DOI 10.37882/2223-2966.2025.06-2.25

МЕТОДЫ ЗАЩИТЫ МАРКИРОВАННОГО СЕТЕВОГО ПОТОКА С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ ЛОСКУТА: АНАЛИЗ УСТОЙЧИВОСТИ И ПРИМЕНЕНИЯ

METHODS FOR PROTECTING MARKED NETWORK TRAFFIC USING THE PATCHWORK TECHNIQUE: RESILIENCE ANALYSIS AND APPLICATION

L. Molkova
M. Gofman

Summary. This paper explores attacks on marked network traffic and methods of protecting it using the patchwork technique. A mathematical model for network traffic marking is presented, including the process of marker insertion and detection. The study analyzes the resilience of the method against various types of attacks, including timing perturbations, dummy packet insertion, repackaging, and multi-flow attacks with added noise. Simulation results are provided, confirming the reliability of the proposed approach under varying network conditions.

Keywords: traffic marking, patchwork method, traffic attacks, data protection, network analysis, noise resilience, timing perturbations, bipolar markers.

Молькова Лолита Юрьевна
Аспирант, Петербургский государственный университет путей сообщения Императора Александра I
lolita-molkova@mail.ru
Гофман Максим Викторович
доктор технических наук, профессор, Петербургский государственный университет путей сообщения Императора Александра I
gofman@pgups.ru

Аннотация. В данной статье рассматриваются атаки на маркированный сетевой поток и методы его защиты с использованием технологии метод лоскута. Приведена математическая модель маркирования сетевого трафика, включая процесс внедрения маркеров и их детектирование. Проанализированы характеристики устойчивости метода к различным видам атак, включая временные возмущения, вставку фиктивных пакетов, переупаковку и многопоточные атаки с добавлением шума. Представлены результаты моделирования, подтверждающие надежность предложенного подхода в условиях изменяющихся параметров сети.

Ключевые слова: маркирование трафика, метод лоскута, атаки на трафик, защита данных, сетевой анализ, устойчивость к шуму, временные возмущения, биполярные маркеры.

Введение

Современные киберугрозы становятся всё более изощрёнными, часто реализуясь в несколько этапов через анонимные или частично контролируемые сети. Злоумышленники используют цепочки скомпрометированных промежуточных узлов, шифрование, переупаковку пакетов и подмену заголовков для сокрытия своей активности и усложнения отслеживания [1–3]. Такие атаки могут быть реализованы через скрытые каналы, и из-за сетевых помех и высокой изменчивости трафика шаблоны атак, содержащиеся в потоке, могут быть искажены или утеряны, делая выявление нарушителя крайне затруднительным [4–6].

Существует два основных подхода к анализу сетевого трафика: активный и пассивный. В активном анализе маркер сетевого потока применяется для оперативного управления потоком данных и повышения уровня защиты, а при пассивном — для наблюдения, выявления аномалий и отслеживания утечек [7–10].

За последние два десятилетия рост сложности сетей, увеличение объёмов передаваемых данных и развитие цифровых угроз стимулировали активные исследования и разработку новых методов мониторинга и управления трафиком. Разрабатываются новые алгоритмы и методы для мониторинга, оценки и управления сетевыми потоками [11], [12]. Современные технологии позволяют анализировать параметры пакетов (размер, интервалы, направление) и с помощью машинного обучения определять типы протоколов [13-16], прогнозировать их использование [17] и обнаруживать аномальное поведение [18], включая кибератаки [19]. Однако пассивные методы анализа могут быть использованы злоумышленниками для получения конфиденциальной информации, таких как посещаемые веб-страницы [20], язык общения в VoIP [21] и даже частичное расшифрование защищенных разговоров [22, 23].

При этом пассивный анализ имеет ряд ограничений: сложность алгоритмов, необходимость большого объема обучающих данных и уязвимость к манипуляциям с трафиком. В результате стало наблюдаться активное

развитие методов активного анализа [24], включая внедрение водяных знаков сетевого потока для маркировки данных и повышения точности мониторинга [25, 26]. Однако большинство существующие методов предполагают полный контроль над узлом-источником, что на практике мало реализуемо. В условиях частичного контроля или отсутствия прямого доступа к исходному потоку, маркировка должна выполняться на промежуточных узлах, где трафик может быть нестабилен и подвержен внешним воздействиям.

При анализе сетевого трафика важно учитывать статистические особенности параметров передаваемых пакетов. Исследования показывают, что такие характеристики, как размер пакетов и интервалы между ними, нередко следуют логнормальному распределению пакетов. Это объясняется тем, что природа генерации трафика формируется под влиянием множества факторов объем данных, передаваемых в сети, включая пользовательское поведение, протоколы передачи и особенности приложений [27]. Понимание этих особенностей позволяет не только более точно моделировать сетевую нагрузку, но и разрабатывать эффективные методы внедрения маркеров сетевого потока, минимально искажающих свойства трафика.

Модели распределения сетевого потока

Пакеты в сетевом трафике могут распределяться по различным статистическим законам, наиболее распространёнными среди которых являются логнормальное и пуассоновское распределения пакетов в сетевом потоке.

Пуассоновское распределение применяется для описания событий, происходящих с постоянной средней частотой. В применении к сетевому трафику она позволяет моделировать количество пакетов, поступающих в систему за фиксированный промежуток времени. Оно предполагает, что пакеты поступают независимо друг от друга и с постоянной средней интенсивностью, что характерно для трафика с низкими вариациями и равномерной нагрузкой.

Логнормальное распределение лучше использовать в ситуациях, когда размер пакетов, интервалы между ними и другие параметры изменяются в широких пределах, то есть наблюдается значительная изменчивость параметров трафика. Оно хорошо описывает асимметричное поведение с длинным правым хвостом, характерное для трафика с периодическими пиками активности, нестабильной загрузкой каналов и резкими скачками в скорости передачи данных.

Для упрощенных моделей часто используется пуассоновское распределение, однако при необходимости учета сложных динамических характеристик сетевого трафика предпочтение отдается логнормальному распределению, которое позволяет точнее описывать реальные условия передачи данных. В связи с этим, в данной статье, для моделирования сетевого потока будет использоваться логнормальное распределение пакетов.

Общее описание интервального метода

Интервальный метод маркировки сетевого потока — это способ внедрения водяного знака сетевого потока в сетевой трафик, основанный на изменении временных характеристик передачи пакетов. Сетевой поток разбивается на последовательные интервалы времени фиксированной или переменной длины и в зависимости от заданного шаблона изменяются характеристики пакетов (их наличие, задержку или частоту) внутри каждого интервала [28–33].

Водяной знак сетевого потока кодируется с использованием различий между интервалами: например, наличие пакетов в определённые интервалы может соответствовать биту «1», а их отсутствие — биту «0». Также могут использоваться более сложные схемы, где значение бита определяется числом пакетов, средней задержкой или другими статистических характеристик внутри интервала [32, 34].

Интервальный метод и его устойчивость к атакам

В целях защиты маркированного сетевого потока будет использоваться метод лоскута, основанный на интервальном методе. Этот метод демонстрирует высокую устойчивость к различным видам атак и сетевых возмущений, таких как временные возмущения, вставка фиктивных пакетов, потеря пакетов, заполнение пакетов, разделение или смешивание потоков, а также переупаковка пакетов. Ниже рассмотрим, почему использование маркеров сетевого потока данный метод обеспечивает надежность в условиях указанных атак [35-37]:

1. **Атака на изменения во временных возмущениях (задержки, изменения временных меток)**

Интервальный метод опирается на интервалы между определенными контрольными точками. Это позволяет системе сохранять точность даже при изменении временных характеристик трафика. Благодаря этому даже при варьирующейся задержке передача информации остается отслеживаемой, так как анализ опирается на относительные интервалы, а не фиксированные значения времени.

2. **Атака на внедрение ложных пакетов**

Вставка ложных пакетов, например, в атаках типа DoS или DDoS, когда в поток вставляются фиктивные данные,

метод сохраняет свою устойчивость. Он ориентирован на распознавание закономерностей между оригинальными пакетами, что позволяет эффективно фильтровать посторонние вставки.

3. **Атака на потерю пакетов**

Потери отдельных элементов потока не приводят к значительным искажениям в анализе, поскольку ключевым объектом анализа являются интервалы между маркерами, а не каждый конкретный пакет. Это позволяет системе сохранять работоспособность даже в условиях нестабильного соединения.

4. **Атака на изменение размеров пакетов**

Увеличение объема передаваемых данных (например, при упаковке дополнительных служебных данных) не влияет на корректность функционирования метода, поскольку он не анализирует содержимое или размеры, а только временные характеристики.

5. **Атака на разделение и смешивание потоков**

Даже при нарушении логической структуры передачи информации, метод продолжает корректно функционировать. Метод ориентируется на последовательность маркеров и интервалы между ними, а не на физическую или логическую организацию сетевого трафика.

6. **Атака на переупаковку пакетов**

Даже если порядок пакетов изменяется, интервальный метод позволяет восстановить структуру потока, поскольку анализирует временные характеристики последовательности, а не фиксированные позиции пакетов.

Интервальный метод позволяет сетевым системам оставаться устойчивыми к различным видам атак, поскольку он ориентирован на временные закономерности [37]. Это делает метод гибким и надежным инструментом для использования в нестабильных или потенциально скомпрометированных средах.

Атаки на невидимость: многопоточная атака и аддитивный шум

Дополнительно следует рассмотреть атаки на невидимость [17, 36, 37], такие как многопоточная атака, моделируемая путем добавления аддитивного шума в поток. Эти атаки нацелены на сокрытие реальной картины сетевого трафика, усложняя его анализ и маскируя истинные данные.

Многопоточные атаки и добавление шума

Злоумышленники могут генерировать несколько потоков с разными характеристиками, чтобы запутать систему анализа, усложняя идентификацию реального трафика. Такой метод затрудняет работу систем обнаружения вторжений и снижает эффективность стандартных инструментов анализа.

А также добавление шума может быть использован для заполнения пробелов в трафике или подмены реальных маркеров сетевого потока. Это используется, когда хотят сокрыть следы вторжений, фальсифицировать поведения пользователей или затруднить анализ трафика.

Моделирование многопоточной атаки с добавлением шума

Моделирование подобных атак [32, 36, 37] позволяет получить представление о степени надёжности интервального метода в условиях агрессивной внешней среды.

Позволяет проанализировать стабильности метода при искусственном искажении потока и оценить чувствительности алгоритма к внедрённым ложным данным, а также проверить способности восстановления исходной структуры потока при вмешательстве.

Проведение таких испытаний является важным элементом комплексной проверки эффективности метода лоскута и подтверждает его пригодность для использования в задачах сетевой безопасности при наличии сложных угроз и искажений.

Маркирование сетевого потока по методу лоскута

Метод лоскута представляет собой оригинальный, основанный на интервальном методе, способ внедрения маркеров сетевого потока в поток данных путем трансформации его структуры. Этот метод позволяет формировать своеобразные «лоскуты» в потоке, которые обеспечивают выявление изменений, утечек или манипуляций с данными. Основной принцип заключается в скрытом добавлении маркеров, что позволяет эффективно контролировать целостность передаваемых данных.

Модель вектора сетевых пакетов

Вектор сетевых пакетов определяется следующим формулой:

$$\mathrm{p} = \left(p_0, p_1, \ldots, p_N\right), \quad (1)$$

Где p_i -вектор пакетов, попавших в i-й интервал

N — это количество интервалов

Каждое p_i в векторе пакетов вычисляется по формуле

$$p_i = M * t * v, \quad (2)$$

Где v — случайная величина, имеющая логнормальное распределение

t — длительность временного интервала,

M — максимальное количество пакетов

Модель построения маркера

В этой статье используются две модели построения маркерных последовательностей. Общая структура маркера описывается следующим образом:

$$\mathrm{m} = \left(m_1, m_2, \ldots, m_N\right) = \alpha \otimes \left(1, -1\right) \tag{3}$$

Где $\otimes$— операция кронекерово произведение,

$\alpha = \left(\alpha_0, \alpha_1, \ldots \alpha_{\frac{N}{2}}\right)$ — биполярный вектор [38]

Модель внедрения информационного маркера в сетевой поток с использованием принципа лоскута

Формирование маркированного вектора пакетов выполняется по следующей схеме:

$$\boldsymbol{p}_{marker} = \left(p_0^{'}, p_1^{'}, \ldots, p_N^{'}\right) \tag{4}$$

Процесс построения маркированного вектора следует данным правилам:

$$\left(p_{2(i-1)+1}, p_{2i}\right) = \begin{cases} \left(p_{2(i-1)+1}, p_{2i}\right), \text{ если } p_{2(i-1)+1} \geq p_{2i} \text{ и } m_i = 1 \\ \left(p_{2i}, p_{2(i-1)+1}\right), \text{ если } p_{2(i-1)+1} < p_{2i} \text{ и } m_i = 1 \\ \left(p_{2(i-1)+1}, p_{2i}\right), \text{ если } p_{2(i-1)+1} \leq p_{2i} \text{ и } m_i = -1 \\ \left(p_{2i}, p_{2(i-1)+1}\right), \text{ если } p_{2(i-1)+1} > p_{2i} \text{ и } m_i = -1 \end{cases} \tag{5}$$

Формула расчета корреляции между найденным маркером и переданным

Пусть $\tilde{m}_n$ — восстановленный маркер

m_n— оригинальный маркер

Тогда взаимная корреляция задается формулой:

$$R\left(\tilde{m}, m, k\right) = \sum_n \left(\tilde{m}_n \cdot m_{n+k}\right) \tag{6}$$

Где k — сдвиг, с которым сравниваются элементы восстановленного маркера $\tilde{m}$ и оригинального маркера $\boldsymbol{m}$. Оригинальный маркер сдвигается вправо на k позиций, после чего оценивается степень совпадения с восстановленным маркером.

Целью является найти тот сдвиг, при котором корреляция максимальна. Это значение соответствует предполагаемой позиции вставки маркера в сетевой поток.

Для того чтобы вынести решения о наличие маркера в потоке используется оценка взаимной корреляции, а именно отношение максимального значение к минимальному (по модулю):

$$A = \left| \frac{\max\limits_{k \in \{-N, -N+1, \ldots, N\}} R\left(\tilde{m}, m, k\right)}{\min\limits_{k \in \{-N, -N+1, \ldots, N\}} R\left(\tilde{m}, m, k\right)} \right| \tag{7}$$

Где $\left| \cdot \right|$ — оператор взятие абсолютного значения

A — оценка взаимной корреляции между восстановленным маркером и оригинальным маркером

R — значение корреляции между восстановленным маркером и оригинальным маркером

Если в анализируемом сетевом потоке маркер отсутствует, то величина A близка к 1. Но, если $A \geq \mathrm{t}$, где t — порог вынесения решения о наличие маркера в анализируемом сетевом потоке. То, можно вынести решение о наличии маркера в потоке.

Результаты моделирования для сравнительной оценки устойчивости маркирования сетевого потока

Традиционно в качестве α используется псевдослучайная биполярная последовательность. Но в работе [38] предлагается в качестве α использовать следующий вектор

$$\alpha = \beta \otimes \gamma \tag{8}$$

Где γ — специально расширяющаяся последовательность, длиной N_γ, и β — биполярная последовательность, длиной N_β. При этом $N_\beta * N_\gamma = \frac{N}{2}$

Их Кронекерово произведение $\beta \otimes \gamma$ позволяет создать маркер с улучшенными корреляционными свойствами, так как такая конструкция обеспечивает более равномерное распределение битов и высокую чувствительность к нарушению последовательности.

При моделировании использовалось были применены два маркера:

1. **Псевдослучайная биполярная последовательность**
2. **Предельная биполярная расширяющаяся последовательность (ПБРП)**, предложенная в работе Гофман М.В. [38].

В качестве первого маркера использовалась псевдослучайная биполярная информационная последовательность определяющаяся уравнением (3), при $N_\beta = 28$ и $N_\gamma = 1$, в котором α — псевдослучайная маркерная последовательность, формируемая генератором с определённым начальным значением. Маркировка внедрялась в поток согласно формулам (4) и (5), а обнаружение про-

изводилось с помощью взаимной корреляции по формулам (6) и (7), используя вектор из (3).

Во втором же маркере применялась **предельная биполярная расширяющаяся последовательность (ПБРП)**, построенная по принципу, описанному в [38]. В этом случае α строится по формуле (8). В частности,

$$\beta = (1,1,1-1-11-1)$$

$$\gamma = (-1-11-1)$$

Это дает $N_\beta = 7$, $N_\gamma = 4$, что совпадает с длиной маркера, построенного по первому варианту. Соответственно, при таких длинах обоих маркеров они оказываются равными по длине. Построение, внедрение и обнаружение осуществляется согласно формулам (3), (4), (5), (6), (7) и (8).

Анализ результатов моделирования

Графики, представленные в статье, иллюстрируют два типа ошибок при детектировании маркера:

- **Ложноположительные результаты** — ситуация, когда маркер отсутствует, но детектор ошибочно его фиксирует (рис. 1).
- **Ложноотрицательные результаты** — ситуация, когда маркер присутствует, но детектор его не обнаруживает (рис. 2).

Анализ графиков на рисунках 1 и 2 показывает, что при выборе порога равным 1,4 маркер, построенный на основе ПБРП, демонстрирует лучшие характеристики по сравнению с псевдослучайным маркером. В частности, вероятность ложноположительного срабатывания для ПБРП составляет 0.1394 (13.94 %), в то время как для псевдослучайного маркера она равна 0.1659 (16.59 %). Это свидетельствует о снижении ложных срабатываний на 15.96 %. Аналогично, вероятность ложноотрицательного срабатывания для ПБРП составляет 0.4828 (48.28 %), тогда как для псевдослучайного маркера — 0.7127 (71.27 %), что указывает на снижение данного показателя на 32.29 %.

Использование ПБРП позволяет повысить устойчивость схемы маркирования к ошибкам второго рода и уменьшить вероятность ложного обнаружения, обеспечивая тем самым более высокую надежность выявления маркера в потоке.

Графики показывают, что ПБРП сохраняет высокую детектируемость при изменении параметров шума. В отличие от псевдослучайной биполярной последовательности, предложенная ПБРП демонстрирует более устойчивые характеристики.

Предложенный метод маркирования сетевого потока на основе интервального метода лоскута показывает хорошие результаты при аддитивном логнормальном распределении, обеспечивая надёжность обнаружения маркера в условиях высокой изменчивости сети.

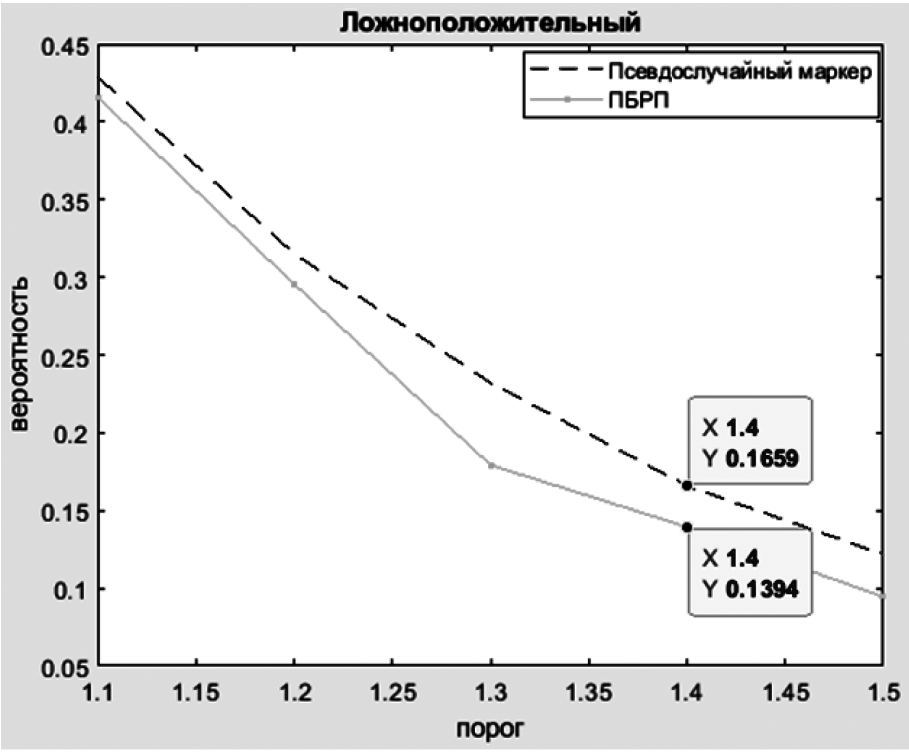

Рис. 1. Ложноположительные результаты

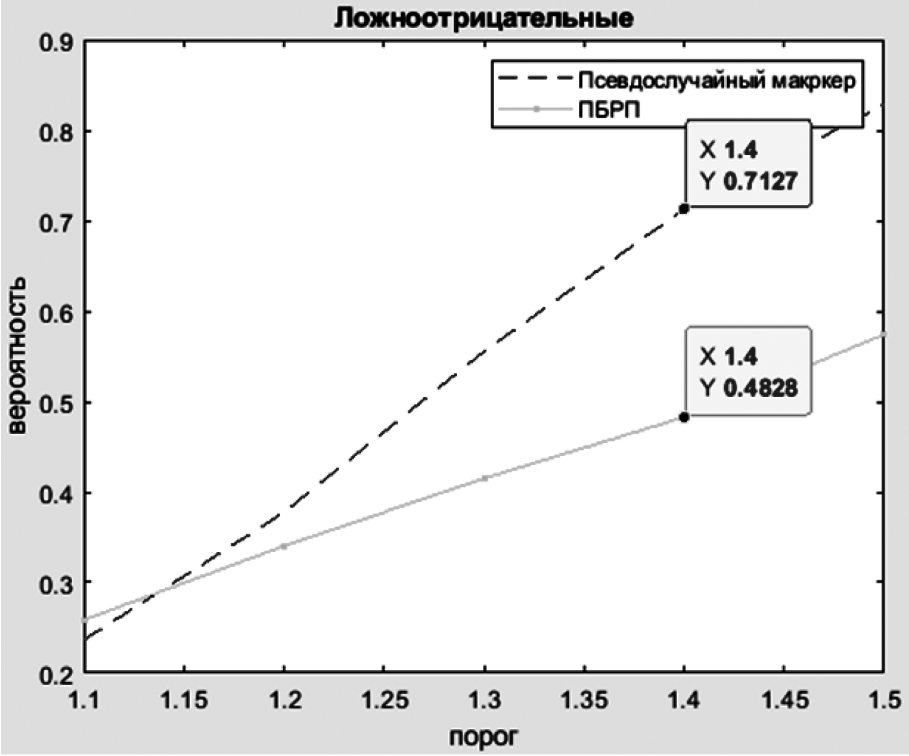

Рис. 2. Ложноотрицательные результаты

Заключение

В данной работе рассмотрен подход к защите сетевого трафика с применением метода лоскута, основанного на интервальном методе маркирования. Разработанная модель продемонстрировала высокую устойчивость к ряду искажений, включая временные возмущения, вставку фиктивных пакетов, потери и переупаковку данных. Особенностью метода является использование предельной биполярной расширяющейся последовательности (ПБРП) в качестве маркера сетевого потока, что обеспечивает его устойчивость при аддитивном шуме и многопоточным атакам. Результаты моделирования показали, что при логнормальном распределение пакетов в сочетании с использованием ПБРП позволяет достичь высокой точности и надежности обнаружения атак даже в условиях нестабильной и зашумленной сетевой среды.

ЛИТЕРАТУРА

1. Blum A., Song D., Venkataraman S.: 'Detection of interactive steppingstones: algorithms and confidence bounds. Proc. 7th Int. Symp. on Recent Advances in Intrusion Detection, Sophia Antipolis, France, September 2004, pp. 258–277
2. Yuan Y., Ge J., Cheng G. DeMarking: A defense for network flow watermarking in real-time //Computers & Security. — 2025. — С. 104355.
3. Feng W. et al. Ip-pealing: a robust network flow watermarking method based on ip packet sequence //Chinese Journal of Electronics. — 2024. — Т. 33. — №. 3. — С. 694–707.
4. Li T. et al. HeteroTiC: A robust network flow watermarking based on heterogeneous time channels //Computer Networks. — 2022. — Т. 219. — С. 109424.
5. Wang X. et al. Sleepy watermark tracing: An active network-based intrusion response framework //IFIP International Information Security Conference. — Boston, MA: Springer US, 2001. — С. 369–384.
6. Feng W. et al. HSTW: A robust network flow watermarking method based on hybrid packet sequence-timing //Computers & Security. — 2024. — Т. 139. — С. 103701.
7. Fu X. et al. On flow marking attacks in wireless anonymous communication networks //Journal of Ubiquitous Computing and Intelligence. — 2007. — Т. 1. — №. 1. — С. 42–53.
8. Yu W. et al. DSSS-based flow marking technique for invisible traceback //2007 IEEE Symposium on Security and Privacy (SP'07). — IEEE, 2007. — С. 18–32.
9. Karnani S., Agrawal N., Kumar R.A comprehensive survey on low-rate and high-rate DDoS defense approaches in SDN: taxonomy, research challenges, and opportunities //Multimedia Tools and applications. — 2024. — Т. 83. — №. 12. — С. 35253–35306.
10. Pan X. et al. Long PN code based traceback in wireless networks //International Journal of Performability Engineering. — 2012. — Т. 8. — №. 2. — С. 173.
11. Bates A. Detecting compute cloud co-residency with network flow watermarking techniques. — 2012.
12. Bates A. et al. Detecting co-residency with active traffic analysis techniques //Proceedings of the 2012 ACM Workshop on Cloud computing security workshop. — 2012. — С. 1–12.

13. Zand A. et al. Rippler: Delay injection for service dependency detection //IEEE INFOCOM 2014-IEEE Conference on Computer Communications. — IEEE, 2014. — С. 2157–2165.
14. Houmansadr A., Borisov N. SWIRL: A Scalable Watermark to Detect Correlated Network Flows //NDSS. — 2011.
15. Cheng L.E. I. et al. Survey of network flow identification technology //Application Research of Computers/Jisuanji Yingyong Yanjiu. — 2013. — Т. 30. — №. 10.
16. Fu X. et al. On countermeasures to traffic analysis attacks //IEEE Systems, Man and Cybernetics SocietyInformation Assurance Workshop, 2003. — IEEE, 2003. — С. 188–195.
17. Levine B.N. et al. Timing attacks in low-latency mix systems //Financial Cryptography: 8th International Conference, FC 2004, Key West, FL, USA, February 9-12, 2004. Revised Papers 8. — Springer Berlin Heidelberg, 2004. — С. 251–265.
18. Fu C. et al. Delay normalization method of defending against timing-based attacks on anonymous communication systems //J. Southeast Univ., Nat. Sci. Ed. — 2009. — Т. 39. — №. 4. — С. 738–741.
19. Zhang L., Wang Z., Liu H. Survey on network flow watermarking technologies //Comput. Sci. — 2011. — Т. 38. — №. 11. — С. 7–11.
20. Chen Z., Pu S., Zhu S. Traceback technology for anonymous network //J. Comput. Res. Dev. — 2012. — Т. 49. — С. 111–117.
21. Nematollahi M.A. et al. Network stream watermarking //Digital Watermarking: Techniques and Trends. — 2017. — С. 165–179.
22. Mittal P. et al. Stealthy traffic analysis of low-latency anonymous communication using throughput fingerprinting //Proceedings of the 18th ACM conference on Computer and Communications Security. — 2011. — С. 215–226.
23. Wang X., Chen S., Jajodia S. Tracking anonymous peer-to-peer voip calls on the internet //Proceedings of the 12th ACM conference on Computer and communications security. — 2005. — С. 81–91.
24. Park Y.H., Reeves D.S. Adaptive timing-based active watermarking for attack attribution through steppingstones //Proc. Second Int. Workshop on Security in Distributed Computing Systems, Washington, DC, USA. — 2005. — С. 107–113.
25. Houmansadr A., Kiyavash N., Borisov N. Non-blind watermarking of network flows //IEEE/ACM Transactions on Networking. — 2013. — Т. 22. — №. 4. — С. 1232–1244.
26. Gong X., Rodrigues M., Kiyavash N. Invisible flow watermarks for channels with dependent substitution, deletion, and bursty insertion errors //IEEE transactions on information forensics and security. — 2013. — Т. 8. — №. 11. — С. 1850–1859.
27. Zhang L. et al. Synchronization in inter-packet delay-based flow correlation techniques //J. Comput. Res. Dev. — 2011. — Т. 48. — №. 9. — С. 1643–1651.
28. Iacovazzi A. et al. DropWat: An invisible network flow watermark for data exfiltration traceback //IEEE Transactions on Information Forensics and Security. — 2017. — Т. 13. — №. 5. — С. 1139–1154.
29. Pyun Y.J. et al. Interval-based flow watermarking for tracing interactive traffic //Computer Networks. — 2012. — Т. 56. — №. 5. — С. 1646–1665.
30. Wang X., Yang M., Luo J. A novel sequential watermark detection model for efficient traceback of secret network attack flows //Journal of network and computer applications. — 2013. — Т. 36. — №. 6. — С. 1660–1670.
31. Yu L. et al. Dynamic interval-based watermarking for tracking down network attacks //2021 IEEE 21st International Conference on Software Quality, Reliability and Security (QRS). — IEEE, 2021. — С. 52–61.
32. Houmansadr A., Borisov N. BotMosaic: Collaborative network watermark for the detection of IRC-based botnets //Journal of Systems and Software. — 2013. — Т. 86. — №. 3. — С. 707–715.
33. Wang X., Chen S., Jajodia S. Network flow watermarking attack on low-latency anonymous communication systems //2007 IEEE Symposium on Security and Privacy (SP'07). — IEEE, 2007. — С. 116–130.
34. Lin M. et al. Network flow watermarking method based on centroid matching of interval group //2015 IEEE International Conference on Progress in Informatics and Computing (PIC). — IEEE, 2015. — С. 628–632.
35. Ramsbrock D., Wang X., Jiang X. A first step towards live botmaster traceback //International Workshop on Recent Advances in Intrusion Detection. — Berlin, Heidelberg: Springer Berlin Heidelberg, 2008. — С. 59–77.
36. Ling Z. et al. Novel packet size-based covert channel attacks against anonymizer //IEEE Transactions on Computers. — 2012. — Т. 62. — №. 12. — С. 2411–2426.
37. Zhang L. et al. Survey on network flow watermarking: model, interferences, applications, technologies, and security //IET Communications. — 2018. — Т. 12. — №. 14. — С. 1639–1648.
38. Гофман М.В., Корниенко А.А. Предельные биполярные последовательности для робастного маркирования цифровых аудиосигналов по методу лоскута //Информатика и автоматизация. — 2023. — Т. 22. — №. 2. — С. 221–260.