection in Mobile Adhoc Network // International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET). – 2015. – Т. 1. – №. 6. – С. 535–541.

12. Pandey A., Baliyan M. Performance Analysis of OLSR and Modified Version of OLSR-ETX/MD/ML in Mesh Networks // International Journal of Computer Science & Communication Networks. – 2012. – Т. 2. – №. 2. – С. 268–271.

13. Ouacha A. et al. OLSR protocol enhancement through mobility integration // 2013 10th IEEE International Conference on Networking, Sensing And Control (ICNSC). – IEEE, 2013. – С. 17–22.

14. Ouacha A. et al. Proactive routing based distributed energy consumption // 2013 8th International Conference on Intelligent Systems: Theories and Applications (SITA). – IEEE, 2013. – С. 1–5.

15. Ouacha A. et al. New Mobility Metric based on MultiPoint Relay Life Duration // SIGMAP. – 2012. – С. 305–309.

16. Rani V. I. U., Reddy K. T. To Improve the Security of OLSR Routing Protocol Based on Local Detection of Link Spoofing // International Journal of Science Engineering Technology, IJSEAT. – 2017. – Т. 5.

17. Prajapati S., Patel N., Patel R. Optimizing performance of OLSR protocol using energy based MPR selection in MANET // 2015 Fifth International Conference on Communication Systems and Network Technologies. – IEEE, 2015. – С. 268–272.

References

1. RFC3626: Optimized Link State Routing Protocol (OLSR)/ T. Clausen, P. Jacquet, 2003. URL: https://tools.ietf.org/html/rfc3626

2. Eremeev A.V., Zaozerskaya L.A., Kolokolov A.A. Zadacha o pokrytii mnozhestva: slozhnost', algoritmy, eksperimental'nye issledovaniya / A.V. Eremeev, L.A. Zaozerskaya, A.A. Kolokolov // Diskretnyy analiz i issledovanie operatsiy, ser. 2, 2000. T. 7, № 2. S. 22–46.

3. Sergin D.A., Vasil'ev A.A. Modelirovanie ataki na mnozhestvo shlyuzov peresylki v ramkakh protokola marshrutizatsii OLSR // PERSPEKTIVA-2024: Sbornik trudov odinnadtsatoy vserossiyskoy molodezhnoy shkoly-seminara po problemam informatsionnoy bezopasnosti. Taganrog, YuFU, 2024. S. 140–146.

4. Moad D., Djahel S., Nait-Abdesselam F. Improving the quality of service routing in OLSR protocol // 2012 International Conference on Communications and Information Technology (ICCIT). – IEEE, 2012. – S. 314–319.

5. Malik D., Mahajan K., Rizvi M. A. Security for node isolation attack on OLSR by modifying MPR selection process // 2014 First International Conference on Networks & Soft Computing (ICNSC2014). – IEEE, 2014. – S. 102–106.

6. Wang X. et al. Trust routing protocol based on cloud-based fuzzy petri net and trust entropy for mobile ad hoc network // IEEE Access. – 2020. – T. 8. – S. 47675–47693.

7. Dyabi M., Hajami A., Allali H. PB-OLSR: Performance Based OLSR // IJCSNS International Journal of Computer Science and Network Security. – 2015. – T. 15.

8. Fatima L., Najib E. Energy and mobility in OLSR routing protocol // Journal of Selected Areas in Telecommunications (JSAT). – 2012. – T. 2012. – №. 3. – S. 1–6.

9. Anandrao L. S., Amey J. Y. Comparison of OLSR and Energy Conserved OLSR // International Journal of Technical Research and Applications. – 2014. – T. 2. – №. 4.

10. Mohit M., Pal S. Stable MPR selection in OLSR for mobile ad-hoc networks // Int. J. Comp. Sci. Inf. Technol. – 2015. – T. 6. – №. 6. – S. 5121–5125.

11. Jaiswal A. K., Tiwari S. Modified OLSR (MOLSR) Protocol for improving optimal route selection with Dynamic MPR selection in Mobile Adhoc Network // International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET). – 2015. – T. 1. – №. 6. – S. 535–541.

12. Pandey A., Baliyan M. Performance Analysis of OLSR and Modified Version of OLSR-ETX/MD/ML in Mesh Networks //International Journal of Computer Science & Communication Networks. – 2012. – T. 2. – №. 2. – S. 268–271.

13. Ouacha A. et al. OLSR protocol enhancement through mobility integration // 2013 10th IEEE International Conference on Networking, Sensing And Control (ICNSC). – IEEE, 2013. – S. 17–22.

14. Ouacha A. et al. Proactive routing based distributed energy consumption // 2013 8th International Conference on Intelligent Systems: Theories and Applications (SITA). – IEEE, 2013. – S. 1–5.

15. Ouacha A. et al. New Mobility Metric based on MultiPoint Relay Life Duration // SIGMAP. – 2012. – S. 305–309.

16. Rani V. I. U., Reddy K. T. To Improve the Security of OLSR Routing Protocol Based on Local Detection of Link Spoofing // International Journal of Science Engineering Technology, IJSEAT. – 2017. – T. 5.

17. Prajapati S., Patel N., Patel R. Optimizing performance of OLSR protocol using energy based MPR selection in MANET // 2015 Fifth International Conference on Communication Systems and Network Technologies. – IEEE, 2015. – S. 268–272.

СЕРГИН Даниил Альбертович, аспирант федерального государственного автономного образовательного учреждения высшего образования «Омский государственный технический университет». 644050, г. Омск, пр. Мира, 11. E-mail: daniil0808_98@mail.ru

ЩЕРБА Евгений Викторович, кандидат технических наук, доцент, доцент кафедры «Комплексная защита информации» федерального государственного автономного образовательного учреждения высшего образования «Омский государственный технический университет». 644050, г. Омск, пр. Мира, 11. E-mail: evscherba@gmail.com

SERGIN Daniil Albertovich, post-graduate student of the Federal State Autonomous Educational Institution of Higher Education "Omsk State Technical University". 644050, Omsk, pr. Mira, 11. E-mail: daniil0808_98@mail.ru

SHCHERBA Evgeny Victorovich, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Complex Information Protection, at the Federal State Autonomous Educational Institution of Higher Education "Omsk State Technical University". 644050, Omsk, pr. Mira, 11. E-mail: evscherba@gmail.com