DOI: 10.55648/1998-6920-2025-19-1-20-27 УДК 004.056:004.057.4

Повышение доступности узлов сети на базе протокола маршрутизации OLSR

Д. А. Сергин[1,2], М. В. Щерба[1], Е. В. Щерба[1]

[1]Омский государственный технический университет (ОмГТУ)
[2]АО «ОНИИП»

Аннотация: В статье предложена и исследована модификация алгоритма выбора шлюзов многоточечной рассылки (MPR) в рамках протокола маршрутизации OLSR, направленная на обеспечение защищенности от атак изоляции и повышение доступности узлов сети. Указанный алгоритм был реализован на базе сетевого симулятора NS-3. Была предложена модель нарушителя, выполнено имитационное моделирование атаки на доступность узлов самоорганизующейся сети и проведено экспериментальное исследование разработанного алгоритма. Полученные результаты позволили подтвердить эффективность разработанного решения.

Ключевые слова: безопасность маршрутизации, сетевые атаки, доступность узлов, протокол OLSR, выбор MPR.

Для цитирования: Сергин Д. А., Щерба М. В., Щерба Е. В. Повышение доступности узлов сети на базе протокола маршрутизации OLSR // Вестник СибГУТИ. 2025. Т. 19, № 1. С. 20–27. https://doi.org/10.55648/1998-6920-2025-19-1-20-27.

Статья поступила в редакцию 14.04.2024;
принята к публикации 10.06.2024.

1. Введение

Динамически организуемые сети устройств «Интернета вещей» могут включать множество узлов, которые в процессе перемещения способны самостоятельно устанавливать новые связи с соседними узлами и терять ранее имевшиеся. При этом каждый узел сети помимо роли оконечного устройства выполняет роль маршрутизатора, т.е. принимает сетевые пакеты, адресованные другим устройствам, и осуществляет дальнейшую пересылку пакетов в соответствии с выбранным направлением. Для организации многошаговых соединений узлы используют протоколы адаптивной маршрутизации, что также позволяет обеспечивать устойчивость к изменениям топологии сети.

Проактивный протокол маршрутизации OLSR (Optimized Link State Routing) является одним из наиболее широко используемых протоколов маршрутизации для динамически организуемых сетей различных типов. Важнейшая особенность протокола OLSR заключается в использовании концепции шлюзов многоточечной рассылки MPR (MultiPoint Relay) [1]. Использование MPR-шлюзов существенно сокращает объем рассылаемой информации по сравнению с традиционным процессом рассылки, в котором каждый узел осуществляет рассылку принимаемых сообщений всем своим соседям [2].

В рамках OLSR информация об активных сетевых соединениях узла генерируется и распространяется только MPR-шлюзами. Каждый узел сети N выбирает из числа своих одношаговых соседей (т.е. из узлов, с которыми у него установлено прямое соединение) несколько узлов, которым разрешается ретранслировать широковещательный трафик от

узла *N*. Это множество узлов именуется MPR-набором узла *N*. Остальным соседям узла *N* запрещается ретранслировать широковещательный трафик, генерируемый *N*. В итоге в сети формируется множество MPR-шлюзов. Чем меньше будет суммарное число MPR-шлюзов среди всех узлов сети, тем меньше будет объём широковещательного трафика в сети.

Множество MPR(*N*) для некоторого узла *N* формируется так, чтобы для каждого двухшагового соседа узла *N* существовал узел из множества MPR(*N*), обеспечивающий связь с этим соседом (рис. 1).

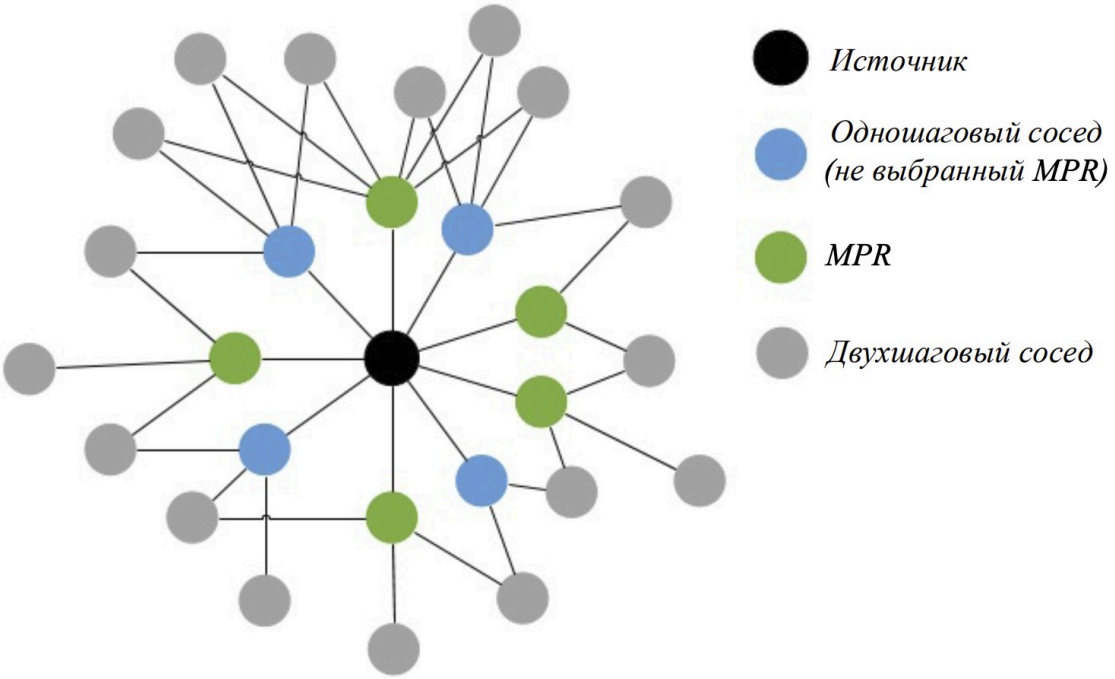

Рис. 1. Пример определения набора MPR-шлюзов

Множественный доступ к среде передачи данных, неустойчивая топология и особенности маршрутизации пакетов повышают сложность обеспечения их безопасной доставки в динамически организуемых сетях. Вредоносные узлы могут целенаправленно препятствовать сетевому взаимодействию посредством различных сетевых атак. В результате одной из наиболее актуальных проблем остается проблема обеспечения безопасности маршрутизации сетевых пакетов. Криптографические методы защиты позволяют обеспечить конфиденциальность и целостность пересылаемых сетевых пакетов, но при этом сохраняется угроза нарушения доступности информации в результате сетевых атак зараженных узлов, препятствующих передаче данных. В частности, можно предположить, что скомпрометированный вредоносный MPR-шлюз в рамках протокола OLSR способен частично или полностью изолировать некоторые узлы сети. Таким образом, проблема нарушения доступности узлов сети при использовании протокола маршрутизации OLSR требует специального исследования.

2. Анализ применяемого алгоритма выбора шлюзов

Итак, каждый узел *N* в сети определяет свой набор шлюзов MPR(*N*) из его симметричного одношагового окружения. Выбор осуществляется таким образом, чтобы суммарное радиочастотное покрытие входящих в MPR(*N*) узлов охватывало все симметричное двухшаговое окружение узла *N* (соседи соседей узла). Полученный набор MPR(*N*) должен удовлетворять следующему требованию: каждый узел в строгом симметричном двушаговом окружении узла *N* должен иметь симметричный канал с MPR(*N*).

Пересчет текущего набора шлюзов MPR(N) выполняется каждый раз при изменении симметричного одношагового и двухшагового окружения.

Информация об активных сетевых соединениях узлов распространяется по сети посредством служебных сообщений HELLO и TC (Topology Control). В пересылке сообщений TC участвуют только шлюзы MPR, остальные узлы принимают и обрабатывают, но не ретранслируют указанные сообщения. Для каждого узла, выбранного в качестве шлюза MPR, формируется список соседних узлов, выбравших его в качестве MPR (список селекторов MPR). Каждый шлюз MPR в своих сообщениях TC должен объявлять маршруты до его селекторов.

Согласно RFC7181, определение множества шлюзов MPR некоторым узлом сети в рамках протокола OLSR происходит по алгоритму, позволяющему минимизировать число одношаговых соседей, входящих в искомое множество. Пусть N_1 – подмножество соседей рассматриваемого узла, которые являются соседями его интерфейса I, а N_2 – множество узлов в пределах 2 переходов, достижимых с интерфейса I, за исключением узлов, достижимых только узлами из N_1 с готовностью WILL_NEVER, узла, выполняющего вычисления, и всех симметричных соседей (узлы, для которых на каком-либо интерфейсе существует симметричная связь с данным узлом). Значение $D(y)$ определяется как степень одношагового соседнего узла y из N_1 (число симметричных соседей узла y, за исключением узлов из N_1 и узла, выполняющего вычисления).

1) В набор MPR добавляются все узлы подмножества N_1 с готовностью WILL_ALWAYS.

2) Рассчитывается значение $D(y)$ для всех узлов в N_1.

3) В набор MPR добавляются те узлы подмножества N_1, которые обеспечивают достижимость узла в N_2 единственным образом. Например, если узел B в подмножестве N_2 доступен только через симметричное соединение к узлу A из N_1, то узел A добавляется в набор MPR. Затем, из N_2 удаляются все узлы, достижимые через узлы из набора MPR.

4) Пока множество N_2 непустое:

– Для каждого узла из N_1 рассчитывается значение достижимости – количество узлов в N_2, достижимых через рассматриваемый соседний узел.

– В набор MPR добавляется узел с наибольшим значением параметра готовности среди узлов из N_1 с ненулевым значением достижимости. При наличии нескольких кандидатов выбирается узел с максимальным значением достижимости. В случае, если таких узлов несколько, выбирается узел с наибольшим значением $D(y)$. Затем из N_2 удаляются все узлы, достижимые через узлы из набора MPR.

5) Окончательный набор MPR формируется в результате объединения наборов MPR для каждого интерфейса. Затем обработка узлов в окончательном наборе MPR производится в порядке возрастания параметра готовности. Рассматриваемый узел y удаляется из окончательного набора MPR, если при его удалении все узлы в N_2 остаются достижимыми, а параметр готовности узла y не имеет значение WILL_ALWAYS.

Несмотря на то, что указанный алгоритм позволяет оптимизировать набор шлюзов MPR, ретранслирующих сетевые пакеты, он также может являться источником уязвимости, используемой для реализации сетевой атаки, направленной на изоляцию некоторого узла [3-5]. Допустим, что для некоторого рассматриваемого узла N только соседние узлы A и B могут обеспечить достижимость узла C из множества двушаговых соседей. В соответствии с предложенным алгоритмом, один из этих двух узлов, например узел A, будет включен в набор MPR узла N. Если при этом узел A является вредоносным, он получает возможность успешно реализовать сетевую атаку, направленную на изоляцию узла N для узла C. Для этого узел A исключает из рассылаемых сообщений HELLO и TC любую информацию о соединениях с узлом N. Поскольку узел C не имеет других возможностей получить маршрут до узла N, в результате реализации сетевой атаки узлом A узел N становится недостижимым для узла C.

3. Альтернативный подход к выбору шлюзов для повышения доступности

В настоящее время исследуется ряд подходов к модификации алгоритма выбора шлюзов MPR в рамках протокола маршрутизации OLSR, направленных на повышение эффективности и безопасности сетевого взаимодействия [6-8]. Основной недостаток указанных подходов заключается в сложности их практической реализации. Кроме того, в ряде случае нарушается обратная совместимость с базовой версией протокола OLSR.

В рамках данной работы, для противодействия атаке изоляции, выполняемой вредоносными узлами сети, авторами предложена простая модификация алгоритма выбора множества шлюзов MPR. В целях повышения доступности легитимных узлов сети предлагается выбирать и использовать дополнительные резервные шлюзы MPR. Для реализации указанного подхода были внесены изменения в четвертый шаг стандартного алгоритма выбора шлюзов MPR. В рамках исходного алгоритма в завершении каждой итерации данного шага из N_2 удаляются все узлы, достижимые через узлы из текущего набора MPR.

В результате модификации алгоритма в завершении каждой итерации четвертого шага из N_2 удаляются только те узлы, которые достижимы не менее чем через два узла из текущего набора MPR. Таким образом, если некоторый узел из двухшагового окружения достижим не менее чем через двух соседей из N_1, то в набор MPR будут добавлены как минимум два узла, обеспечивающих достижимость рассматриваемого узла из N_2. Тем самым обеспечивается избыточность на случай, если один из соседних узлов выйдет из строя, либо окажется вредоносным узлом, выполняющим атаку изоляции.

В частности, в сети на рис. 2 при использовании стандартного алгоритма выбора шлюзов MPR для достижения всех своих двухшаговых соседей узел 0 будет выбирать в качестве шлюза MPR узел 1.

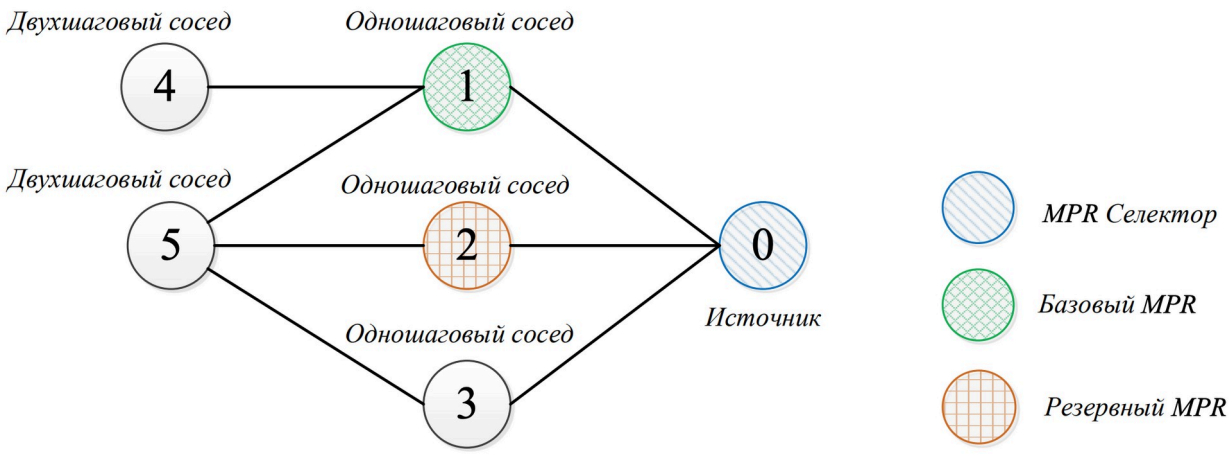

Рис. 2. Пример определения набора MPR-шлюзов

В то же время при использовании модифицированного алгоритма выбора шлюзов MPR, для достижения своих двухшаговых соседей узел 0 будет выбирать в качестве шлюзов MPR два узла из своих одношаговых соседей, например узел 1 и узел 2. Таким образом, при проведении узлом 1 атаки, направленной на изоляцию узла 0, модифицированный алгоритм позволит обеспечить достижимость узла 0 для узла 5 через резервный маршрут в обход узла нарушителя.

4. Описание эксперимента и анализ результатов

В рамках экспериментальных исследований было выполнено имитационное моделирование атаки, направленной на изоляцию узла, при использовании оригинального и модифицированного алгоритма выбора шлюзов MPR в рамках протокола маршрутизации OLSR при помощи сетевого симулятора. Одним из наиболее широко используемых сетевых симуляторов с открытым исходным кодом является ns-3. Открытый исходный код симулятора позволяет вносить изменения в алгоритмы работы сетевых протоколов [9].

Для реализации эксперимента в сетевом симуляторе было выполнено построение сетевой топологии, состоящей из 6 узлов (рис. 3). Все узлы использовали протокол маршрутизации OLSR. В ходе эксперимента производились наблюдения изменений в таблицах маршрутизации узлов сети для определения сетевой связности.

Для моделирования сетевой атаки, направленной на изоляцию узлов, предложенная ранее модель нарушителя была реализована на базе протокола OLSR в рамках симулятора ns-3. В рамках рассматриваемой топологии узел 1 выступал в качестве вредоносного узла, реализующего сетевую атаку, направленную на изоляцию узла 0. Для этого узел 1 модифицировал сообщения HELLO и TC протокола OLSR, чтобы исключить из объявляемых каналов связи IP-адреса интерфейсов узла 1.

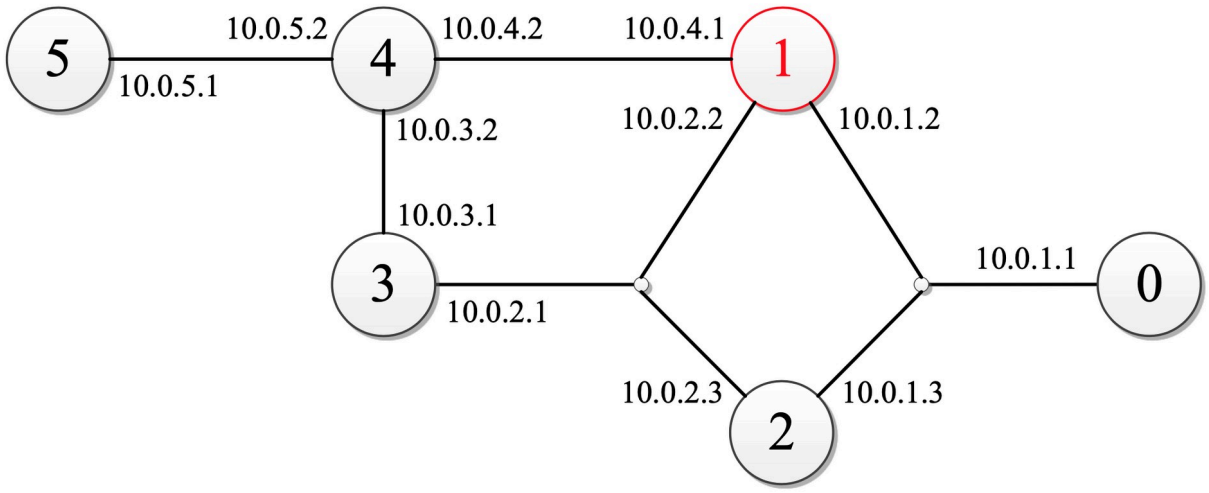

Рис. 3. Топология моделируемой сети.

При использовании на всех узлах сети стандартного алгоритма выбора шлюзов MPR рамках протокола OLSR, после выбора шлюзов MPR и заполнения таблиц маршрутизации каждым узлом, узел 1, выбранный в качестве шлюза MPR, начинает отправлять соседним узлам нелегитимные сообщения TC, которые не содержат объявление канала связи до узла 0.

Вследствие отправки поддельных сообщений TC, узел 5 не имеет в своей таблице маршрутизации маршрута до узла 0 и не может взаимодействовать с данным узлом в течение всего сеанса моделирования. При отправке потока данных по протоколу UDP от узла 5 до узла 0 пакеты не доставляются до узла назначения. Полученный результат позволил подтвердить адекватность предложенной и реализованной модели узла нарушителя.

При использовании на всех узлах сети модифицированного алгоритма выбора шлюзов MPR рамках протокола OLSR, узел 0 выбирает два шлюза MPR – узел 1 и узел 2, который также объявляет канал связи к узлу 0. Таким образом, в рамках данного эксперимента именно узел 2 обеспечивает достижимость узла 0 для других узлов сети. В результате узел 5 содержит маршрут до узла 0 в своей таблице маршрутизации (табл. 1), а поток данных UDP от узла 5 до узла 0 доставляется без потерь пакетов.

Таблица 1. Таблица маршрутизации узла 5 в результате моделирования

Адрес назначения	Адрес следующего перехода	Дистанция
10.0.1.1	10.1.5.2	4
10.0.1.3	10.1.5.2	3
10.0.1.2	10.1.5.2	2
10.0.2.1	10.1.5.2	2
10.0.2.2	10.1.5.2	2
10.0.2.3	10.1.5.2	2
10.0.3.1	10.1.5.2	2
10.0.4.1	10.1.5.2	2
10.0.3.2	10.1.5.2	1
10.0.4.2	10.1.5.2	1
10.1.5.2	10.1.5.2	1

5. Заключение

Таким образом, результат экспериментального исследования позволил подтвердить эффективность предложенного решения. Модифицированный алгоритм выбора шлюзов MPR в рамках протокола маршрутизации OLSR позволяет противодействовать атакам, направленным на изоляцию узлов, выполняемых единственным узлом-нарушителем, и повышает доступность узлов самоорганизующейся сети за счёт выбора дополнительных резервных шлюзов MPR, которые позволяют обеспечить сетевую связность в случае отказа основного шлюза MPR. Преимуществом указанного подхода является простота его практической реализации и обратная совместимость с базовой версией протокола OLSR.

Следует отметить, что применение указанного алгоритма выбора шлюзов MPR также может приводить к увеличению количества сетевых пакетов, ретранслируемых по сети, и сопутствующих накладных расходов на их обработку. В то же время, оценка влияния данных факторов на снижение эффективности сетевого взаимодействия представляет собой отдельную задачу, которая может быть решена в ходе дальнейших исследований.

Литература

1. 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: 10.04.2024).
2. *Clausen T., Hansen G., Christensen L., Behrmann G.* The Optimized Link State Routing Protocol Evaluation through Experiments and Simulation // IEEE Symposium on wireless personal mobile communications. Aalborg, Denmark, September 9, 2001. P. 56-62.
3. *Clausen T., Herberg U., Yi J.* Security Threats to the Optimized Link State Routing Protocol Version 2 (OLSRv2). 2017. RFC 8116. URL: https://tools.ietf.org/html/rfc8116 (дата обращения: 10.04.2024).
4. *Щерба Е. В., Никонов В. И., Литвинов Г. А.* Обеспечение безопасности протоколов маршрутизации для телекоммуникационных сетей с динамической топологией // Доклады Томского государственного университета систем управления и радиоэлектроники. 2018. Т. 21. № 3. С. 19–29.
5. *Litvinov G. A., Shcherba E. V.* Modeling Message Spoofing Attacks on the OLSR Routing Protocol // 2019 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). Yekaterinburg, 2019. P. 299-302.
6. *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). Guntur, India, 2014. P. 102-106.

7. *Nabou A., Laanaoui M.D., Ouzzif M.* New MPR Computation for Securing OLSR Routing Protocol Against Single Black Hole Attack // Wireless Personal Communications. 2021. Vol. 117. P. 525-544.
8. *Idboufker N., Mssassi S., Alaoui C. M., Zougagh H.* Election of MPR Nodes and Detection of Malicious Nodes Based on a Byzantine Fault in the OLSR Protocol Case of a Scale-Free Network // Electronics. 2023. Vol. 12. № 16. 3390.
9. *Riley G. F., Henderson T. R.* The ns-3 network simulator // Modeling and tools for network simulation. 2010. P. 15-34.

Сергин Даниил Альбертович
аспирант кафедры «Комплексная защита информации», Омский государственный технический университет (ОмГТУ, 644050, Омск, пр-т Мира, 11), сотрудник АО «ОНИИП» (644009, Омск, улица Масленникова, 231) тел. +7 913 962 5129, e-mail: daniil0808_98@mail.ru, ORCID ID: 0009-0006-6609-2093.

Щерба Мария Витальевна
к.т.н., доцент кафедры «Комплексная защита информации», Омский государственный технический университет (ОмГТУ, 644050, Омск, пр-т Мира, д. 11), тел. +7 904 582 6519, e-mail: mariz3@mail.ru, ORCID ID: 0000-0002-1994-5093.

Щерба Евгений Викторович
к.т.н., доцент кафедры «Комплексная защита информации», Омский государственный технический университет (ОмГТУ, 644050, Омск, пр-т Мира, д. 11), тел. +7 904 322 2689, e-mail: evscherba@gmail.com, ORCID ID: 0000-0003-4401-4343.

Авторы прочитали и одобрили окончательный вариант рукописи.
Авторы заявляют об отсутствии конфликта интересов.
Вклад соавторов: *Каждый автор внес равную долю участия как во все этапы проводимого теоретического исследования, так и при написании разделов данной статьи.*

Improving the Accessibility of Network Nodes Based on the OLSR Routing Protocol

Daniil A. Sergin[1,2], Maria V. Shcherba[1], Evgeniy V. Shcherba[1]

[1] Omsk State Technical University (OmSTU)
[2] Omsk Scientific Research Institute of Instrument Engineering

Abstract: The article proposes and investigates a modification of the algorithm for selecting multipoint relays (MPR) within the OLSR routing protocol, aimed at ensuring protection from isolation attacks and increasing the accessibility of network nodes. Algorithm was implemented on the basis of the NS-3 network simulator. An intruder model was proposed, an attack simulation on the availability of nodes of a self-organizing network was performed, and an experimental investigation of the developed algorithm was carried out. The results obtained allowed us to confirm the effectiveness of the developed solution.

Keywords: routing security, network attacks, node availability, OLSR protocol, MPR selection.

For citation: Sergin D. A., Shcherba M. V., Shcherba E. V. Povyshenie dostupnosti uzlov seti na baze protokola marshrutizacii OLSR [Improving the Accessibility of Network Nodes Based on the OLSR Routing Protocol]. *Vestnik SibGUTI*, 2025, vol. 19, no. 1, pp. 20–27. https://doi.org/10.55648/1998-6920-2025-19-1-20-27.

The article was submitted: 14.04.2024;
accepted for publication 10.06.2024.

References

1. *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: 10.04.2024).
2. *Clausen T., Hansen G., Christensen L., Behrmann G.* The Optimized Link State Routing Protocol Evaluation through Experiments and Simulation. IEEE Symposium on wireless personal mobile communications. Aalborg, Denmark, September 9, 2001. P. 56-62.
3. *Clausen T., Herberg U., Yi J.* Security Threats to the Optimized Link State Routing Protocol Version 2 (OLSRv2). 2017. RFC 8116. available at: https://tools.ietf.org/html/rfc8116 (accessed: 10.04.2024: 10.04.2024).
4. *Shcherba E. V., Nikonov V. I., Litvinov G. A.* Obespechenie bezopasnosti protokolov marshrutizacii dlya telekommunikacionnyh setej s dinamicheskoj topologiej [Ensuring the security of routing protocols for telecommunication networks with dynamic topology]. Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki. 2018. vol. 21. no 3. pp. 19–29.
5. *Litvinov G. A., Shcherba E. V.* Modeling Message Spoofing Attacks on the OLSR Routing Protocol. 2019 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). Yekaterinburg, 2019. pp. 299-302.
6. *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). Guntur, India, 2014. pp. 102-106.
7. *Nabou A., Laanaoui M. D., Ouzzif M.* New MPR Computation for Securing OLSR Routing Protocol Against Single Black Hole Attack. Wireless Personal Communications. 2021. Vol. 117. pp. 525-544.
8. *Idboufker N., Mssassi S., Alaoui C. M., Zougagh H.* Election of MPR Nodes and Detection of Malicious Nodes Based on a Byzantine Fault in the OLSR Protocol Case of a Scale-Free Network. Electronics. 2023. Vol. 12. no 16. 3390.
9. *Riley G. F., Henderson T. R.* The ns-3 network simulator. Modeling and tools for network simulation. 2010. pp. 15-34.

Daniil A. Sergin

Ph.D. Student of the Department of Communications and Information Security at Omsk State Technical University (OmSTU, Russia, 644050, Omsk, Mira ave. 11), phone: +7 913 962 5129, e-mail: daniil0808_98@mail.ru, ORCID ID: 0009-0006-6609-2093.

Maria V. Shcherba

Cand.Sc. (Engineering), Assoc. Prof of the Department of Communications and Information Security at Omsk State Technical University (OmSTU, Russia, 644050, Omsk, Mira ave. 11), phone: +7 904 582 6519, e-mail: mariz3@mail.ru, ORCID ID: 0000-0002-1994-5093.

Evgeniy V. Shcherba

Cand.Sc. (Engineering), Assoc. Prof of the Department of Communications and Information Security at Omsk State Technical University (OmSTU, Russia, 644050, Omsk, Mira ave. 11), phone: +7 904 322 2689, e-mail: evscherba@gmail.com, ORCID ID: 0000-0003-4401-4343.