ФОРМАЛИЗАЦИЯ, СВОЙСТВА И СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПОРОГОВОЙ МЕТРИКИ УСТОЙЧИВОСТИ ОДНОРАНГОВЫХ АНОНИМНЫХ СЕТЕЙ С TOR/I2P-ПОДОБНЫМИ АРХИТЕКТУРАМИ

В.Д. Зюзин, *Нижегородский государственный университет им. Н.И. Лобачевского, v.d.zyuzin@gmail.com.*

УДК 004.056:004.7:004.272.7:529.7

Аннотация. В работе предложен вероятностно-пороговый аппарат оценки устойчивости одноранговых анонимных сетей к анализу трафика. Введены метрики вероятности перехвата (ВП) и вероятности успешного соединения (ВУС), а также пороговые показатели n_{50} и их обобщение n_{a}, задающие минимальный размер сети для достижения требуемого уровня безопасности. На базе комбинаторных моделей маршрутизации (классическая *Tor*-тип и две предложенные модификации без/с повторами узлов) выполнены вычислительные эксперименты на сетке $m = 1 \ldots 10,\ j = 1 \ldots 10$. Показано, что предложенные модели снижают порог n_{50} по сравнению с *Tor*-подобной архитектурой: на 6-12 % (без повторов) и до 20-25 % (с повторами) при малых m и j, сохраняя преимущество 2-7 % при росте параметров. Полученные результаты позволяют обосновывать выбор длины маршрута и минимального масштаба домена безопасности при проектировании анонимных сетей и виртуальных частных сетей.

Ключевые слова: одноранговые сети; анонимизация трафика; виртуальные частные сети; *Tor*; *I2P*; маршрутизация; вероятность перехвата; вероятность успешного соединения; пороговые метрики.

FORMALIZATION, PROPERTIES, AND COMPARATIVE ANALYSIS OF THE THRESHOLD ROBUSTNESS METRIC FOR PEER-TO-PEER ANONYMOUS NETWORKS WITH TOR/I2P-LIKE ARCHITECTURES

V.D. Zyuzin*, N.I. Lobachevsky State University of Nizhny Novgorod.*

Annotation. A probabilistic-threshold framework is proposed for evaluating the robustness of peer-to-peer anonymous networks against traffic analysis. The study introduces the interception probability (IP) and the successful connection probability (SCP), as well as threshold metrics n_{50} and their generalized form n_{a}, which define the minimum network size required to achieve a given level of security. Based on combinatorial routing models (classical Tor-type and two proposed hybrid variants – without and with node repetitions), computational experiments were performed on a grid of parameters $m = 1 \ldots 10$ and $j = 1 \ldots 10$. The results show that the proposed models reduce the threshold n_{50} compared to Tor-like architectures by 6-12 % (without repetitions) and up to 20-25 % (with repetitions) for small m and j, while maintaining a 2–7 % advantage as parameters increase. The obtained results provide a basis for selecting optimal route lengths and determining the minimal security domain size when designing anonymous communication and virtual private network systems.

***Keywords*:** peer-to-peer networks; traffic anonymization; virtual private networks; *Tor*; *I2P*; routing; interception probability; successful connection probability; threshold metrics.

Введение

Одноранговые сети (*Peer-to-Peer* – *P*2*P*) играют ключевую роль в современных распределенных системах, обеспечивая децентрализованный обмен данными, балансировку нагрузки и высокую устойчивость к отказам [1-3]. В отличие от классической клиент-серверной архитектуры, *P*2*P*-сети не имеют центральной точки отказа, но с ростом возможностей анализа трафика и усилением интереса к массовому наблюдению [4-7] защита конфиденциальности и устойчивости в таких сетях становится крайне важной.

Маршрутизация через промежуточные узлы – основной метод анонимизации в системах *Tor, I2P, Tarzan* и др. – призвана скрыть связь узла-инициатора и узла-получателя, однако она подвержена различным атакам. Одной из самых серьезных угроз является корреляция трафика: активные методы сопоставления временных паттернов и объемов пакетов между точками входа и выхода позволяют разоблачать участников связи [8-11]. Например, исследование *DeepCorr* показало, что современные методы машинного обучения способны восстанавливать сопоставления потоков с высокой точностью, несмотря на шум и задержки [5]. Анализ обзоров *Traffic Analysis Attacks on Tor* подтверждает, что наблюдатель с доступом к части сети может вычислить соответствие входящих и исходящих потоков без дешифрования содержимого [6]. Кроме того, методы *fingerprinting, DNS*-корреляции (*DefecTor*) и низкозатратные атаки через *NetFlow* увеличивают уязвимость *Tor*-подобных систем к анализу трафика [7, 9, 10].

*P*2*P*-сети имеют свои классические уязвимости: атаки *Sybil, Eclipse*, загрязнение маршрутов и отказ в обслуживании (*DoS/DDoS*) [12-14]. Например, обзор *A Survey of Peer-to-Peer Security Issues* осветил проблему дезинформации маршрутов и атак на доверие участников [12]. В более свежем обзоре *Recent Advancements in Secure Peer-to-Peer* представлены новые угрозы с учетом машинного обучения и динамики сетей [14].

В предыдущих исследованиях [15-18] была сформирована математическая база для комбинаторной оценки числа маршрутов в одноранговых сетях, предложены модификации классических *Tor*-подобных моделей, включающие два варианта: (1) участие узла-инициатора и узла-получателя в цепочке маршрутизации; (2) снятие ограничения на повторное использование узлов в маршруте. Однако при этом оставались неформализованными количественные показатели устойчивости соединений к частичной компрометации узлов.

Цель настоящей работы – развить ранее предложенный комбинаторный аппарат за счет введения количественных метрик, позволяющих оценивать устойчивость маршрутов к компрометации.

Для этого вводятся метрика вероятности перехвата (ВП) – вероятность того, что маршрут передачи данных проходит хотя бы через один скомпрометированный промежуточный узел, и метрика вероятности успешного соединения (ВУС), дополняющая вероятность безопасного установления маршрута без компрометации. На их основе формируется пороговая метрика n_{50}, определяющая минимальный размер сети n, при котором при компрометации m промежуточных узлов вероятность перехвата не превышает 0,5. Дополнительно рассматривается обобщенная форма n_{α}, задающая аналогичный порог при произвольном уровне α (например, 0,3 или 0,1).

Предложенные метрики позволяют перейти от комбинаторного подсчета маршрутов к вероятностно-пороговому анализу устойчивости одноранговых сетей к трафиковому анализу и частичной компрометации узлов.

Формализация структуры одноранговой системы и базовые комбинаторные модели маршрутов

Рассматривается одноранговая система следующего вида:

$$A \to X_1 \to \cdots X_j \to B$$

где: A – узел-инициатор; B – узел-получатель; X_1 – первый промежуточный узел; X_j – последний промежуточный узел.

В такой системе передача данных от узла-инициатора к узлу-получателю осуществляется через j промежуточных узлов, выбранных из множества n узлов сети. Каждый маршрут представляет собой упорядоченную последовательность узлов, в которой определены начало, конец и фиксированное количество промежуточных позиций. При этом возможны различные топологические варианты – от полностью уникальных цепочек до маршрутов с частичным повторением вершин.

Для классической луковичной архитектуры *Tor*-типа показано, что число независимых маршрутов при фиксированном числе промежуточных узлов (j) определяется произведением (1):

$$F_{Tor}(n, j) = \prod_{i=1}^{j}(n - i - 1), n \geq j + 2 \quad (1)$$

где: $F_{Tor}(n, j)$ – количество возможных маршрутов через j промежуточных узлов в классической луковичной архитектуре *Tor*-типа; n – общее количество узлов в рассматриваемой одноранговой сети (включая узла-инициатора (A) и узла-получателя (B)); j – число промежуточных узлов, через которые должен пройти маршрут между узлом-инициатором (A) и узлом-получателем (B).

Формула (1) отражает идею последовательного выбора узлов без повторов: первый промежуточный узел выбирается из $n-2$ возможных, второй – из $n-3$ и так далее до j-го включительно. Такое построение обеспечивает строгое разделение ролей в маршруте и исключает замыкание цепочки на уже посещенные узлы, что соответствует принципам луковичной маршрутизации *Tor*. Стоит отметить, что данная формула учитывает число уникальных маршрутов между узлом-инициатором и узлом-получателем при отсутствии повторов и при условии, что сами узел-инициатор и узел-получатель не участвуют в промежуточной передаче. Модель отражает строго упорядоченную схему *Tor*, в которой маршруты формируются узлом-инициатором заранее и остаются фиксированными на всем протяжении сессии.

В ряде практических задач (например, при адаптивной маршрутизации в децентрализованных виртуальных частных сетях (ВЧС)) возникает необходимость ослабления этих ограничений.

В работе [17] было предложено обобщение классической схемы, в котором узел-инициатор и узел-получатель могут участвовать в цепочке маршрутизации с целью увеличения комбинаторного пространства маршрутов. Для данной модели количество возможных маршрутов без повторного участия промежуточных узлов определяется выражением (2):

$$F_1(n,j)=\begin{cases}0 & n<j\\ n-2 & j=1, n\geq 3\\ (n-1)+(n-2)^2 & j=2, n\geq 2\\ (n-2)\times\big((n-1)+(n-2)+(n-3)\big) & j=3, n\geq 3\\ ((n-1)+(j-2)(n-2)+(n-2)(n-j))\Pi_{m=2}^{j-1}(n-m) & 4\leq j\leq n\end{cases} \quad (2)$$

где: $F_1(n,j)$ – количество возможных маршрутов без повторного участия промежуточных узлов для одноранговой системы, состоящей из n узлов и j промежуточных узлов.

В работе [18] было получено универсальное выражение (3), позволяющее учитывать повторное использование промежуточных узлов, что еще увеличивает комбинаторное пространство маршрутов:

$$F_2(j,n)=\frac{(n-1)^{j+1}-(-1)^{j+1}}{n} \quad (3)$$

где: $F_2(n,j)$ – количество возможных маршрутов с повторным участием промежуточных узлов для одноранговой системы, состоящей из n узлов и j промежуточных узлов.

Комбинированное рассмотрение моделей (1-3) позволяет описывать всю иерархию маршрутизационных моделей. Эти зависимости становятся основой для последующего построения вероятностных метрик вероятности перехвата (ВП) и вероятности успешного соединения (ВУС), а также для определения пороговых характеристик устойчивости (n_{50} и $n_{\text{а}}$).

Вероятностные метрики устойчивости (ВП и ВУС)

Для количественной оценки устойчивости одноранговых сетей к частичной компрометации узлов вводятся две взаимодополняющие метрики: ВП и ВУС, позволяющие оценить, насколько маршруты между доверенными участниками связи остаются защищенными при наличии скомпрометированных промежуточных узлов.

Рассматривается сеть из n узлов, где два из них – узел-инициатор (A) и получатель (B) – считаются доверенными. Оставшиеся $n-2$ узлов потенциально могут быть захвачены злоумышленником. Предположим, что маршрут содержит j промежуточных узлов и, что злоумышленник контролирует ровно m из них ($0 \leq m \leq n-2$). Перехват трафика возможен, если хотя бы один из построенных маршрутов проходит через один из скомпрометированных узлов.

Поскольку исключение перехваченных узлов из маршрута эквивалентно сокращению эффективного размера сети с n до $(n-m)$, вероятность успешного соединения выражается через отношение числа «чистых» маршрутов к общему количеству всех маршрутов:

$$\text{ВУС}(m,n,j)=\frac{F(n-m,j)}{F(n,j)} \quad (4)$$

где: F обозначает обобщенную комбинаторную функцию, определяющую количество возможных маршрутов для заданной архитектуры. Дополняющая вероятность характеризует долю маршрутов, которые хотя бы один раз проходят через захваченные узлы. Она задает ВП:

$$\text{ВП}(m,n,j)=1-\text{ВУС}(m,n,j) \quad (5)$$

Формулы (4-5) универсальны и корректны для любого диапазона параметров m, n, и j. При $m = 0$ все маршруты считаются безопасными: ВУС = 1, ВП = 0. При увеличении числа скомпрометированных узлов m доля безопасных маршрутов монотонно уменьшается, и при $m \geq n-j$ построение маршрута становится невозможным: ВУС → 0, ВП → 1.

С практической точки зрения метрика ВП отражает вероятность успешного захвата хотя бы одного маршрута злоумышленником при произвольном распределении компрометированных узлов, а ВУС – вероятность того, что маршрут останется защищенным. Таким образом, ВП и ВУС образуют основу вероятностного анализа устойчивости сети и позволяют перейти от чисто комбинаторных оценок количества маршрутов к оценке реальной надежности передачи данных при частичной компрометации инфраструктуры.

Использование данных метрик дает возможность:

- количественно описывать эффект увеличения числа узлов сети (n) на устойчивость маршрутов;
- оценивать критические значения m и j, при которых сеть теряет защищенность;
- проводить сравнительный анализ различных архитектур маршрутизации.

Полученные зависимости (4-5) служат исходной основой для построения пороговых характеристик устойчивости n_{50} и n_{a}, рассматриваемых далее.

Пороговые метрики устойчивости (n_{50} и n_{a})

Метрики ВП и ВУС позволяют количественно оценивать вероятность компрометации маршрутов, однако для практического применения удобнее использовать скалярные пороговые показатели, определяющие момент перехода сети в «устойчивое» состояние. Такие показатели позволяют установить минимальный масштаб сети, при котором вероятность перехвата становится статистически незначимой, а вероятность успешного соединения преобладает.

Пороговая метрика n_{50} определяется как минимальное количество узлов n, при котором вероятность перехвата ВП не превышает 0,5 для заданных j и m:

$$n_{50}(m,j) = min\{n: \text{ВП}(m,n,j) \leq 0{,}5\} \quad (6)$$

Фактически n_{50} характеризует минимальный размер сети, обеспечивающий вероятность безопасного соединения не менее 50 %. Иными словами, при $n < n_{50}$ атакующий имеет преимущество: вероятность компрометации маршрута превышает 0,5; при $n \geq n_{50}$ система переходит в устойчивый режим, где вероятность успешного соединения становится доминирующей.

Аналогично вводится обобщенная метрика n_{a}, задающая порог для произвольного уровня безопасности α ($0 < \alpha < 1$):

$$n_{\alpha}(m,j) = min\{n: \text{ВП}(m,n,j) \leq \alpha\} \quad (6)$$

С точки зрения анализа защищенности сети, зависимость $n_{\text{a}} = F(m,j)$ описывает границу перехода от уязвимого состояния к устойчивому. Для каждой фиксированной длины маршрута j можно определить набор пар (m, n_{a}), при которых выполняется требуемое условие безопасности. Эти точки образуют

поверхность устойчивости, по которой можно судить о влиянии числа скомпрометированных узлов и топологической сложности сети на ее надежность.

Практическая интерпретация метрик имеет следующий вид:

- если $n < n_{\text{a}}$, сеть считается уязвимой (вероятность перехвата превышает α);
- если $n \geq n_{\text{a}}$, вероятность перехвата ниже α, и сеть функционирует в устойчивом режиме;
- при $\alpha = 0{,}5$ метрика n_{50} указывает минимальное значение n, при котором вероятность успешного соединения и вероятность перехвата становятся равновесными.

Использование n_{50} и n_{a} удобно не только для теоретических оценок, но и для прикладных задач проектирования одноранговых сетей. При фиксированных m и j можно вычислить минимально необходимое количество узлов для обеспечения требуемого уровня анонимности. В практических сценариях это позволяет оптимизировать баланс между избыточностью маршрутов, затратами на поддержание соединений и требуемой степенью устойчивости к трафиковому анализу.

Результаты вычислительных экспериментов и сравнительный анализ пороговых метрик устойчивости

Для количественной проверки теоретических положений проведено вычислительное моделирование, включающее определение пороговой метрики устойчивости $n_{50}(m, j)$ для диапазонов параметров $m = 1 \ldots 10$ и $j = 1 \ldots 10$.

Для каждой комбинации параметров вычислялись значения n_{50} для трех архитектур маршрутизации: F_{Tor}, F_1 и F_2.

Относительное улучшение определялось выражениями (7):

$$G_1 = \frac{n_{50}^{F_{Tor}} - n_{50}^{F_1}}{n_{50}^{F_{Tor}}} \times 100\%;\ G_2 = \frac{n_{50}^{F_{Tor}} - n_{50}^{F_2}}{n_{50}^{F_{Tor}}} \times 100\% \qquad (7)$$

Результаты вычислений пороговой метрики устойчивости n^{50} для диапазонов параметров $m = 1 \ldots 10$ и $j = 1 \ldots 10$ приведены в табл.1.

Таблица1.

j	m	n_{50} (F_{Tor})	n_{50} (F_1)	n_{50} (F_2)	$G_{F_{Tor}}^{F_1}$, %	$G_{F_{Tor}}^{F_2}$, %
1	1	4	4	4	0	0
1	2	6	6	6	0	0
1	3	8	8	8	0	0
1	4	10	10	10	0	0
1	5	12	12	12	0	0
1	6	14	14	14	0	0
1	7	16	16	16	0	0
1	8	18	18	18	0	0
1	9	20	20	20	0	0
1	10	22	22	22	0	0
2	1	6	5	5	16,7	16,7
2	2	10	9	9	10	10
2	3	13	12	12	7,7	7,7

j	m	n_{50} (F_{Tor})	n_{50} (F_1)	n_{50} (F_2)	$G_{F_{Tor}}^{F_1}$, %	$G_{F_{Tor}}^{F_2}$, %
2	4	17	16	16	5,9	5,9
2	5	20	19	19	5	5
2	6	23	22	22	4,3	4,3
2	7	27	26	26	3,7	3,7
2	8	30	29	29	3,3	3,3
2	9	34	33	33	2,9	2,9
2	10	37	36	36	2,7	2,7
3	1	8	7	7	12,5	12,5
3	2	13	12	11	7,7	15,4
3	3	18	17	16	5,6	11,1
3	4	23	22	21	4,3	8,7
3	5	28	26	26	7,1	7,1
3	6	33	31	31	6,1	6,1
3	7	37	36	36	2,7	2,7
3	8	42	41	41	2,4	2,4
3	9	47	46	45	2,1	4,3
3	10	52	51	50	1,9	3,8
4	1	10	9	8	10	20
4	2	17	15	14	11,8	17,6
4	3	23	21	21	8,7	8,7
4	4	29	28	27	3,4	6,9
4	5	35	34	33	2,9	5,7
4	6	42	40	39	4,8	7,1
4	7	48	46	46	4,2	4,2
4	8	54	53	52	1,9	3,7
4	9	61	59	58	3,3	4,9
4	10	67	65	65	3	3
5	1	12	11	9	8,3	25
5	2	20	18	17	10	15
5	3	28	26	25	7,1	10,7
5	4	35	34	33	2,9	5,7
5	5	43	42	40	2,3	7
5	6	51	49	48	3,9	5,9
5	7	59	57	56	3,4	5,1
5	8	66	65	63	1,5	4,5
5	9	74	72	71	2,7	4,1
5	10	82	80	79	2,4	3,7
6	1	14	13	11	7,1	21,4
6	2	23	22	20	4,3	13
6	3	33	31	29	6,1	12,1
6	4	42	40	38	4,8	9,5
6	5	51	49	47	3,9	7,8
6	6	60	58	57	3,3	5
6	7	69	68	66	1,4	4,3

j	m	n_{50} (F_{Tor})	n_{50} (F_1)	n_{50} (F_2)	$G_{F_{Tor}}^{F_1}$, %	$G_{F_{Tor}}^{F_2}$, %
6	8	78	77	75	1,3	3,8
6	9	88	86	84	2,3	4,5
6	10	97	95	93	2,1	4,1
7	1	16	15	12	6,2	25
7	2	27	25	23	7,4	14,8
7	3	37	36	33	2,7	10,8
7	4	48	46	44	4,2	8,3
7	5	59	57	55	3,4	6,8
7	6	69	67	65	2,9	5,8
7	7	80	78	76	2,5	5
7	8	90	89	86	1,1	4,4
7	9	101	99	97	2	4
7	10	112	110	108	1,8	3,6
8	1	18	17	14	5,6	22,2
8	2	30	29	26	3,3	13,3
8	3	42	41	38	2,4	9,5
8	4	54	53	50	1,9	7,4
8	5	66	65	62	1,5	6,1
8	6	78	77	74	1,3	5,1
8	7	90	89	86	1,1	4,4
8	8	102	101	98	1	3,9
8	9	114	113	110	0,9	3,5
8	10	127	125	122	1,6	3,9
9	1	20	19	15	5	25
9	2	34	32	29	5,9	14,7
9	3	47	45	42	4,3	10,6
9	4	61	59	56	3,3	8,2
9	5	74	72	69	2,7	6,8
9	6	88	86	83	2,3	5,7
9	7	101	99	96	2	5
9	8	114	113	110	0,9	3,5
9	9	128	126	123	1,6	3,9
9	10	141	140	137	0,7	2,8
10	1	22	21	17	4,5	22,7
10	2	37	35	31	5,4	16,2
10	3	52	50	46	3,8	11,5
10	4	67	65	61	3	9
10	5	82	80	76	2,4	7,3
10	6	97	95	91	2,1	6,2
10	7	112	110	106	1,8	5,4
10	8	127	125	121	1,6	4,7
10	9	141	140	136	0,7	3,5
10	10	156	155	151	0,6	3,2

Интерпретация результатов

Из анализа данных, представленных в табл. 1, видно, что при увеличении числа скомпрометированных узлов m и длины маршрута j пороговая метрика n_{50} монотонно возрастает. Это естественно отражает закономерность: чем больше узлов находится под контролем злоумышленника или чем длиннее маршрут, тем больше вероятность того, что хотя бы один из промежуточных узлов окажется скомпрометированным, а значит, сети требуется большее количество участников для достижения устойчивого режима. Для всех моделей наблюдается почти линейный рост n_{50} по параметру m, что подтверждает пропорциональное увеличение риска перехвата при добавлении каждого нового захваченного узла.

Однако характер роста различается в зависимости от типа модели. В классической архитектуре *Tor* увеличение m вызывает более резкий рост n_{50}, тогда как в разработанных модификациях, особенно в модели с повторами (F_2), наклон зависимости менее выражен. Это означает, что гибридные алгоритмы маршрутизации обеспечивают более плавное нарастание порога и дольше сохраняют сеть в устойчивом состоянии даже при росте числа атакуемых узлов.

Увеличение длины маршрута j также оказывает заметное влияние на момент вхождения системы в устойчивое состояние: с ростом j точка, при которой вероятность перехвата становится равной 0,5, смещается в область больших n. Иными словами, чем длиннее цепочка маршрутизации, тем позже сеть достигает порога n_{50}. Этот эффект особенно ярко проявляется в классической модели *Tor*, тогда как в предложенных решениях пересечение кривой ВП = 0,5 наступает при меньших n, что указывает на более быструю стабилизацию системы.

Наиболее выраженные различия между моделями наблюдаются при малых значениях j и m. Так, при $j = 4–5$ и $m = 1–2$ модель без повторов (F_1) снижает порог n_{50} на 6-12 %, а модель с повторами (F_2) – до 20-25 %. Это означает, что при относительно коротких маршрутах и ограниченном числе скомпрометированных узлов предложенные архитектуры позволяют достичь устойчивого состояния при значительно меньшем размере сети. При увеличении j и m разница между моделями постепенно сглаживается: эффект снижается до 2-7 %, но сохраняется во всем диапазоне параметров, что подтверждает общую устойчивость предложенных решений.

Сравнение моделей показывает, что реализация с разрешенными повторами узлов (F_2) всегда обеспечивает наименьший порог n_{50} и, следовательно, наиболее быстрое вхождение сети в устойчивый режим. Повторное использование узлов увеличивает число допустимых маршрутов, повышает энтропию топологии и снижает вероятность успешного анализа трафика. Модель F_1 (без повторов) остается промежуточным компромиссом между избыточностью и детерминированностью, обеспечивая умеренное, но устойчивое улучшение по сравнению с *Tor*.

Заключение

В работе предложен и формализован вероятностно-пороговый аппарат оценки устойчивости одноранговых анонимных сетей к анализу трафика: введены метрики вероятности перехвата (ВП) и вероятности успешного соединения (ВУС), а также пороговые показатели n_{50} и их обобщение n_{a}. На базе комбинаторных моделей маршрутизации показано, что гибридные решения (варианты без повторов и с повторами узлов) системно снижают требуемый размер сети для входа в «устойчивый режим» по сравнению с классической *Tor*-тип архитектурой. По результатам вычислительных экспериментов на сетке $m = 1 \ldots 10,\ j = 1 \ldots 10$

получено: при малых m и j выигрыш по порогу достигает ~6-12 % (без повторов) и до ~20-25 % (с повторами); при росте параметров эффект ожидаемо снижается, но сохраняется на уровне 2-7 % даже в «тяжелой» зоне. Отмечено также, что увеличение длины маршрута j оттягивает момент пересечения ВП=0,5 к большим n, однако гибридные модели смещают порог влево относительно *Tor*, обеспечивая более быструю стабилизацию.

Практическая значимость заключается в том, что n_{50} и n_{a} дают инженерно-интерпретируемую норму минимального масштаба домена безопасности при заданных m и j. Это позволяет проектировать анонимные сети с гарантированным уровнем риска, рационально выбирать длину маршрута на этапе установления соединения и обосновывать объем избыточности топологии. В прикладных условиях выбор варианта маршрутизации должен определяться масштабом и структурой сети. Для малых одноранговых доменов с ограниченным числом участников и короткими цепочками соединений целесообразно использовать модель с разрешенными повторами узлов (F_2), обеспечивающую быстрое достижение устойчивости за счет роста комбинаторного пространства маршрутов. Напротив, в более крупных сетях, где количество узлов значительно и вероятность случайных пересечений маршрутов возрастает, предпочтительно применение варианта без повторов (F_1), позволяющего удерживать предсказуемость топологии и снижать избыточность трафика при сохранении требуемого уровня анонимности.

Литература

1. Dingledine R., Mathewson N., Syverson P. Tor: The Second-Generation Onion Router // Proc. USENIX Security Symposium, 2004.
2. Freedman M., Morris R. Tarzan: A Peer-to-Peer Anonymizing Network Layer // ACM Conference on Computer and Communications Security (CCS), 2002.
3. Rennhard B., Plattner B. Introducing MorphMix: Peer-to-Peer Based Anonymous Internet Usage with Collusion Detection // Workshop on Privacy in the Electronic Society (WPES), 2002.
4. Jansen R., Johnson A., Syverson P. A Study of Bandwidth Denial-of-Service Attacks against Tor // USENIX Security Symposium, 2019.
5. Nasr M., Bahramali A., Houmansadr A. DeepCorr: Strong Flow Correlation Attacks on Tor Using Deep Learning // Proc. ACM CCS, 2018. – P. 1962-1976.
6. Cai X., Zhang X., Joshi B., Johnson R. Traffic Analysis Attacks on Tor: A Survey // MIT CSAIL Security Reading, 2023.
7. Biryukov A., Pustogarov I. DefecTor: DNS Leaks in Tor Revealed by Traffic Correlation // Proc. ACM CCS, 2016. DOI: 10.1145/2976749.2978397.
8. Overdorf R., Winter P., Jansen R. A Survey of De-anonymisation Attacks on Tor // arXiv preprint arXiv:2009.13018, 2020.
9. Tor Project. New Low-Cost Traffic Analysis Attacks and Mitigations // Tor Project Blog, 2023. URL: https://blog.torproject.org/new-low-cost-traffic-analysis-attacks-mitigations/ (дата обращения – 05.10.2025).
10. Tor Project. Traffic Correlation Using NetFlows // Tor Project Blog. – 2021. – URL: https://blog.torproject.org/traffic-correlation-using-netflows/ (дата обращения – 05.10.2025).
11. Johnson R., Jansen R., Juarez M. Flow Correlation Attacks on Tor Onion Service Sessions // Proc. NDSS Symposium, 2024.
12. Wallach D.S. A Survey of Peer-to-Peer Security Issues // Proc. International Symposium on Applications and the Internet (SAINT'02, Tokyo), 2002. – P. 400-414.

13. Jain R., Kumar R., Katti R. Security in P2P Networks: Survey and Research Directions // Computer Networks, 2015. – Vol. 83. – P. 311-336.
14. Khan M., Prakash A. Recent Advancements in Secure Peer-to-Peer Networks: A Survey // arXiv preprint arXiv:2509.19539, 2025.
15. Болдыревский П.Б. Формализация расчета вариантов маршрута в одноранговых сетях для задач информационной безопасности // Экономика и качество систем связи, 2025. – № 1(35). – С. 66-76.
16. Болдыревский П.Б. Разработка комбинаторных моделей для оценки количества допустимых маршрутов в одноранговых сетях с использованием инициатора и получателя в качестве промежуточных узлов // Экономика и качество систем связи, 2025. – № 1(35). – С. 76-84.
17. Зюзин В.Д. Комбинаторная модель оценки количества допустимых маршрутов при произвольном количестве промежуточных узлов с учетом включения инициатора и получателя // Вопросы защиты информации, 2025. – № 2. – С. 25-33.
18. Зюзин В.Д. Комбинаторная оценка алгоритма множественных стартовых соединений при снятии ограничения на повтор узлов // Экономика и качество систем связи, 2025. – № 3(38). – С. 181-190.