CYBER-THREAT PROPAGATION OVER NETWORK-SLICING ARCHITECTURES

Michele Cirillo, Mario Di Mauro, Vincenzo Matta, Giuseppe Basileo

Department of Information and Electrical Engineering and Applied Mathematics (DIEM)
University of Salerno (Italy)

ABSTRACT

This work deals with cyber-threat propagation across a communication network designed according to the *network-slicing* paradigm. Exploiting the multi-dimensional Birth-Death-Immigration model, we examine threat percolation from a vulnerable slice to a virtually secured slice. The analysis quantifies the role played by slice-coupling on threat propagation, revealing how cross-slice attacks can be particularly dangerous in applications where the attacker opens a door in some slice relative, e.g., to ordinary services, breaking through into a slice that delivers critical services such as healthcare or financial services.

***Index Terms*—** Network slicing, threat propagation, Birth-Death-Immigration model.

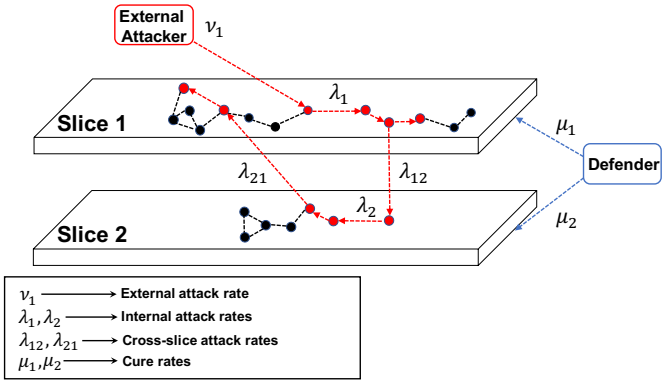


Fig. 1: Intra-slice and inter-slice propagation mechanisms.

1. INTRODUCTION AND RELATED WORK

The Network Function Virtualization (NFV) and Software Defined Networking (SDN) paradigms define the so-called *network softwarization*, a process based on the idea of decoupling the network infrastructure (e.g., physical equipments) from its logical counterpart (e.g., software-based functionalities). In particular, logical networks *sharing a common physical infrastructure* are referred to as *network slices*. Often, a network slice can be identified with a particular network domain (e.g., Automotive, IoT, Mobile Broadband) which provides its service independently from other slices. In principle, slices are logically isolated, but cross-slice communication is permitted to increase network flexibility and allow for dynamic service composition [1–4]. On the other hand, cross-slice communication poses new security challenges since a threat could propagate from a slice to another [5].

Several useful works addressed threat propagation over modern network architectures such as networks of IoT devices or 5G communication networks. In [6], variants of the classic SIR (Susceptible-Infected-Recovered) model were adopted to characterize the epidemic behavior of modern IoT threats, such as the real-world malware named Mirai. Percolation theory was applied in [7] to model malware propagation over large-scale IoT networks. In [8], a dynamic virus propagation model named IDEPSR was proposed to characterize propagation effects of novel threats in a smart-city scenario. A common feature of these works is that the attack involves an isolated network, and no interaction with other networks (i.e., slices) is considered. In comparison, existing works on cross-network interactions mainly focus on specific filtering rules (e.g., access control, confidentiality, authentication, security policies) to prevent threat migration between distinct networks [9, 10]. Recently, attacks to network slices were considered in [11], with reference to a Distributed-Denial-of-Service attack aimed at damaging a mobile network.

However, none of the aforementioned works characterizes the threat *propagation dynamics* over network-slicing architectures, which are instead critical to design and allocate proper countermeasures. This problem is addressed in the present work, where we exploit the elegant Birth-Death-Immigration (BDI) model conceived by Kendall in [12] to study the growth of populations. The BDI model has been recently shown to be useful to predict the propagation dynamics of scanning cyber-threats [13], and to devise optimized (in a game-theoretic sense) allocation of countermeasures [14]. In order to model cross-slice interactions, in this model we call upon a *multi-dimensional* variant of Kendall's BDI model, originally proposed in [15] in the context of genetics to account for various genotypes in a population.

2. MODEL

The considered scenario is illustrated in Fig. 1. We have two network slices. Slice 1 is a *vulnerable* slice that offers standard-users' services to exposed devices, such as IoT or mobile devices. Slice 2 is a *well-protected* slice designed to deliver critical services, such as healthcare or financial services. We assume that slice 1 is attacked by a cyber-threat, injected by an attacker with an *external* rate ν_1. The threat can: i) propagate within slice 1 by compromising some network nodes, which become in turn *secondary* attack sources sustaining an *internal* rate λ_1; ii) percolate into slice 2 according to a cascade effect, with a *cross-slice* rate λ_{12}, further triggering a new propagation process into slice 2 sustained by an internal attack rate λ_2. Depending on the application scenario, feedback from 2 to 1 is permitted, namely, nodes within slice 2 can compromise nodes within slice 1 with a further cross-slice rate λ_{21}. To counteract the threat propagation, it is reasonable to assume that the network administrator could deliver suitable countermeasures (e.g., security patches, antiviruses). Formally, we assume that the compromised nodes of slices 1 and 2 recover at cure rates μ_1 and μ_2, respectively.

2.1. Multi-Dimensional BDI Model

Let us consider S slices of a network architecture. For $s = 1, 2, \ldots, S$, the number of compromised nodes within slice s at time t is denoted by $N_s(t)$. We assume that at time $t = 0$ the system is in a safe state, namely, $N_s(t) = 0$ for all s. Under a multi-dimensional BDI model, the propagation mechanism sketched in the previous section (readily generalized to S slices) assumes that both "birth" (new compromised node) and "death" (cured node) events are ruled by independent exponential random variables. These assumptions give rise to a continuous-time Markov process that can be conveniently described as follows. First, let us consider the vector obtained by stacking the compromised nodes within slice s, denoted by $N_s(t)$, into the vector (we use boldface letters for vectors and matrices) $\boldsymbol{N}(t) = [N_1(t), N_2(t), \ldots, N_S(t)]^\top$. Given that the system is in state $\boldsymbol{N}(t) = \boldsymbol{n} = [n_1, n_2, \ldots, n_S]^\top$, the overall attack rate $\bar{\lambda}_s(\boldsymbol{n})$ and cure rate $\bar{\mu}_s(\boldsymbol{n})$ relative to slice s, and originating from the compromised nodes, are given by:

$$\bar{\lambda}_s(\boldsymbol{n}) = \nu_s + \lambda_s n_s + \sum_{k \neq s}^{S} \lambda_{ks} n_k, \qquad \bar{\mu}_s(\boldsymbol{n}) = \mu_s n_s, \quad (1)$$

where ν_s is the external attack rate perceived within slice s; λ_s is the internal attack rate sustained by one node in slice s; λ_{ks} is the cross-slice rate sustained by one node in slice k to attack slice s; and μ_s is the cure rate relative to slice s. Now, given state $\boldsymbol{n}$ at time t, the subsequent event can be either the successful attack or recovery of a single node within a single slice, namely, the admissible transitions are $\boldsymbol{n} \mapsto \boldsymbol{n} + \boldsymbol{u}_s$ or $\boldsymbol{n} \mapsto \boldsymbol{n} - \boldsymbol{u}_s$, where $\boldsymbol{u}_s$ is the S-dimensional vector with all zero entries but for the s-th entry that is equal to 1. Letting $p(\boldsymbol{n}; t) = \mathbb{P}[\boldsymbol{N}(t) = \boldsymbol{n}]$ be the probability that the system is in state n at time t, from the aforementioned generative mechanism we can derive the pertinent Chapman-Kolmogorov forward equations [15]:

$$\begin{aligned} \frac{dp(\boldsymbol{n}; t)}{dt} &= \sum_{s=1}^{S} \bar{\lambda}_s(\boldsymbol{n} - \boldsymbol{u}_s)\, p(\boldsymbol{n} - \boldsymbol{u}_s; t) \\ &+ \sum_{s=1}^{S} \bar{\mu}_s(\boldsymbol{n} + \boldsymbol{u}_s)\, p(\boldsymbol{n} + \boldsymbol{u}_s; t) \\ &- \sum_{s=1}^{S} \big(\bar{\lambda}_s(\boldsymbol{n}) + \bar{\mu}_s(\boldsymbol{n})\big) p(\boldsymbol{n}; t). \end{aligned} \quad (2)$$

Detailed knowledge of $p(\boldsymbol{n}; t)$ would be useful to characterize the propagation mechanism and, hence, to provide a quantitative assessment of the necessary countermeasures. Unfortunately, no analytical method is currently available to retrieve $p(\boldsymbol{n}; t)$ from (2) under general assumptions [15]. Working in the moment-generating-function domain, differential equations involving moments of $\boldsymbol{N}(t)$ can be derived, albeit the derivation is cumbersome, and obtaining manageable closed-form solutions and relative insights is generally hard. Nevertheless, we will show in the forthcoming analysis that useful insights on the main factors and trade-offs governing threat propagation under the setting described in Fig. 1, can be obtained by means of a first-order analysis that focuses on the expected number of compromised nodes:

$$E_s(t) = \mathbb{E}[N_s(t)], \quad \boldsymbol{E}(t) = \mathbb{E}[\boldsymbol{N}(t)], \quad (3)$$

which can be shown to evolve according to the following system of differential equations [15]:

$$\frac{d\boldsymbol{E}(t)}{dt} = (\boldsymbol{\Lambda} - \boldsymbol{M})^\top \boldsymbol{E}(t) + \boldsymbol{\nu}, \quad (4)$$

where $\boldsymbol{\nu} = [\nu_1, \nu_2, \ldots, \nu_S]^\top$ and:

$$\boldsymbol{\Lambda} = \begin{pmatrix} \lambda_1 & \cdots & \lambda_{1S} \\ \vdots & \ddots & \vdots \\ \lambda_{S1} & \cdots & \lambda_S \end{pmatrix}, \qquad \boldsymbol{M} \triangleq \begin{pmatrix} \mu_1 & & 0 \\ & \ddots & \\ 0 & & \mu_S \end{pmatrix}. \quad (5)$$

3. MAIN RESULT

In the BDI formalism, the setting of Fig. 1 corresponds to $\nu_2 = 0$ (since slice 2 does not experience an external attack) and $\lambda_{12} > 0$ (since attacks within slice 1 reverberate into slice 2). Backpropagation can be present or not (i.e., $\lambda_{21} \geq 0$).

Proposition 1 (Number of Compromised Nodes)**.** *Let $\nu_2 = 0$ and $\lambda_{12} > 0$, and consider the definitions in Table 1. If*

$$\delta_1 \neq \delta_2 \quad \text{or} \quad \lambda_{21} \neq 0, \quad (6)$$

Excess Rates	$\delta_1 = \lambda_1 - \mu_1, \qquad \delta_2 = \lambda_2 - \mu_2$
Error Exponents	$\phi^{\pm} = \frac{\delta_1 + \delta_2}{2} \pm \sqrt{\left(\frac{\delta_1 - \delta_2}{2}\right)^2 + \lambda_{12}\lambda_{21}}$
Propagation Modes	$f^{\pm}(t) = \frac{e^{\phi^{\pm} t} - 1}{2\,\phi^{\pm}}$

Table 1: Useful quantities employed in Proposition 1.

the expected numbers of compromised nodes within slices 1 *and* 2 *are, respectively:*[1]

$$\begin{aligned} E_1(t) &= \nu_1 \left(1 + \frac{\frac{\delta_1-\delta_2}{2}}{\sqrt{\left(\frac{\delta_1-\delta_2}{2}\right)^2 + \lambda_{12}\lambda_{21}}}\right) f^+(t) \\ &\quad + \nu_1 \left(1 - \frac{\frac{\delta_1-\delta_2}{2}}{\sqrt{\left(\frac{\delta_1-\delta_2}{2}\right)^2 + \lambda_{12}\lambda_{21}}}\right) f^-(t), \qquad (7) \\ E_2(t) &= \frac{\lambda_{12}\nu_1}{\sqrt{\left(\frac{\delta_1-\delta_2}{2}\right)^2 + \lambda_{12}\lambda_{21}}} \left[f^+(t) - f^-(t)\right]. \end{aligned}$$

If

$$\delta_1 = \delta_2 = \delta \quad \text{and} \quad \lambda_{21} = 0, \qquad (8)$$

we have:

$$E_1(t) = \frac{\nu_1}{\delta} e^{\delta t} - \frac{\nu_1}{\delta}, \;\; E_2(t) = \lambda_{12}\nu_1 \frac{e^{\delta t}}{\delta^2}(\delta t - 1) + \frac{\lambda_{12}\nu_1}{\delta^2}. \qquad (9)$$

Sketch of proof. The system in (4) can be solved by standard tools from differential calculus. The solution is a superposition of exponential modes of propagation, whose exponents are determined by the eigenvalues ϕ^+ and ϕ^- of the matrix:

$$\boldsymbol{\Lambda} - \boldsymbol{M} = \begin{pmatrix} \lambda_1 - \mu_1 & \lambda_{12} \\ \lambda_{21} & \lambda_2 - \mu_2 \end{pmatrix}. \qquad (10)$$

The different results in (7) and (9) arise because under condition (6) matrix $\boldsymbol{\Lambda} - \boldsymbol{M}$ is diagonalizable, whereas under (8) it is not. The proof is omitted for space constraints. □

The result in Proposition 1 is useful to capture the factors influencing the attack propagation and to devise proper countermeasures. To this end, we will now focus on two application settings that are relevant in the network slicing context. In particular, we will focus on (7), since (8) appears as a special case that is expected to be less frequent in practice.

[1]When $\phi^{\pm} = 0$, the formulas in (7) are intended to hold with $f^{\pm}(t) = \lim_{\phi^{\pm}\to 0}(e^{\phi^{\pm} t} - 1)/\phi^{\pm} = t$. Likewise, the case $\delta = 0$ in (9) is handled by letting $\delta \to 0$ to get $E_1(t) = \nu_1 t$ and $E_2(t) = \lambda_{12}\,\nu_1\, t^2/2$.

3.1. One-way Propagation

In one-way slice-crossing, a door could have been opened from slice 1 to slice 2 without backpropagation from 2 to 1. This corresponds to apply (7) with $\lambda_{21} = 0$, yielding:

$$\begin{aligned} &\phi^+ = \max(\delta_1, \delta_2), \;\; \phi^- = \min(\delta_1, \delta_2), \\ &E_1(t) = \frac{\nu_1}{\delta_1} e^{\delta_1 t} - \frac{\nu_1}{\delta_1}, \\ &E_2(t) = \frac{\lambda_{12}\nu_1}{|\delta_1 - \delta_2|}\left(\frac{e^{\phi^+ t}}{\phi^+} - \frac{e^{\phi^- t}}{\phi^-}\right) + \frac{\lambda_{12}\nu_1}{\delta_1\delta_2}. \end{aligned} \qquad (11)$$

First of all, we observe that, as it must be, the behavior of $E_1(t)$ is determined solely by what happens within slice 1, due to the absence of feedback from slice 2. Furthermore, we see from (11) that different propagation regimes may arise, depending on the amount of cures in the two slices, relative to the internal attack rates. In other words, the relevant parameters to ascertain the propagation regime are δ_1 and δ_2.

If at least one of the slices is not internally protected, namely, if either δ_1 or δ_2 are positive, then slice 2 undergoes an *exponential* propagation, with rate determined by the maximum (i.e., worst-case) exponent between δ_1 and δ_2. For example, assume that the defender mitigates well the attack in slice 1 but not in slice 2, i.e., that $\delta_1 < 0$ and $\delta_2 > 0$ — see Fig. 2a. In this case from (11) we get, for sufficiently large t:

$$E_1(t) \approx \frac{\nu_1}{|\delta_1|}, \qquad E_2(t) \approx \underbrace{\frac{\lambda_{12}\nu_1}{\delta_2 + |\delta_1|}}_{\nu_2'} \frac{e^{\delta_2 t}}{\delta_2}. \qquad (12)$$

It can be readily checked that the evolution of $E_2(t)$ in (12) has the form of a classical one-dimensional Kendall model with immigration rate ν_2'. Notably, we see that such equivalent rate ν_2' is smaller than the steady-state value of $E_1(t)$ multiplied by the transfer rate λ_{12}. This is because $E_1(t)$ starts from 0 and converges monotonically to the steady-state value $\nu_1/|\delta_1|$, implying that during the entire evolution slice 2 sees, on average, an external rate smaller than $\nu_1/|\delta_1|$.

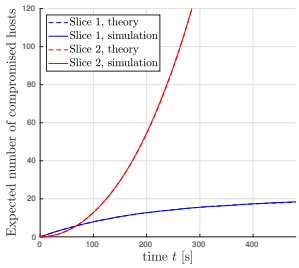
On the other hand, in practice it is more likely that resources will be available to secure a slice delivering a critical service, which corresponds to the reverse scenario where $\delta_1 > 0$ and $\delta_2 < 0$ — see Fig. 2b. Specializing (11) to the latter setting, we have that:

$$E_1(t) \approx \frac{\nu_1 e^{\delta_1 t}}{\delta_1}, \qquad E_2(t) \approx \frac{\lambda_{12}}{\delta_1 + |\delta_2|} \frac{\nu_1 e^{\delta_1 t}}{\delta_1}, \qquad (13)$$

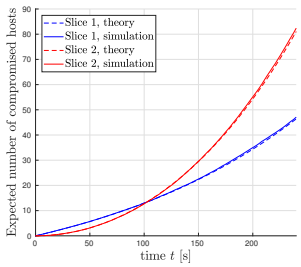
showing that the exponential propagation taking place within slice 1 due to insufficient protection, reverberates into slice 2 through a transfer factor $\lambda_{12}/(\delta_1 + |\delta_2|)$.

Finally, when both slices are individually well-protected ($\delta_1 < 0$ and $\delta_2 < 0$, see Fig. 2c), Eq. (11) yields:

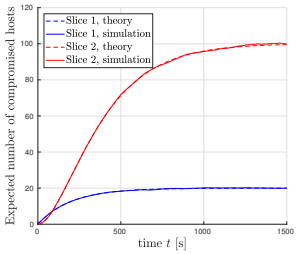
$$E_1(t) \approx \frac{\nu_1}{|\delta_1|}, \qquad E_2(t) \approx \frac{\lambda_{12}\nu_1}{\delta_1\delta_2} = \underbrace{\lambda_{12}\frac{\nu_1}{|\delta_1|}}_{\nu_2'} \frac{1}{|\delta_2|}, \qquad (14)$$



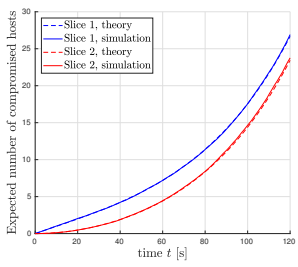
(a) One-way propagation. $\delta_1 = -\delta_2 = -0.005$.



(b) One-way propagation. $\delta_1 = -\delta_2 = 0.005$.



(c) One-way propagation. $\delta_1 = \delta_2 = -0.005$.



(d) Strong mutual coupling. $\delta_1 = \delta_2 = -0.005, \lambda_{21} = 0.025$.

Fig. 2: For all cases we set $\nu_1 = 0.1$ and $\lambda_{12} = 0.025$, and the simulation values are estimated over 10^4 Monte Carlo runs.

revealing that, in this case, slice 2 reaches the same steady-state as a one-dimensional Kendall model, triggered by an equivalent rate ν_2' that is given by the steady-state number of nodes $\nu_1/|\delta_1|$ compromised within slice 1, multiplied by the transfer rate λ_{12}. We notice that the propagation is stabilized, but never annihilated since the external driving rate ν_1 keeps propagation always alive within slice 1 and, hence, within slice 2 through the transfer rate λ_{12}.

The bottom line is that, under one-way propagation: i) knowledge of the inner parameters λ_1 and λ_2 of the individual slices is sufficient for the network administrator to determine the amount of resources necessary to stabilize the threat; and ii) an attack starting from a slice that is internally exposed ($\delta_1 > 0$) can induce *exponential propagation* within a slice that is internally secured ($\delta_2 < 0$), implying that the network administrator should be able to secure also the former to protect the latter.

3.2. Strong Mutual Coupling

We now address the case that both slices are individually secured ($\delta_1 < 0$ and $\delta_2 < 0$) but there is strong coupling between them — see Fig. 2d. Technically, under this setting we assume that:

$$\sqrt{\lambda_{12}\lambda_{21}} \gg \frac{|\delta_1 + \delta_2|}{2}, \tag{15}$$

namely, the geometric average of the mutual rates is much larger that the arithmetic average of the excess of self-rates. Exploiting (7), we see that under condition (15) the dominant exponent becomes:

$$\phi^+ \approx \sqrt{\lambda_{12}\lambda_{21}}, \tag{16}$$

showing that, when the coupling between the slices is mutual (i.e., bidirectional) and sufficiently strong, protection of the individual slices might not be sufficient to avoid exponential spread of the attack within the slices. What matters is the combined effect induced by coupling. From a quantitative perspective, the network administrator should control the maximal exponent ϕ^+ in Table 1. As compared to the curing capacity necessary to combat the attack rates λ_1 and λ_2, a larger amount of cures is necessary to face the additional rate $\sqrt{\lambda_{12}\lambda_{21}}$ determined by mutual coupling. This introduces a significant challenge that was absent in the one-way propagation scenario, since in practice the mutual rates λ_{12} and λ_{21} are seldom known, as they do not depend on intrinsic characteristics of the individual slices known at the design stage. In contrast, they may arise *during the attack*, as the result of a specific operational condition strictly related to the nature of the attack itself. For example, given the event that a shared hardware resource is compromised from slice 1, a certain coupling is induced between the two slices, which was absent before the event. Thus, the network administrator is not in the position to estimate λ_{12} and λ_{21} beforehand, and, hence, to estimate the excess of cures to be allocated.

4. CONCLUSION

We exploited a multi-dimensional variant of Kendall's birth-death-immigration model to examine the propagation of malicious threats across network-slicing architectures. The analysis led to the following main conclusions. If a threat percolates from a vulnerable slice (e.g., offering ordinary services) into a well-protected slice (e.g., offering critical services such as healthcare services), resources must be invested to protect carefully *both* slices. However, in practice resources are typically not enough to protect every type of network service, especially during zero-day attacks, where one must accept periods where the network is exposed to unprecedented threats. Therefore, software-based security solutions must be complemented with architectural solutions aimed at i) protecting as much as possible cross-slice interactions; and ii) guaranteeing slice isolation if an ongoing attack is detected. A certain *hardware redundancy* should be carefully planned such that, when a vulnerable slice damages a shared resource, the latter must be isolated and the other slices must be suddenly reallocated to a backup resource.

5. REFERENCES

[1] L. Cominardi, T. Deiss, M. Filippou, V. Sciancalepore, F. Giust, and D. Sabella, "MEC support for network slicing: Status and limitations from a standardization viewpoint," *IEEE Communications Standards Magazine*, vol. 4, no. 2, pp. 22–30, 2020.

[2] L. Suarez, D. Espes, F. Cuppens, C T. Phan, and P. Le Parc, "Managing secure inter-slice communication in 5G network slice chains," in *Data and Applications Security and Privacy*, LNCS, vol. 12122, pp. 24–41, 2020.

[3] B. Bordel, R. Alcarria, D. Sánchez-de-Rivera, and Á. Sánchez, "An inter-slice management solution for future virtualization-based 5G systems," in *Advanced Information Networking and Applications.* Springer, Cham., vol. 926, pp. 1059–1070, 2019.

[4] 5G-MoNArch (EU Proj.). Available online: https://5g-monarch.eu/wp-content/uploads/2019/05/5G-MoNArch_761445_D2.3_Final_overall_architecture_v1.0.pdf.

[5] The Evolution of Security in 5G - White Paper. Available online: https://www.5gamericas.org/wp-content/uploads/2019/08/5G-Security-White-Paper_8.15.pdf.

[6] A. Mahboubi, S. Camtepe, and K. Ansari, "Stochastic modeling of IoT botnet spread: A short survey on mobile malware spread modeling," *IEEE Access*, vol. 8, pp. 228818–228830, 2020.

[7] A. Zhaikhan, M. A. Kishk, H. El Sawy, and M. S. Alouini, "Safeguarding the IoT from malware epidemics: A percolation theory approach," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 6039–6052, 2021.

[8] H. Xia, L. Li, X. Cheng, C. Liu, and T. Qiu, "A dynamic virus propagation model based on social attributes in city IoT," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8036–8048, 2020.

[9] R. F. Olimid and G. Nencioni, "5G network slicing: A security overview," *IEEE Access*, vol. 8, pp. 99999–100009, 2020.

[10] V. L. Nguyen, P. C. Lin, B. C. Cheng, R. H. Hwang, and Y. D. Lin, "Security and privacy for 6G: A survey on prospective technologies and challenges," *IEEE Communications Surveys & Tutorials*, 2021.

[11] V. N. Sathi and C. S. R. Murthy, "Distributed slice mobility attack: A novel targeted attack against network slices of 5G networks," *IEEE Networking Letters*, vol. 3, no. 1, pp. 5–9, 2021.

[12] D. G. Kendall, "On some modes of population growth leading to R. A. Fisher's logarithmic series distribution," *Biometrika*, vol. 35, no. 1/2, pp. 6–15,1948.

[13] V. Matta, M. Di Mauro, M. Longo, and A. Farina, "Cyber-Threat mitigation exploiting the birth-death-immigration model," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 12, pp. 3137–3152, 2018.

[14] P. Addesso, M. Barni, M. Di Mauro, and V. Matta, "Adversarial Kendall's model towards containment of distributed cyber-threats," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3604–3619, 2021.

[15] J. Mode, "Some multi-dimensional birth and death processes and their applications in population genetics," *Biometrics*, vol. 18, no. 4, pp. 543–567, 1962.