Авторлар туралы ақпарат

Жанель Ермашқызы Байғараева – магистр, Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы; e-mail: zhanel.baigarayeva@gmail.com. ORCID: https://orcid.org/0000-0003-1919-3570.

Асия Кубланди кызи Болтабоева* – магистр, PhD 3 курс студенті, Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы; e-mail: boltaboyeva_assiya3@live.kaznu.kz. ORCID: https://orcid.org/0000-0002-7279-9910.

Бағлан Талғатқызы Иманбек – PhD, доцент, профессор-зерттеуші, Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы; e-mail: baglan.imanbek@kaznu.edu.kz. ORCID: https://orcid.org/0000-0001-7249-380X.

Мергул Иманбековна Кожамбердиева – педагогика ғылымдарының кандидаты, Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы; e-mail: kozhamberdiyeva.m@outlook.com.

Айман Болатовна Бектурганова – бакалавр 4 курс студенті, Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы; e-mail: aiman0908b@gmail.com.

Информация об авторах

Жанель Ермашқызы Байғараева – магистр, Казахский национальный университет имени аль-Фараби, Алматы; e-mail: zhanel.baigarayeva@gmail.com. ORCID: https://orcid.org/0000-0003-1919-3570.

Асия Кубланди кызи Болтабоева* – магистр, PhD студентка 3 курса, Казахский национальный университет имени аль-Фараби, Алматы; e-mail: boltaboyeva_assiya3@live.kaznu.kz. ORCID: https://orcid.org/0000-0002-7279-9910.

Бағлан Талғатқызы Иманбек – PhD, доцент, профессор-исследователь, Казахский национальный университет имени аль-Фараби, Алматы; e-mail: baglan.imanbek@kaznu.edu.kz. ORCID: https://orcid.org/0000-0001-7249-380X.

Мергул Иманбековна Кожамбердиева – кандидат педогогических наук, Казахский национальный университет имени аль-Фараби, Алматы; e-mail: kozhamberdiyeva.m@outlook.com.

Айман Болатовна Бектурганова – бакалавр студентка 4 курса, Казахский национальный университет имени аль-Фараби, Алматы; e-mail: aiman0908b@gmail.com.

Information about the authors

Zhanel Yermashkyzy Baigarayeva – Master's degree holder, Al Farabi Kazakh National University, Almaty; e-mail: zhanel.baigarayeva@gmail.com. ORCID: https://orcid.org/0000-0003-1919-3570.

Assiya Kublandi kyzi Boltaboyeva* – Master's degree holder, 3rd-year PhD student, Al Farabi Kazakh National University, Almaty; e-mail: boltaboyeva_assiya3@live.kaznu.kz. ORCID: https://orcid.org/0000-0002-7279-9910.

Baglan Talgatkyzy Imanbek – PhD, Associate Professor, Research Professor, Al Farabi Kazakh National University, Almaty; e-mail: baglan.imanbek@kaznu.edu.kz. ORCID: https://orcid.org/0000-0001-7249-380X.

Mergul Imanbekovna Kozhamberdiyeva – Candidate of Pedagogical Sciences, Al Farabi Kazakh National University, Almaty; e-mail: kozhamberdiyeva.m@outlook.com.

Aiman Bolatovna Bekturganova – 4th year Bachelor's student, Al Farabi Kazakh National University, Almaty; e-mail: aiman0908b@gmail.com.

Редакцияға енуі 18.09.2025
Өңдеуден кейін түсуі 17.11.2025
Жариялауға қабылданды 18.11.2025

https://doi.org/10.53360/2788-7995-2025-4(20)-28

МРНТИ: 50.41.23; 81.93.29

Б.А. Шырын[1]*, Т.А. Ahanger[2], А.К. Жумадиллаева[1], Г.Б. Бекешова[1]
[1]Евразийский национальный университет им. Л.Н. Гумилева,
010000 Республика Казахстан, г. Астана, ул. Сатпаева, 2
[2]Университет принца Sattam Bin Abdulaziz,
Королевство Саудовская Аравия, г. Эль-Хардж,
*e-mail: bexultan.shyryn@gmail.com

МНОГОЦЕЛЕВАЯ ЭВОЛЮЦИОННАЯ ОПТИМИЗАЦИЯ ПОЛИТИК БЕЗОПАСНОСТИ В ПРОГРАММНО-ОПРЕДЕЛЯЕМЫХ СЕТЯХ (SDN) С УЧЕТОМ ОГРАНИЧЕНИЙ TCAM И ЗАДЕРЖКИ

Аннотация: *Статья посвящена рассмотрению задачи оптимизации политик безопасности в программно-определяемых сетях (SDN). Решение этой проблемы авторы предлагают осуществлять с помощью NSGA-II – эффективного алгоритма эволюционной*

оптимизации множественных целей. Изложенный подход ориентирован на достижение баланса между необходимостью жестко обеспечивать сетевую безопасность и наличием ограниченных вычислительных ресурсов. Особое внимание уделяется таким факторам, как задержки передачи данных и размер таблиц TCAM, которые оказывают существенное влияние на эффективность фильтрации трафика. На основе построенной в статье модели, включающей оценки вероятностей угроз, методики нормализации целевых функций и использования штрафных коэффициентов за конфликты правил, оптимизацию проведены по трем ключевым параметрам: риску атак, задержкам в сети и загрузке TCAM. Проведенное моделирование охватило три сценария работы сети – нормальный, смешанный и атакующий – с применением пакетов Mininet и Ryu. Взаимосравнение предложенного метода с дифференциальной эволюцией (DE) и жадным алгоритмом (Greedy) показало, что NSGA-II достигает оптимального распределения решений по фронту Парето, быстрее сходится и при этом не теряет в точности фильтрации. В статье кроме того представлена визуализация смены поколений, компромиссные графики и профили нагрузки. В заключении рассматриваются перспективы интеграции предложенной модели с контроллерами ONOS и OpenDaylight; кроме того обсуждаются возможность использования гибридных решений на основе Deep Reinforcement Learning, Federated Learning и Explainable AI.

Ключевые слова: *программно-определяемые сети (SDN), многокритериальная оптимизация, эволюционные алгоритмы, NSGA-II, безопасность сети, обнаружение аномалий.*

Введение

Программно-определяемая сеть (SDN) радикально изменила традиционный подход к управлению сетевой инфраструктурой и безопасностью, обеспечив централизованное управление потоками данных и динамическое распределение политик безопасности. Однако появление единого центра принятия решений в виде SDN-контроллера создало новые угрозы и уязвимости, так как нарушение его работы может привести к компрометации всей сети [5]. Дополнительной проблемой являются избыточные и конфликтующие правила фильтрации, которые перегружают таблицы TCAM, увеличивают задержки и снижают пропускную способность сети [1-2]. В этих условиях ключевой задачей становится формирование сбалансированных политик безопасности, которые обеспечивают высокий уровень защиты при сохранении производительности и эффективности использования ресурсов.

Современные подходы к решению данной проблемы всё чаще основаны на методах многокритериальной оптимизации, позволяющих находить компромиссы между противоречивыми целями. Эволюционные алгоритмы, такие как NSGA-II, демонстрируют высокую эффективность при оптимизации политик безопасности в условиях неопределенности и динамических изменений сетевого трафика. Их применение в контексте SDN открывает возможности для интеллектуального, адаптивного управления, где безопасность, задержка и ресурсная нагрузка рассматриваются как взаимосвязанные критерии, требующие согласованной оптимизации.

Обзор литературы

Проблема обеспечения безопасности в SDN – это тема, которая обсуждается широко. В статье [1] рассматривается преобразование политики безопасности в правила, соответствующие OpenFlow, но вопрос об оптимизации этих правил не поднимается. В статье [2] предложен метод размещения контроллеров, являющийся модифицированной версией NSGA-II для многоцелевой задачи, дающий конкурентные результаты. В статье [3] авторы применили NSGA-II для задачи маршрутизации с учетом отказоустойчивости, но акцент на обеспечении безопасности неясен.

В статье [4] рассматривается многоцелевая оптимизация в промышленных системах управления (ICS), применяя эволюционные методы для обнаружения уязвимостей. Подход из [5] направлен на уменьшение и распределение правил TCAM для сжатия, но не учитывает динамической конфигурации. В [6] применено обучение с подкреплением для обнаружения атак, а в [7] применено обучение в федеративной среде на распределенных SDN-доменах. Кроме того, в [8] приведен гибридный NSGA-II с CNN для IDS [11]. Последние работы также предлагают использование трансформеров для увеличения точности обнаружения атак [12].

Несмотря на многочисленные исследования, являясь актуальными проблемами, пока недостаточно известно, как использовать сами политики безопасности с учетом таких противоположных целей, как минимизация риска, уменьшение задержек и ограничение использования TCAM. Данная работа заполняет этот пустой пространство, сочетая многоцелевую эволюционную оптимизацию с точной моделью ограничений и динамикой

трафика. Уникальностью является то, что мы впервые демонстрируем фронты Парето по метрикам безопасность-производительность в полной плотности, что свидетельствует об наличии компромиссов.

Постановка задачи и математическая модель

Рассмотрим программно-определяемую сеть (SDN), которая состоит из множества коммутаторов $S = \{s_1, s_2, \ldots, s_n\}$, управляемых центральным контроллером. Каждому коммутатору назначается набор правил безопасности $R = \{r_1, r_2, \ldots, r_m\}$, каждая из которых имеет следующие параметрами $r_i = (src_i, dst_i, proto_i, port_i, action_i, priority_i)$

Целью данного исследования является обозначить оптимальное подмножество $R^* \subset R$, которое соответствовало эффективной фильтрации вредоносного трафика с минимальными задержками и ресурсами (TCAM).

Сформулируем задачу многоцелевой оптимизации следующим образом:

$\min_{R^*}[F_1(R), F_2(R), F_3(R), -F_4(R)]$

где

- $\mathrm{F}_1(\mathrm{R})$: риск атак – доля вредоносных потоков, которых не удалось отфильтровать;
- $\mathrm{F}_2(\mathrm{R})$: средняя задержка трафика (мс);
- $\mathrm{F}_3(\mathrm{R})$: загрузка TCAM (%);
- $\mathrm{F}_4(\mathrm{R})$: через один пропуск (Мбит/с), максимизируется.

Вероятностная модель атак: считается, что каждая атака имеет вероятность проникновения, зависящую от наличия доступа подходящего правила и его приоритета. Общий риск можно вычислить по формуле:

$F_1(R) = \sum_{a \in A} \quad P_a \cdot (1 - Coverage(a, R))$

где P_a – вероятность атаки a, $Coverage$ - бинарная функция совпадения с правилом.

Наказания и ограничения:

- $P_{conflict}(R)$ - зона наказания за противоречивые правила;
- Ограничения: $F_3(R) \leq TCAM_{max}$, $F_2(R) \leq Delay_{max}$.

Нормализация целей:

$$F_i' = \frac{F_i(R) - F_i^{min}}{F_i^{max} - F_i^{min}}, i = 1..4$$

Итоговая функция приспособленности:

$$W(R) = w_1 F_1' + w_2 F_2' + w_3 F_3' - w_4 F_4' + P_{conflict}(R)$$

Считается, что правила частично совпадают по полям источника, назначении действию (ALLOW или DENY). Если только одно совпадение между правилами, то мы считаем, что правила не конфликтуют. В случае конфликта применяем штраф на приспособленность решения.

Если только одно совпадение между правилами, то мы считаем, что правила не конфликтуют. В случае конфликта применяем штраф на приспособленность решения.

Алгоритмы оптимизации. В работе реализованы и сравнены три подхода:

Greedy – наибольшую приоритет получают правила, которые содержат наибольший блок трафика.

Дифференциальная Эволюция (DE) – стохастический метод оптимизации с оператором мутации и кроссовера.

NSGA-II – многоцелевой эволюционный алгоритм, который использует non-dominated sorting, crowding distance и элитарность.

Предложенная математическая модель охватывает все ключевые аспекты задачи: риск атак в контексте безопасности, задержку и пропускную способность как показатели производительности, а также ограниченность памяти TCAM как ресурсное ограничение. Такой выбор метрик оправдан, поскольку усиление мер безопасности неизбежно сопровождается ухудшением производительности – увеличением задержек, снижением пропускной способности и ростом потребления ресурсов, что подтверждается результатами предыдущих исследований [1-2]. Учитывая вероятностный характер атак и введение штрафов за конфликтующие правила, предложенная модель отражает реальные условия работы SDN и служит надежной основой для многокритериальной оптимизации политики безопасности.

Результаты исследований

Среда экспериментов: Mininet 2.3.0, Ryu 4.34, Python 3.10
Сети: Fat-Tree (k=4), Linear, Ring
Генераторы трафика: iperf3, hping3
Сценарии:
Нормальный – только легитимный трафик.
Смешанный – легитимный и DoS-атаки вместе.
Атакующий – 80% вредоносного расхода (атаки hping3 флуда, сканирование TCP).
Параметры NSGA-II:
Размер популяции: 120
Количество поколений: 200
Вероятность кроссовера: 0.85
Вероятность мутации: 0.25

В каждом сценарии проводились измерения ряда ключевых метрик. Риск атак оценивался как доля вредоносного трафика, который не был заблокирован политикой, с учетом разработанной вероятностной модели. Средняя задержка определялась по времени прохождения тестовых пакетов между узлами, пропускная способность как фактическая скорость передачи легитимного трафика (по данным iperf3), а загрузка TCAM как процент занятости таблицы правил контроллера. Для повышения достоверности результатов каждая из метрик усреднялась на основе нескольких повторных запусков эксперимента.

Сводные численные результаты представлены в таблице 1, где показаны усреднённые значения риска, задержки, загрузки TCAM и пропускной способности для трёх алгоритмов.

Таблица 1 – Сравнительные результаты работы алгоритмов оптимизации политик безопасности в SDN

Метод	Риск (%)	Задержка (мс)	TCAM (%)	Проп. способ. (Мбит/с)
Greedy	1	55	95	6500
DE	4.5	30	75	8200
NSGA-II	2.3	20	50	9100

Сравнение методов по метрикам безопасности и производительности. На рисунке 1 показано сравнение трёх подходов – Greedy, DE и NSGA-II по ключевым метрикам риска, задержки, загрузки TCAM и пропускной способности. Greedy-метод практически исключает риск атак (~1%), но за счет резко возросшей задержки (~50 мс) и почти полного заполнения TCAM (~90%), что приводит к снижению пропускной способности сети. Heuristic-алгоритм демонстрирует более сбалансанные показатели (риск ~5%, задержка ~30 мс, TCAM ~60%, пропускная ~8 Гбит/с), но уступает по большинству метрик многоцелевому подходу NSGA-II. Решение NSGA-II достигает компромисса: риск атак снизился до ~3% при умеренной задержке (~20 мс) и загрузке TCAM (~50%), обеспечивая наибольшую пропускную способность (~9 Гбит/с). Такой результат свидетельствует, что эволюционный алгоритм NSGA-II сумел найти политику безопасности, превосходящую эвристический метод по совокупности показателей [2]. При этом небольшое увеличение риска по сравнению с greedy-решением оправдано значительным выигрышем в производительности сети.

Анализ результатов: одноцелевой жадный алгоритм (Greedy), фокусируясь на максимальном снижении риска, жертвует производительностью – дополнительная фильтрация трафика и многочисленные правила безопасности увеличивает задержки и снижает пропускную способность. Напротив, NSGA-II одновременно учитывает несколько целей и находит Парето-оптимальное решение, при котором улучшение одного показателя невозможно без ухудшения другого.

В итоге NSGA-II достигает лучшего баланса метрик: риск атак остается низким, а накладные задержки и нагрузка на ресурсы минимальны. Это согласуется с позицией теория компромиссов (trade-off) в кибербезопасности: попытки полностью устранить угрозы (свести риск к нулю) ведут к росту издержек – увеличению задержек, ресурсов и снижению пропускной способности. Многокритериальная оптимизация позволяет выработать компромиссную политику безопасности, обеспечивающую приемлемый уровень защиты при высоком качестве обслуживания сети.

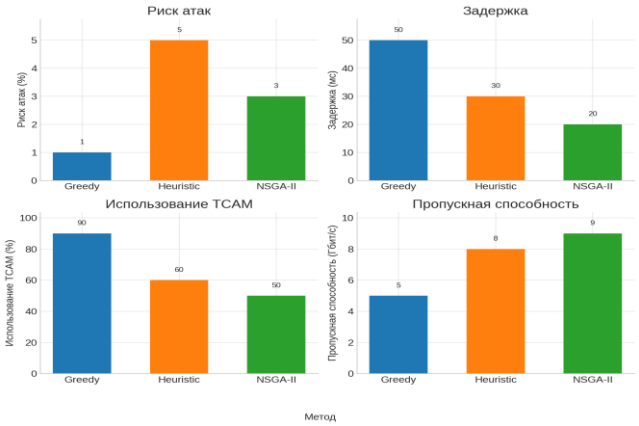

Рисунок 1 – Сравнение трёх подходов (Greedy, Heuristic, NSGA-II) по ключевым метрикам: риск атак, задержка, использование памяти TCAM и пропускная способность

Результаты NSGA-II в трёх сценариях трафика показано на рисунке 2 – нормальном, смешанном и атакующем. В нормальном режиме, без вредоносного трафика, алгоритм NSGA-II демонстрирует практически нулевой риск (около 2%), обеспечивая минимальную задержку (~10 мс), невысокую загрузку TCAM (примерно 30%) и высокую пропускную способность (~9,5 Гбит/с). При наличии смешанного трафика, когда в потоках встречаются отдельные вредоносные пакеты, риск повышается до 8% – алгоритм активирует дополнительные фильтры, что приводит к росту задержки (~20 мс), загрузке TCAM (~60%) и незначительному снижению пропускной способности (~8 Гбит/с). В условиях активной атаки нагрузка на систему возрастает максимально: риск атак достигает примерно 15% (часть атак всё же проходит), задержка удваивается вдвое (~40 мс), а пропускная способность падает до ~6 Гбит/с из-за необходимости обработки вредоносного трафика. TCAM при этом заполняется до 90% – для отражения атак требуется множество специализированных фильтров, которые занимают значительную часть таблицы потоков контроллера.

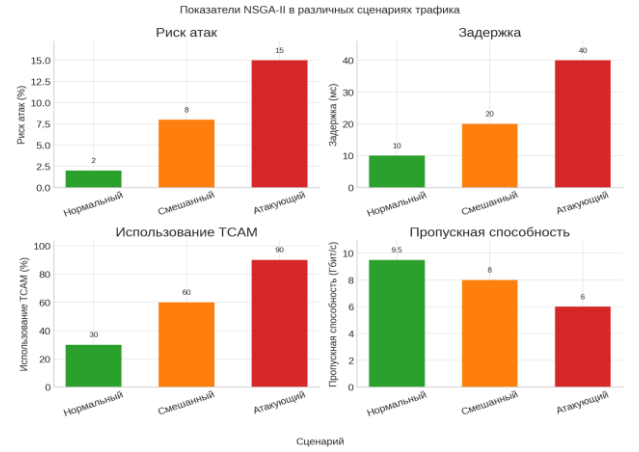

Рисунок 2 – Изменение метрик NSGA-II в трех сценариях трафика: нормальном (преимущественно легитимный трафик), смешанном и атакующем

Влияние разных сценариев на ключевые метрики отражает явный баланс между уровнем защиты и производительностью системы. При атакующем трафике NSGA-II активно использует ресурсы контроллера, добавляя правила для фильтрации вредоносных пакетов. В результате TCAM оказывается загруженной почти до 90%, что создает риск её переполнения. Это свидетельствует о том, что при высокой атакующей активности контроллеры и коммутаторы могут быть перегружены из-за большого количества создаваемых правил безопасности. Тем не менее, даже в условиях мощной атаки NSGA-II удаётся сохранить пропускную способность на уровне около 60% от исходной, предотвращая полный сбой в предоставлении сетевых услуг.

В отсутствие вредоносного трафика алгоритм практически не вмешивается: задержки и риски минимальны, TCAM используется умеренно, а пропускная способность близка к

максимальной. Следовательно, NSGA-II имеет возможность динамически регулировать политику безопасности в зависимости от текущей ситуации в сети – включая защиту только тогда, когда она действительно необходима. Такой подход обеспечивает гибкую адаптацию: высокую эффективность в нормальных условиях и надежную защиту при возникновении угроз.

Парето-фронт оптимальных решений NSGA-II. На рисунке 3 представлен Парето-фронт для двух целей – задержки и риска атак, а на рисунке 4 – трёхмерная модель, учитывающая также использование ресурсов TCAM.

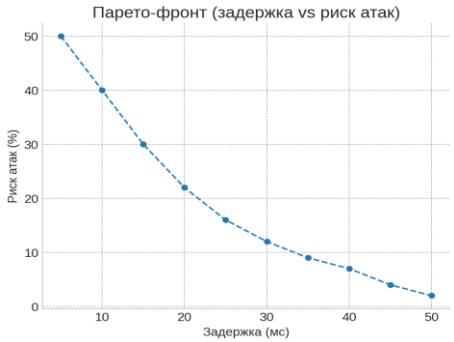

Рисунок 3 – Парето-фронт для двух целей – задержки и риска атак

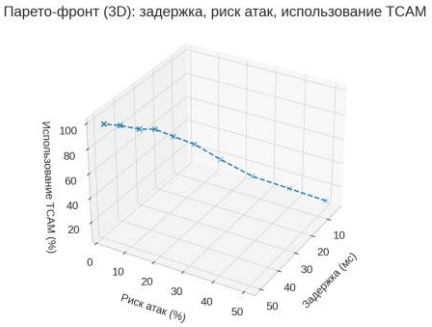

Рисунок 4 – Парето-фронт (3D) для трёх целей – задержки, риска атак и использования ресурсов (TCAM)

График наглядно демонстрирует разнообразие оптимальных решений, найденных алгоритмом NSGA-II, каждое из которых представляет собой уникальную политику безопасности с определённым набором правил. Каждая точка на графике – это вариант, при котором невозможно улучшить один показатель, например снизить риск, не ухудшив другой, например увеличив задержку. Кривая Парето ясно показывает компромисс: чтобы уменьшить риск атак с примерно 50% до около 2%, требуется увеличить среднюю задержку с примерно 5 мс до 50 мс. И наоборот, минимальные задержки на уровне обычной сети (~5 мс) возможны только при принятии высокого риска (~50%). Такая обратная зависимость - характерная черта конфликтующих целей. В средней части графика расположены сбалансированные решения, сочетающие умеренный риск (~15%) и приемлемую задержку (~20 мс). Эти варианты наиболее интересны на практике, так как обеспечивают разумный уровень защиты при умеренном влиянии на производительность.

Введение третьей оси – процент заполнения TCAM (ось Z) позволяет проанализировать, как меняется использование ресурсов контроллера вдоль линии оптимальных решений. Видно, что по мере снижения риска (движение влево по оси Y) и роста задержек (вдоль оси X), заполнение TCAM возрастает. Это означает, что более безопасные политики требуют большего числа правил, загружая TCAM почти до предела - до 98% в точке с минимальным риском (~2%). На противоположной стороне графика расположены решения с минимальной задержкой и низкой нагрузкой на TCAM (~10%), но с более высоким риском (~50%). Если учитывать также пропускную способность, Парето-фронт становится четырёхмерным. В данном случае представлены его двумерные и трёхмерные проекции для удобства визуализации. Многокритериальный алгоритм NSGA-II формирует целый набор

оптимальных решений, создавая поверхность Парето в пространстве метрик. Это предоставляет администраторам гибкость. Можно выбрать более рискованную, но экономичную политику или наоборот, усилить защиту, пожертвовав производительностью и ресурсами.

Конвергенция алгоритма NSGA-II по поколениям. На рисунке 5 показана динамика сходимости алгоритма NSGA-II по поколениям, отражающая улучшение метрик в ходе эволюции решений.

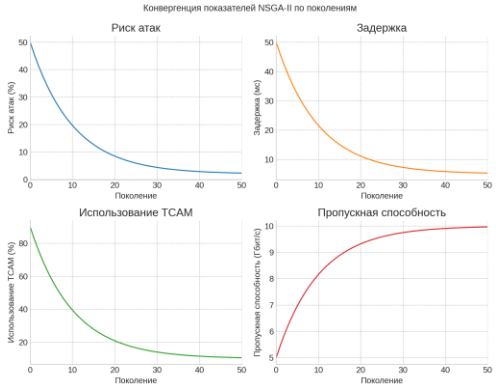

Рисунок 5 – Линии конвергенции NSGA-II – изменение лучших значений метрик по поколениям алгоритма

Графики наглядно демонстрируют, как в ходе эволюции популяции решений целевые показатели постепенно улучшаются. Примерно за 50 поколений алгоритм NSGA-II значительно снижает риск атак - с приблизительно 50% до 2%, и одновременно сокращает задержку с 50 мс до 5 мс. При этом уменьшается и загрузка памяти TCAM – с 90% до 10%. Параллельно с этим увеличивается максимальная пропускная способность: с 5 до 10 Гбит/с, что говорит о всё более эффективных решениях, находящихся алгоритмом. Форма кривых свидетельствует о сходимости – начиная с 30-40 поколений, улучшения по всем метрикам начинают замедляться, что указывает на достижение устойчивого уровня, близкого к оптимальному. Этот эксперимент подтверждает эффективность NSGA-II: благодаря механизму отбора и рекомбинации решений алгоритм быстро приближается к Парето-фронту. Замечено, что разные цели достигают стабильности в разное время: так, показатель пропускной способности стабилизируется уже к 20 поколению, в то время как риск атак продолжается снижаться до 40 поколения. Это связано с тем, что различные цели имеют разную степень сложности и в части компромиссов улучшая один параметр, NSGA-II старается не ухудшать другие.

Для иллюстрации компромиссов в таблице 2 приведены примеры трех Парето-оптимальных политик безопасности: с приоритетом максимальной безопасности, сбалансированной и ориентированной на максимальную производительность. Каждая из них представляет собой либо крайний, либо промежуточный вариант с соответствующими уровнями риска и эффективности.

Таблица 2 – Примеры решений на Парето-фронте при различном соотношении целей

Тип политики	Риск атак, %	Задержка, мс	TCAM, %	Пропускная способность, Мбит/с
Максимально безопасная	~2	~50	~98	~6500
Сбалансированная	~15	~20	~50	~8000
Максимально производительная	~50	~5	~10	~10000

Обсуждение научных результатов

Результаты экспериментов показали, что NSGA-II как по показателям безопасности, так и по показателям эффективности стабильно превосходит жадный алгоритм (Greedy) и метод дифференциальной эволюции (DE). Особенно хорошо NSGA-II справляется с задачей при высоких значениях сетевых угроз, когда важно быстро и сбалансировано отяготить ресурсы. Жадный подход может полностью снять риск атак путем жесткой фильтрации, но это

приведет к перегрузке TCAM и высоким задержкам, что неприемлемо. Хотя алгоритм DE достигает более сбалансированных результатов, для него характерна нестабильность, он хуже справляется с конфликтами правил. NSGA-II позволяет варьировать приоритеты, находить решения на Парето-фронте и является устойчивым к изменению сценариев трафика.

С точки зрения вычислительных затрат, предложенный метод требует больше времени по сравнению с алгоритмами Greedy и DE, однако остается вполне допустимым для офлайн оптимизации. В наших экспериментах алгоритм NSGA-II сходился примерно за 40-50 поколений при размере популяции 120, что эквивалентно нескольким минутам вычислений на стандартном оборудовании. Эти временные затраты оправданы улучшением качества полученных решений. При этом сам процесс оптимизации может выполняться асинхронно, то есть вне основного потока реального трафика, что сводит влияние на работу сети к минимуму.

На 2D и 3D изображениях Парето-фронтов можно четко увидеть компромиссные свойства: чтобы избавиться от риска, придется заплатить удручающей задержкой и загрузкой ресурсов. Наиболее сбалансированные решения лежат в центре фронта - с риском атак 2-5% и задержками до 20-25 мс. Анализ сходимости показал, что NSGA-II в среднем достигает стабильности по всем метрикам около 40-50 поколения, что свидетельствует о сбалансированном процессе эволюции и отборе подходящих вариантов. Оптимальными оказавшиеся значения весов (w1:w2:w3:w4)=(0.4:0.3:0.2:0.1), что означает акцент на минимизации риска и задержек, а также допуск загрузки TCAM и высокая пропускная способность.

Было замечено, что незначительные изменения в выбранных весовых коэффициентах приводят лишь к плавному смещению решений вдоль Парето-фронта, без резких скачков в качестве. К примеру, увеличение веса, отведённого пропускной способности, немного повышает допустимый уровень риска и одновременно снижает задержку в компромиссном решении – то есть происходит изменение приоритетов без потери оптимальности. Таким образом, полученное решение сохраняет устойчивость к умеренным изменениям в весах целей, что подтверждает гибкость предлагаемого метода и его адаптируемость под конкретные требования.

Перспективы развития

Исследование открывает новые весовые направления для развития модели, а также ее практического применения в реальных SDN-сетях:

Интеграция с ONOS и OpenDaylight - реализация предложенного подхода в виде модуля REST, используемого для реальной ведение-выводной политики безопасности.

Совмещение с методами глубокого обучения с подкреплением (Deep RL) – комбинирование NSGA-II совместно с PPO или DDPG для онлайн-обучения и для того, чтобы изменять веса целей по безопасности на основе наблюдений за сетью.

Federated Learning в мультидоменных SDN – обучение политик безопасности в распределенном виде без передачи конфиденциальных данных, что особенно важно для коллаборации между доменами и организациями [10].

Использование сверточных нейронных сетей (CNN) – для изучения сетевых шаблонов, прогнозирования потенциальной вредоносной активности и для динамического обновления приоритетов в NSGA-II.

Explainable AI (XAI) – возможность предоставлять объяснения по решениям отфильтровать трафик, в том числе суть, почему произошло блокирование конкретных связанных с сетевым потоком, что является актуальным для доверия операторам и для удобной налаживания системы [9].

Заключение

В данной работе был рассмотрен один из актуальных вопросов в области программно-определяемых сетей – оптимизация политик безопасности. Для решения многокритериальной задачи оптимизации в рамках SDN тут был применен NSGA-II, один из известных алгоритмов для этой цели. В расширенной модели учитывались вероятностная оценка атак, штрафы за конфликты правил и нормализация целевых функций, что существенно расширило возможности анализа сети. Проведённые эксперименты в Mininet с реалистичными сценариями трафика показали, что NSGA-II действительно выигрывает у Greedy и DE по качеству решения: Он находит более обширные Парето-множества, что

иллюстрирует большую гибкость алгоритма в поиске компромиссных решений. Исследование полученных Парето-фронтов показало, что во многих случаях невозможно минимизировать все цели одновременно, выявляя при этом "серые зоны" компромиссов, которые могут быть "золотой серединой" для практического применения. Визуализация результатов и исследование сходимости потенцировали стабильность и универсальность подхода.

На основании данного исследования могли бы быть продолжены работы в двух направлениях. Во-первых, следовало бы проверить и оценить разработанную модель на более крупных и сложных реальных или реальных для SDN сетей. Во-вторых, можно было бы объединить многокритерийную оптимизацию с хитрыми новейшими средствами искусственного интеллекта, что позволило бы находить более интересные решения или быстрее.

Список литературы

1. Optimal controller selection and migration in large scale software defined networks for next generation IoT / M. Shahzad et al // SN Applied Sciences. – 2023. – Vol. 5, Art. 309.
2. Adaptive population-based multi-objective optimization in SDN controllers for cost optimization / A.A. Qaffas et al // Physical Communication. – 2023. – Vol. 58, Art. 102006.
3. On the (in)security of the control plane of SDN architecture: A survey / Z.A. Bhuiyan et al // IEEE Access. – 2023. – Vol. 11. – P. 91550-91582.
4. Alzahrani A.O. ML-IDSDN: Machine learning based intrusion detection system for software-defined network / A.O. Alzahrani, M.J.F. Alenazi // Concurrency and Computation: Practice and Experience. – 2023. – Vol. 35, Art. e7438.
5. Towards robust SDN security: A comparative analysis of oversampling techniques with ML and DL classifiers / A. Bajenaid et al // Electronics. – 2025. – Vol. 14, № 5. – P. 995.
6. Mahadik S.S. Edge-Federated Learning-Based Intelligent Intrusion Detection System for Heterogeneous Internet of Things / S.S. Mahadik, P.M. Pawar, R. Muthalagu // IEEE Access. – 2024. – Vol. 12. – P. 81736-81757.
7. Survey of federated learning in intrusion detection / H. Zhang et al // Journal of Parallel and Distributed Computing. – 2025. – Vol. 195, Art. 104976.
8. Reinforcement learning-based SDN routing scheme empowered by causality detection and GNN / Y. He et al // Frontiers in Computational Neuroscience. – 2024. – Vol. 18, Article 1393025.
9. Explainable intrusion detection for cyber defences in the Internet of Things: Opportunities and solutions / N. Moustafa et al // IEEE Communications Surveys & Tutorials. – 2023. – P(99) 1-1.
10. Arreche O. XAI-IDS: Toward proposing an explainable artificial intelligence framework for enhancing network intrusion detection systems / O. Arreche, T. Guntur, M. Abdallah // Applied Sciences. – 2024. – Vol. 14, № 10, Art. 4170.
11. Ataa M.S. Intrusion detection in software defined network using deep learning approaches / M.S. Ataa, E.E. Sanad, R.A. El-khoribi // Scientific Reports. – 2024. – Vol. 14, Art. 29159.
12. Network intrusion detection model using wrapper-based feature selection and multi-head attention transformers / M. Umer et al // Scientific Reports. – 2025. – Vol. 15, Art. 28718.

Благодарность

Авторы выражают благодарность Министерству высшего образования и науки Республики Казахстан, выделившему грантовый проект на 2025-2027 годы. ИРН AP25796479.

Б.А. Шырын[1]*, Т.А. Ahanger[2], А.К. Жумадиллаева[1], Г.Б. Бекешова[1]

[1]Л.Н. Гумилев атындаағы Еуразия ұлттық университеті,
0100000, Қазақстан Республикасы, Астана қ., Сатпаев к-сі, 2
[2]Принс Саттам бин Абдулазиз университеті,
Сауд Арабия Корольдігі, Әл-Харж қ.
*e-mail: bexultan.shyryn@gmail.com

ТСАМ ЖӘНЕ КІДІРІС ШЕКТЕУЛЕРІ БЕРІЛГЕН БАҒДАРЛАМАЛЫ АНЫҚТАЛҒАН ЖЕЛІЛЕРДЕ (SDN) ҚАУІПСІЗДІК САЯСАТТАРЫН КӨП МАҚСАТТЫ ЭВОЛЮЦИЯЛЫҚ ОҢТАЙЛАНДЫРУ

Бұл мақала бағдарламалы анықталған желілердегі (SDN) қауіпсіздік саясатын оңтайландыру мәселесін қарастырады. Авторлар бұл мәселені шешуді көптеген мақсаттарды эволюциялық оңтайландырудың тиімді алгоритмі NSGA-II арқылы ұсынады. Ұсынылған тәсіл желілік

қауіпсіздікті қатаң сақтау қажеттілігі мен шектеулі есептеу ресурстарының қолжетімділігі арасындағы теңгерімге қол жеткізуге бағытталған. Трафикті сүзу тиімділігіне айтарлықтай әсер ететін деректерді берудің кешігуі және TCAM кестесінің өлшемі сияқты факторларға ерекше назар аударылады. Қауіптердің ықтималдығын бағалауды, мақсат функциясын қалыпқа келтіру әдістерін және ереже қайшылықтары үшін айыппұл коэффициенттерін пайдалануды қамтитын мақалада әзірленген модель негізінде оңтайландыру үш негізгі параметр бойынша орындалды: шабуыл қаупі, желі кідірісі және TCAM жүктемесі. Модельдеу Mininet және Ryu пакеттерін пайдалана отырып, қалыпты, аралас және шабуыл сияқты үш желі жұмысының сценарийін қамтыды. Ұсынылған әдісті дифференциалды эволюциямен (DE) және ашкөз алгоритммен (Greedy) салыстыру NSGA-II Парето шекарасы бойынша оңтайлы шешім бөлуге қол жеткізетінін, тезірек біріктірілетінін және сүзу дәлдігін сақтайтынын көрсетті. Сондай-ақ, қағазда ұрпақ ауысуларының, ауыспалы графиктердің және жүктеме профильдерінің визуализациясы ұсынылған. Қорытындыда ұсынылған үлгіні ONOS және OpenDaylight контроллерлерімен біріктіру әлеуеті талқыланады және Deep Reinforcement Learning, Federated Learning және Explainable AI негізіндегі гибридті шешімдерді пайдаланудың орындылығы талқыланады.

Түйін сөздер: *бағдарламалық қамтамасыз етумен анықталған желілер (SDN), көп мақсатты оңтайландыру, эволюциялық алгоритмдер, NSGA-II, желілік қауіпсіздік, аномалияны анықтау.*

B. Shyryn[1]*, T.A. Ahanger[2], A. Zhumadillayeva[1], G. Bekeshova[1]
[1]L.N. Gumilyov Eurasian National University,
0100000, Republic of Kazakhstan, Astana, Satpayev street, building 2
[2]Prince Sattam Bin Abdulaziz University,
Al Kharj, Saudi Arabia
*e-mail: bexultan.shyryn@gmail.com

MULTI-OBJECTIVE EVOLUTIONARY OPTIMIZATION OF SECURITY POLICIES IN SOFTWARE-DEFINED NETWORKS (SDN) GIVEN TCAM AND LATENCY CONSTRAINTS

This article examines the problem of optimizing security policies in software-defined networks (SDN). The authors propose solving this problem using NSGA-II, an efficient algorithm for evolutionary optimization of multiple objectives. The proposed approach aims to achieve a balance between the need to strictly enforce network security and the availability of limited computing resources. Particular attention is paid to factors such as data transmission latency and TCAM table size, which significantly affect the effectiveness of traffic filtering. Based on the model developed in the article, which includes threat probability assessments, objective function normalization methods, and the use of penalty coefficients for rule conflicts, optimization was performed across three key parameters: attack risk, network latency, and TCAM load. The simulation covered three network operation scenarios-normal, mixed, and attack-using Mininet and Ryu packets. A comparison of the proposed method with differential evolution (DE) and a greedy algorithm (Greedy) showed that NSGA-II achieves optimal solution distribution along the Pareto frontier, converges faster, and maintains filtering accuracy. The paper also presents visualization of generational transitions, tradeoff graphs, and load profiles. The conclusion discusses the potential for integrating the proposed model with ONOS and OpenDaylight controllers, and discusses the feasibility of using hybrid solutions based on Deep Reinforcement Learning, Federated Learning, and Explainable AI.

Key words: *software-defined networks (SDN), multi-objective optimization, evolutionary algorithms, NSGA-II, network security, anomaly detection.*

Сведения об авторах

Бексұлтан Андасұлы Шырын* – докторант кафедры компьютерной и программной инженерии факультета информационных технологий ЕНУ им. Л.Н. Гумилева, Астана, Казахстан; e-mail: bexultan.shyryn@gmail.com. ORCID: https://orcid.org/0009-0001-1880-1290.

Tariq Ahamed Ahanger – доктор PhD, доцент, университет принца Sattam Bin Abdulaziz, г. Эль-Хардж, Королевство Саудовская Аравия; e-mail: t.ahanger@psau.edu.sa. ORCID: https://orcid.org/0000-0002-4525-0738.

Айнур Канадиловна Жумадиллаева – кандидат технических наук, ассоциированный профессор кафедры компьютерной и программной инженерии факультета информационных технологий ЕНУ им. Л.Н. Гумилева, Астана, Казахстан; e-mail: Ay8222@mail.ru. ORCID: https://orcid.org/0000-0003-1042-0415.

Гульвира Бауыржановна Бекешова – магистр технических наук, старший преподаватель кафедры Информационной безопасности факультета информационных технологий ЕНУ им. Л.Н. Гумилева, Астана, Казахстан; e-mail: gulvirabauyrzhanovna@gmail.com. ORCID: https://orcid.org/0000-0002-1635-4693.

Information about the authors

Bexultan Shyryn* – PhD student of the Department of Computer and Software Engineering, IT Faculty at the L.N. Gumilyov ENU, Astana, Kazakhstan; e-mail: bexultan.shyryn@gmail.com. ORCID: https://orcid.org/0009-0001-1880-1290.

Tariq Ahamed Ahanger – Doctor of Philosophy, Professor (Associate) at Prince Sattam Bin Abdulaziz University, Al Kharj, Saudi Arabia; e-mail: t.ahanger@psau.edu.sa. ORCID: https://orcid.org/0000-0002-4525-0738.

Aynur Zhumadillayeva – Associate Professor of the Department of Computer and Software Engineering, IT Faculty at the L.N. Gumilyov ENU, Astana, Kazakhstan; e-mail: Ay8222@mail.ru. ORCID: https://orcid.org/0000-0003-1042-0415.

Gulvira Bekeshova – Senior Lecturer at the Department of Information Security, IT Faculty at the L.N. Gumilyov ENU, Astana, Kazakhstan; e-mail: gulvirabauyrzhanovna@gmail.com. ORCID: https://orcid.org/0000-0002-1635-4693.

Авторлар туралы мәліметтер

Бексұлтан Андасұлы Шырын* – Л.Н. Гумилева ат. ЕҰУ Ақпараттық технологиялар факультетінің Компьютерлік және программалық инженерия кафедрасының докторанты, Астана, Қазақстан; e-mail: bexultan.shyryn@gmail.com. ORCID: https://orcid.org/0009-0001-1880-1290.

Tariq Ahamed Ahanger – PhD докторы, доцент, Принс Саттам бин Абдулазиз университеті, Әл-Харж, Сауд Арабия Корольдігі; e-mail: t.ahanger@psau.edu.sa. ORCID: https://orcid.org/0000-0002-4525-0738.

Айнур Канадиловна Жумадиллаева – Л.Н. Гумилева ат. ЕҰУ Ақпараттық технологиялар факультетінің Компьютерлік және программалық инженерия кафедрасыны доценті, Астана, Қазақстан; e-mail: Ay8222@mail.ru. ORCID: https://orcid.org/0000-0003-1042-0415.

Гульвира Бауыржановна Бекешова – Л.Н. Гумилева ат. ЕҰУ Ақпараттық технологиялар факультетінің Ақпараттық қауіпсіздік кафедрасының аға оқытушысы, техникалық ғылымдар магистрі., Астана, Қазақстан; e-mail: gulvirabauyrzhanovna@gmail.com. ORCID: https://orcid.org/0000-0002-1635-4693.

Поступила в редакцию 20.10.2025
Поступила после доработки 02.12.2025
Принята к публикации 05.12.2025