COMBINATORIAL ANALYSIS OF ROUTING SCENARIOS IN THE MULTIPLE - START CONNECTIONS ALGORITHM FOR PEER - TO - PEER NETWORKS

V.D. Zyuzin,N.A. Bashmurov,P.B. Boldyrevskii

Department of Mathematical Modelling of Economic Processes, Lobachevsky State University of Nizhni Novgorod, 23 Gagarin Av., Nizhni Novgorod 603022, Russia

ABSTRACT

Virtual private networks (VPNs) and peer-to-peer (P2P) systems are widely employed to protect information from unauthorised interception and analysis. However, traditional traffic-routing approaches in such networks remain vulnerable to "man-in-the-middle" attacks, especially during the initial connection-establishment phase. One promising countermeasure is the multiple-start connections (MSC) algorithm, whose core idea is that the initiator node simultaneously sends several initial packets to different intermediate nodes, thereby complicating an attacker's ability to identify the actual data path. A recently proposed enhancement permits the initiator and recipient nodes themselves to re-appear as intermediates, further increasing the combinatorial diversity of possible forwarding routes. Implementing this enhancement, however, requires a rigorous formalisation of the number of routing scenarios – something not yet achieved for the general case of an arbitrary number of routing steps and transmitted packets. The aim of this study is to formalise the calculation of the total number of possible routing scenarios in the MSC algorithm when the initiator and recipient may be reused as intermediate nodes for any given number of steps. Such a formalisation will enable precise control over route combinatorics and the development of practical methods to constrain it, including accounting for real-world network limitations. Future work will prepare the model for subsequent investigation of the proposed approach's resilience to man-in-the-middle attacks.

KEYWORDS

Routing protocols, Network security

1. INTRODUCTION

The rapid development of telecommunications and the ubiquity of distributed systems have sharply raised the bar for information-security requirements [1–4]. Traditional virtual-private-network (VPN) technologies – such as OpenVPN, WireGuard, and others – are typically organised in a client–server fashion [5–7]. While this simplifies administration, it creates a single point of failure and can facilitate man-in-the-middle (MITM) attacks [8]. Peer-to-peer (P2P) VPNs, by contrast, distribute routing responsibilities across all nodes, increasing flexibility and fault tolerance [9–11]; yet in some cases they complicate the task of securing connections [12].

One promising mechanism for improving traffic protection during session establishment is the multiple-start connections (MSC) algorithm [13–15]. Its essence is that the initiator (sender) node (A) does not rely on a single tunnel to the recipient (B); instead, it simultaneously opens several

DOI:10.5121/ijitmc.2025.13301

parallel tunnels through different nodes. An eavesdropper must therefore monitor all potential paths, greatly increasing the difficulty of mounting MITM attacks. Recent studies [16, 17] have examined an additional complication – allowing both the initiator (A) and the recipient (B) to re-appear as intermediate hops – thereby multiplying the total number of possible forwarding scenarios.

Extending the MSC algorithm, however, creates a need for a strict formalisation of the number of unique routes and for accounting for every possible packet-transfer case [17]. The aim of this article is to develop a detailed combinatorial analysis that quantitatively evaluates the combinatorial explosion in scenario count [18] as the number of routing hops and the number of simultaneously dispatched start packets increase. The formulae proposed here can serve as a foundation for further research into the security of P2P VPNs and for building probabilistic models of their resistance to MITM attacks.

2. THEORETICAL FORMALISATION

We present a formalisation of the MSC algorithm based on a combinatorial approach for peer-to-peer networks. Consider a system of $n$nodes in which node (A) is the initiator and node (B) is the recipient. In the general case, the initiator (A) simultaneously sends $k$start packets.

At the first routing step, initiator (A) chooses the recipients from the remaining $(n-1)$ nodes (excluding itself), so the total number of possible forwarding scenarios is given by the standard combinatorial expression:

$$C_{n-1}^{k} = \underbrace{C_{n-2}^{k-1}}_{Bis\ there} + \underbrace{C_{n-2}^{k}}_{Bno} \quad (1)$$

where the first term C_{n-2}^{k-1} represents the number of scenarios in which the recipient node (B) is necessarily included among the addressees (e.g., configuration BC), and the second term C_{n-2}^{k} gives the number of scenarios in which node (B) is not involved (e.g., configuration CD).

At the second routing step, we must separately examine the two situations: (i) the recipient node (B) was among the first-hop addressees, and (ii) (B) was not among them.

In the scenario where the recipient node (B) is among the first-hop recipients (for example, the configuration BC), both nodes (B) and (C) assume the same role that the initiator node (A) had in hop 1: each must choose its addressees from the remaining $(n-1)$ nodes, excluding itself. For the recipient node (B), the number of possible forwarding choices is C_{n-1}^{k}. For node (C), by contrast, we must again distinguish whether the recipient node (B) is or is not included among its own list of addressees:

$$\left(C_{n-2}^{k-1} + C_{n-2}^{k}\right) \quad (2)$$

The total number of variants for this scenario (with the recipient node (B) is therefore expressed as follows:

$$\underbrace{C_{n-1}^{k}}_{ForB} \times \underbrace{\left(C_{n-2}^{k-1} + C_{n-2}^{k}\right)^{k-1}}_{ForC} \quad (3)$$

Here, in the general case (for any number of packets k)), the exponent $(k-1)$ denotes the number of nodes – other than the recipient (B) – that simultaneously received packets in the previous step and now behave like the initiator node.

If, on the other hand, the recipient node (B) was not among the first-hop addressees (for example, configuration CD), then – just as in the initial step – all nodes are in equivalent positions, and the total number of scenarios is given by the following expression:

$$\left(C_{n-2}^{k-1} + C_{n-2}^{k}\right)^{k} \qquad (4)$$

Next, by combining these two scenarios—one in which the recipient node (B) is present and one in which it is absent – we obtain the final formula for the second step:

$$\underbrace{\underbrace{\underbrace{C_{n-2}^{k-1}}_{1\ step\ (Bis\ there)} \times \underbrace{C_{n-1}^{k}}_{ForB} \times \underbrace{\left(\underbrace{C_{n-2}^{k-1}}_{Bis\ there} + \underbrace{C_{n-2}^{k}}_{Bno}\right)^{k-1}}_{\text{nodes other than } B}}_{2\ step,\ 2.1\ (Bis\ there)} + \underbrace{\underbrace{C_{n-2}^{k}}_{1\ step\ (Bis\ there)} \times \underbrace{\left(\underbrace{C_{n-2}^{k-1}}_{Bis\ there} + \underbrace{C_{n-2}^{k}}_{Bno}\right)^{k}}_{2\ step,\ 2.2\ (Bno)}}_{2\ steps}}_{2\ steps} \qquad (5)$$

To simplify the notation, let us introduce the following symbols:

$$a = C_{n-2}^{k-1}, b = C_{n-2}^{k}, c = a + b = C_{n-1}^{k}$$

With these symbols in place, expression (5) can be condensed into the following compact form:

$$\underbrace{\underbrace{\underbrace{\underbrace{a}_{1\ step\ (Bis\ there)} \times \underbrace{c}_{ForB} \times \underbrace{\left(\underbrace{a}_{Bis\ there} + \underbrace{b}_{Bno}\right)^{k-1}}_{\text{nodes other than } B}}_{2\ step,\ 2.1\ (Bis\ there)} + \underbrace{\underbrace{b}_{1\ step\ (Bis\ there)} \times \underbrace{\left(\underbrace{a}_{Bis\ there} + \underbrace{b}_{Bno}\right)^{k}}_{2\ step,\ 2.2\ (Bno)}}_{2\ steps}}_{2\ steps} \qquad (6)$$

Or:

$$a \times c \times (a+b)^{k-1} + b \times (a+b)^{k} \qquad (6a)$$

An illustrative example of the MSC algorithm with three routing steps is presented in *Figure 1*. The scheme demonstrates how identical packets are redistributed by intermediate nodes, leading to multiple possible forwarding outcomes.

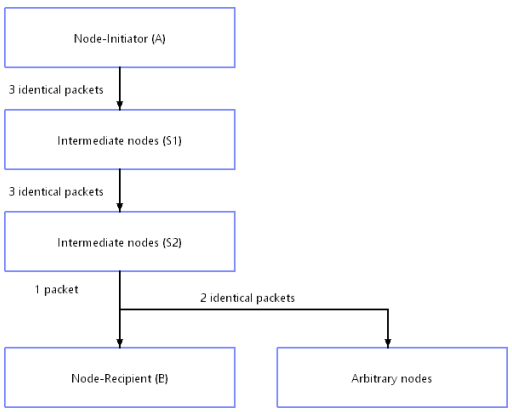

Figure 1. Example of the MSC algorithm execution for three routing steps

At the third and subsequent steps, the structure of the expressions obtained at the previous step repeats. Each new step generates factors that are combinations of expressions from the preceding steps. In the general case, the pattern for the third and later steps can be expressed as follows:

$$\begin{cases} a \text{ is multiplined by } c \times (a+b)^{k-1} \\ b \text{ and } c \text{ are multiplined by } (a+b)^{k} \end{cases} \quad \text{(A)}$$

Thus, the total number of scenarios after three steps is given by the following expression:

$$a \times c \times (a+b)^{k} \times \left(a \times c \times (a+b)^{k-1} + b \times (a+b)^{k}\right)^{k-1} + \\ + b \times \left(a \times c \times (a+b)^{k-1} + b \times (a+b)^{k}\right)^{k} \quad (7)$$

If the third hop is the final one, an additional routing rule of the MSC algorithm [14–17] must be taken into account:

- If the sender at the penultimate hop was the recipient node (B), it forwards all k $k$packets to nodes other than itself;
- If the sender was any other node, exactly one of the k packets must be addressed to the recipient node (B).

With this constraint, pattern (A) is modified for the last hop and can be written as follows:

$$\begin{cases} a \text{ is multiplined by } c \times a^{k-1} \\ b \text{ and } c \text{ are multiplined by } a^{k} \end{cases} \quad (B)$$

where the factor b is omitted, because it represents combinations of nodes in which the recipient node (B) is not involved.

Accordingly, formula (7), with this MSC routing rule taken into account, becomes:

$$a \times c \times a^{k} \times \left(a \times c \times a^{k-1} + b \times a^{k}\right)^{k-1} + b \times \left(a \times c \times a^{k-1} + b \times a^{k}\right)^{k} \quad (8)$$

After algebraic manipulations, formula (8) simplifies to:

$$\left(a^{k+1} \times c + b \times \left(a \times c \times a^{k-1} + b \times a^{k}\right)\right) \times \left(a \times c \times a^{k-1} + b \times a^{k}\right)^{k-1} = \\ = \left(a^{k+1} \times c + b \times a^{k}(c+b)\right) \times \left(a^{k}(c+b)\right)^{k-1} = \\ = a^{k} \times (a \times c + b \times (c+b)) \times a^{k^2-k} \times (c+b)^{k-1} = \\ = a^{k^2} \times (c+b)^{k-1} \times (a \times c + b \times (c+b))$$

And takes the final form:

$$a^{k^2} \times (c+b)^{k-1} \times (a \times c + b \times (c+b)) \quad (9)$$

Taking into account that $c = a + b$, we finally obtain:

$$a^{k^2} \times (a+2b)^{k-1} \times (a^2+ab+b \times (a+2b)) \qquad (10)$$

Building on the established patterns (A) and (B), the formulas for the fourth step were derived in an analogous way:

$$a^{k^3} \times (a+2b)^{k^2-k} \times (a^2+ab+b \times (a+2b))^{k-1} \times \\ \times \left((a^2+ab) \times (a+2b) + b \times (a^2+ab+b \times (a+2b))\right) \qquad (11)$$

And likewise for the fifth step:

$$a^{k^4} \times (a+2b)^{k^3-k^2} \times (a^2+ab+b \times (a+2b))^{k^2-k} \times \\ \times \left((a^2+ab) \times (a+2b) + b \times (a^2+ab+b \times (a+2b))\right)^{k-1} \times \\ \times ((a^2+ab) \times (a^2+ab+b \times (a+2b)) + b \times \\ \times \left((a^2+ab) \times (a+2b) + b \times (a^2+ab+b \times (a+2b))\right) \qquad (12)$$

Let us now rewrite the simpler formula (6), explicitly isolating $c = a + b$:

$$a \times (a+b) \times (a+b)^{k-1} + b \times (a+b)^k \qquad (13)$$

If the second hop is the final one, then—taking the above-mentioned MSC routing rule into account – formula (13) simplifies to:

$$a \times (a+b) \times a^{k-1} + b \times a^k \qquad (14)$$

And, after transformations, takes the form:

$$a^k \times (a+2b) \qquad (15)$$

From the derivations of formulas (15), (10), (11) and (12) above, it is evident that with each subsequent step the structure of the previous step's expressions is preserved, while a new factor – formed as a linear combination of the preceding factors – is introduced. In the general case this yields a recursive system of formulas for the number of routing scenarios $N(j)$:

$$N(j) = \begin{cases} a, & j = 1 \\ N_{j-1}^k \times A_{j-1}^{-1} \times A_j, & j \geq 2 \end{cases} \qquad (16)$$

Where the auxiliary factors $A(j)$ are defined as follows:

$$A(j) = \begin{cases} 1, & j = 1 \\ a+2b, & j = 2 \\ (a^2+ab) \times A_{j-2} + bA_{j-1}, & j \geq 3 \end{cases} \qquad (17)$$

Substituting the original values of $a$and $b$back into formulas (16) and (17) and rewriting them in terms of binomial coefficients, we obtain the final system of formulas:

$$N(j,k,n) = \begin{cases} \binom{n-2}{k-1}, & j = 1 \\ N_{j-1}^k \times A_{j-1}^{-1} \times A_j, & j \geq 2 \end{cases} \qquad (18)$$

Where:

$$A(j,k,n) = \begin{cases} 1, & j = 1 \\ \binom{n-1}{k} + \binom{n-2}{k}, & j = 2 \\ \binom{n-2}{k-1} \times \binom{n-1}{k} \times A_{j-2} + \binom{n-2}{k} \times A_{j-1}, & j \geq 3 \end{cases} \quad (19)$$

This system of formulas fully describes the number of possible routing scenarios in the MSC algorithm for any number of hops and enables the solution of tasks related to managing and optimising routes in secure peer-to-peer networks.

According to formulas (18) and (19), let us present a calculation example for the case of $n = 4$ nodes, $k = 2$ start packets, and $j = 2$ routing steps.

Step 1 ($j = 1$):

$$N(1,2,4) = \binom{4-2}{2-1} = \binom{2}{1} = 1$$

So, at the first hop there are 2 possible scenarios.

Step 2 ($j = 2$):

First compute auxiliary factor:

$$A(2,2,4) = \binom{n-1}{k} + \binom{n-2}{k} = \binom{3}{2} + \binom{2}{2} = 3 + 1 = 4$$

Then:

$$N(1,2,4) = (N(1,2,4))^2 \times A_1^{-1} \times A_2$$

Since $A_1 = 1$, we have:

$$N(1,2,4) = (2)^2 \times 1 \times 4 = 16$$

For $n = 4$, $k = 2$, and $j = 2$, the MSC algorithm yields a total of 16 possible routing scenarios.

3. RESULTS AND DISCUSSION

The derived system of formulas (16) - (19) provides an exact method to calculate the number of possible routing scenarios in the MSC algorithm. As demonstrated in the worked example, even for a small-scale configuration ($n = 4, k = 2, j = 2$), the number of routing scenarios rapidly increases to 16. This highlights the combinatorial explosion effect, where the scenario count grows exponentially with the number of routing steps.

Compared to traditional client–server VPN models, where the routing path is predetermined and static, the MSC approach significantly enhances unpredictability. In a classical scheme, an attacker attempting a man-in-the-middle (MITM) attack needs to compromise only a single route. In contrast, in MSC, the attacker must simultaneously monitor a rapidly growing set of possible paths, which becomes practically infeasible as n, k, and j increase.

This exponential growth of scenarios can therefore be directly interpreted as a factor of resilience against MITM attacks. The diversity of potential routes raises the cost of adversarial interception

and complicates traffic analysis. At the same time, this diversity comes at the price of additional packet duplication and potential routing overhead, which must be carefully managed.

A limitation of the current theoretical model is the absence of constraints reflecting real-world network conditions. In practice, nodes may have limited bandwidth, non-uniform reliability, and varying latency. Introducing such restrictions into the combinatorial framework would provide more realistic performance estimates. Future research should also focus on integrating probabilistic models of node availability and simulating MSC in real P2P VPN implementations (e.g., WireGuard or N2N).

4. CONCLUSION

In this study, a rigorous combinatorial formalisation of the MSC algorithm was presented. The obtained formulas enable exact calculation of the number of routing scenarios for arbitrary network sizes, numbers of start packets, and routing steps. The analysis demonstrates that the number of scenarios increases exponentially, which substantially strengthens the algorithm's resistance to MITM attacks by forcing an adversary to cover an infeasibly large set of routes.

In comparison with traditional VPN approaches, the MSC algorithm introduces significantly greater uncertainty into route establishment. This advantage, however, must be balanced against practical limitations, such as network overhead, packet duplication, and resource constraints of intermediate nodes.

Future work will address these limitations by extending the model with real-world parameters, including bandwidth restrictions, node reliability, and latency, as well as by validating the combinatorial predictions with simulation results. Such refinements will not only increase the accuracy of the model but also support the practical deployment of MSC-based routing in secure peer-to-peer networks.

REFERENCES

[1] M. Ciampa, *Security+ Guide to Network Security Fundamentals*, 2nd ed. Boston, MA, USA: Course Technology, 2005, 512 pp., ISBN: 978-0619216276.

[2] M. van Steen and A. S. Tanenbaum, *Distributed Systems*, 4th ed. Amsterdam, Netherlands: distributed-systems.net, 2023.

[3] V. I. Miroshnikov, I. A. Kuleshov, and V. I. Talagaev, "Trends and specifics of modern telecommunication systems," *Communication Equipment Technology*, no. 4 (160), 2022.

[4] A. N. Alpatov, "Development of distributed technologies and systems," *Industrial Science & Education*, no. 2 (14), 2015.

[5] S. Mackey, I. Mihov, A. Nosenko, F. Vega, and Y. Cheng, "A performance comparison of WireGuard and OpenVPN," in *Proc. 10th ACM Conf. on Data and Application Security and Privacy (CODASPY '20)*, New York, NY, USA: ACM, 2020, pp. 162–164.

[6] A. V. Roslyakov, *Virtual Private Networks: Fundamentals of Design and Use*. Moscow, Russia: Eko-Trendz, 2006, 300 pp. ISBN: 978-5-88405-078-5.

[7] A. V. Roslyakov, *Virtual Private Networks (VPN): Models and Analysis Methods*. Saarbrücken, Germany: LAP LAMBERT AcademicPublishing, 2011, 328 pp.

[8] W. J. Tolley, B. Kujath, M. T. Khan, N. Vallina-Rodriguez, and J. R. Crandall, "Blind in/on-path attacks and applications to VPNs," in *Proc. 30th USENIX Security Symp.*, 2021, pp. 3129–3146.

[9] S. Aoyagi, M. Takizawa, M. Saito, H. Aida, and H. Tokuda, "ELA: a fully distributed VPN system over peer-to-peer network," in *Proc. 2005 Symp. on Applications and the Internet*, Trento, Italy, 2005, pp. 89–92, doi: 10.1109/SAINT.2005.25.

[10] L. Deri and R. Andrews, "N2N: A layer two peer-to-peer VPN," in *Lecture Notes in Computer Science*, vol. 5122. Berlin, Germany: Springer, 2008, pp. 53–64, doi: 10.1007/978-3-540-70587-1_5.

[11] Y. Zou, *Network Performance and Key Management of VPN Tunnels between Autonomous Vehicles*, M.S. thesis, School of Electrical Engineering and Computer Science, KTH Royal Institute of Technology, Stockholm, Sweden, 2024, 120 pp.

[12] M. Varvello, I. Querejeta-Azurmendi, A. Nappa, P. Papadopoulos, G. Pestana, and B. Livshits, "VPN0: A privacy-preserving decentralized virtual private network," *arXiv preprint*, arXiv:1910.00159, 2019.

[13] A. A. Ryabov and M. A. Teterkin, "An approach to connection establishment in distributed VPNs," in *Proc. XXIII Scientific Conf. on Radiophysics Dedicated to the 100th Anniversary of N.A. Zheleztsov*, Nizhny Novgorod, Russia, May 2019, pp. 531–532.

[14] V. D. Zyuzin, A. A. Ryabov, and M. A. Teterkin, "Using the multiple-start connections method to obfuscate VPN sessions," in *Proc. XXVI Scientific Conf. on Radiophysics Dedicated to the 120th Anniversary of M.T. Grekhova*, Nizhny Novgorod, Russia, May 2022, pp. 535–536.

[15] P. B. Boldyrevskii and V. D. Zyuzin, "The multiple-start connections method as a tool for enhancing information security in peer-to-peer VPNs," *Engineer's Bulletin of the Don*, no. 12 (120), pp. 240–252, 2024.

[16] P. B. Boldyrevskii and V. D. Zyuzin, "Development of combinatorial models for estimating the number of permissible routes in peer-to-peer networks using the initiator and recipient as intermediate nodes," *Economics and Quality of Communication Systems*, no. 1 (35), pp. 76–84, 2025.

[17] V. D. Zyuzin and N. A. Bashmurov, "Formalising the calculation of scenario counts in the multiple-start connections algorithm using combinatorics," *Information Security Issues*, no. 1, pp. 19–25, 2025.

[18] G. Pólya, "Combinatorial enumeration for groups, graphs and chemical compounds," *Acta Mathematica*, vol. 68, pp. 145–254, 1937.