Description of Lateral Movement Using Absorbing Markov Chains

1st Smieško Juraj
Faculty of Management Science and Informatics
University of Zilina
Zilina, Slovakia
juraj.smiesko@fri.uniza.sk

2nd Smiešková Monika
Faculty of Management Science and Informatics
University of Zilina
Zilina, Slovakia
monika.smieskova@fri.uniza.sk

***Abstract*—The paper presents a basic description of lateral movement progression using absorbing Markov chains. The states of the chain represent observable phases of an attack, while the compromise of a critical system and attack detection are modeled as absorbing states. The advanced mathematical framework of absorbing Markov chains is applied to modeling the progression of lateral movement. Finally, the proposed approach is demonstrated on an eight-state state space. The paper reflects current research activities at the department and extends the content of the Information Systems Theory course.**

***Index Terms*—first-order Markov chain, absorption probability, fundamental matrix, lateral movement, Windows Event Log**

I. Introduction

One of the tasks of a university department is to integrate teaching with current scientific research and to transfer knowledge from both basic and applied research into specialized courses. In this way, students acquire knowledge reflecting current developments in information and communication technologies and their practical applications.

Current research focuses on the analysis and modeling of advanced cyberattacks, particularly lateral movement. Since lateral movement has a sequential nature, it is well suited for modeling using Markov chains, and two basic approaches can be applied to its detection.

The first approach is based on modeling normal network traffic and subsequently evaluating deviations from typical sequences of states and transitions. The second approach directly models lateral movement, with states and transitions representing individual steps taken by the attacker.

This paper focuses on the second approach, namely describing the progression of lateral movement using absorbing Markov chains. The transient states of the chain represent individual phases of lateral movement, while the absorbing states represent either system compromise or the detection and termination of the attack.

II. Related Work

Markov chains are widely used in anomaly and intrusion detection to model sequential user behavior by representing observed activities as discrete states and estimating transition probabilities from historical data.

Ju [1] used a higher-order Markov model to profile users based on UNIX command sequences. Tian et al. [2] applied a homogeneous Markov chain to system-call sequences, where low-probability sequences were treated as potential anomalies. Pei et al. [3] proposed HERCULE, a graph-based approach for reconstructing attack scenarios from correlated system logs using community discovery. Tynymbayev [4] employed a Hidden Markov Model within UEBA using real SIEM data containing authentication, process, registry, and network events. These studies demonstrate the suitability of Markov models for identifying deviations from normal system behavior.

III. Stochastic Process, Random Chain, and Markov Property

A stochastic process is defined as a system of random variables

$$\{X(\omega, t)\}_{\omega\in\Omega,;t\in T}, \tag{1}$$

where Ω represents the sample space of elementary events and T the set of time instants. In technical applications, the abbreviated notation $\{X(t)\}_{t\in T}$ is commonly used.

If we consider discrete time $T = \{0, 1, 2, \ldots\}$ and the process has a state space $S = \{s_1, s_2, \ldots, s_m\}$, we refer to it as a discrete-time *random chain*.

A random chain is a Markov chain if

$$\begin{aligned} &P(X_{n+1} = s_j \mid X_n = s_i, X_{n-1}, \ldots, X_0) \\ &\quad = P(X_{n+1} = s_j \mid X_n = s_i). \end{aligned} \tag{2}$$

The one-step transition probabilities

$$p_{ij} = P(X_{n+1} = s_j \mid X_n = s_i) \tag{3}$$

form a stochastic matrix

$$\mathbf{P} = p_{ij}, \qquad p_{ij} \geq 0, \qquad \sum_j p_{ij} = 1. \tag{4}$$

For a homogeneous Markov chain, the transition probabilities are time-invariant. The transition probabilities over n steps are contained in the matrix $\mathbf{P}^n$:

$$\mathbf{P}^n = p_{ij}(n), \qquad p_{ij}(n) \geq 0, \qquad \sum_j p_{ij}(n) = 1. \tag{5}$$

A more detailed analysis of Markov chains can be found in [5], [6] and [7].

IV. Classification of Markov Chain States

When analyzing a Markov chain, it is important not only to determine the probabilities of transitions, but also to characterize the relationships between the states. This classification is particularly important when modeling sequential processes.

A state s_j is called *reachable* from state s_i if there exists at least one $n \geq 0$ such that

$$\exists\, n \geq 0, \quad p_{i,j}(n) > 0, \qquad s_i \to s_j \tag{6}$$

Reachability therefore means that there exists at least one sequence of transitions through which the process can move from state i to state j.

In the context of lateral movement, for example, state s_i may represent network reconnaissance and state s_j the acquisition of administrative access. Reachability between these two states then means that there is a non-zero probability that the attacker can move from the network reconnaissance phase, through one or more intermediate phases, to the administrative access phase.

Let the chain be in state s_i at time 0. $X(t_0) = s_i$. We define the first return time to this state as

$$T_i = \min\{n \geq 1 : X(t_n) = i\}, \tag{7}$$

The probability that the process ever returns to state i is

$$f_{i,i} = P(T_i < \infty \mid X(t_0) = i). \tag{8}$$

According to the value of $f_{i,i}$, the states of the chain are classified as *transient* and *recurrent*.

A state i is called a *transient state* if $f_{i,i} < 1$. This means that there is a non-zero probability that, after leaving state i, the process will never return to this state.

In the lateral movement progression model, the transient states represent individual phases of an ongoing attack. These may include, for example:

- network reconnaissance and discovery of available devices,
- acquisition or misuse of authentication credentials,
- remote authentication,
- establishment of an administrative session,
- privilege escalation.

The process may repeatedly move between some of these phases, but there is a non-zero probability that, after leaving a particular phase, it will never return to it and the progression will continue toward one of the final outcomes.

A state s_i is called *recurrent* if $f_{i,i} = 1$. In this case, if the process starts in state s_i, it returns to this state in finite time with probability one.

Recurrent states can be further classified according to the expected first return time as positive and null recurrent.

A state s_i is called *positive recurrent* if $E(T_i) < \infty$, and *null recurrent* if $E(T_i) = \infty$.

A state s_i is called absorbing if, once reached, the process cannot leave this state: $p_{i,i}(1) = 1$.

When modeling the progression of lateral movement, it is appropriate to interpret absorbing states as the final outcomes of the observed trajectory. In the following, we will consider two such outcomes:

$$S_C = \text{compromise of a critical system}$$

$$S_D = \text{detection and termination of the attack.}$$

It should be emphasized that whether a particular security state is considered absorbing depends on the objective of the specific model. For example, obtaining administrative privileges does not necessarily constitute an absorbing state if the attacker can subsequently continue lateral movement toward a critical system. A state becomes absorbing only when the corresponding outcome is considered final within the defined model.

The above classification makes it possible to naturally divide the state space of the lateral movement model into two basic groups.

The first group consists of *transient states*, which represent individual phases of the attacker's progression. Repeated transitions, returns, or remaining in the current state may occur among these states.

The second group consists of *absorbing states*, which represent the final outcome of the observed process. Once such a state is reached, no further progression is considered within the given model.

V. Absorbing Markov Chain

A Markov chain is called *absorbing* if it contains at least one absorbing state and if at least one absorbing state can be reached from every non-absorbing state. In a standard absorbing Markov chain, the process reaches one of the absorbing states after a finite number of steps with probability one and remains in that state thereafter.

A. Transition Probability Matrix

After an appropriate ordering of the states, the transition matrix of an absorbing Markov chain can be written in block form as

$$\mathbf{P} = \begin{pmatrix} \mathbf{Q} & \mathbf{R} \\ \mathbf{0} & \mathbf{I} \end{pmatrix}, \tag{9}$$

- $\mathbf{Q}$ is the matrix of transition probabilities between transient states,
- $\mathbf{R}$ contains the transition probabilities from transient states to absorbing states,
- $\mathbf{0}$ is the zero matrix,
- $\mathbf{I}$ is the identity matrix corresponding to the absorbing states.

If the chain contains t transient states and r absorbing states, then the matrix $\mathbf{Q}$ has dimensions $t \times t$, the matrix $\mathbf{R}$ has dimensions $t \times r$, and the overall matrix $\mathbf{P}$ has dimensions $(t + r) \times (t + r)$.

In the description of lateral movement, the matrix $\mathbf{Q}$ describes transitions between the individual phases of an attack that is still in progress. Its element Q_{ij} expresses the

probability that the progression moves from transient state s_i to transient state s_j.

The matrix $\mathbf{R}$ describes transitions by which the observed progression terminates. For example, if two absorbing states represent the compromise of a critical system and the detection of the attack, the individual columns of the matrix $\mathbf{R}$ contain the probabilities of immediate transition to these two outcomes. The block $\mathbf{0}$ expresses that, after reaching an absorbing state, the process does not return to the transient phases within the model. The identity matrix $\mathbf{I}$ represents remaining in the reached absorbing state.

B. Fundamental Matrix

Let us assume that the random variable N_j represents the number of visits to the transient state s_j before absorption. It can be expressed as the sum

$$N_j = I_0 + I_1 + I_2 + \cdots , \tag{10}$$

where I_k is a Bernoulli indicator of the Markov chain being in state s_j at time t_k. The expected value of the indicator is

$$\mathbb{E}[I_k] = 0.P(X(t_k) \neq s_j) + 1.P(X(t_k) = s_j) \tag{11}$$

By the linearity of expectation, we then obtain

$$\mathbb{E}[N_j] = \sum_{k=0}^{\infty} \mathbb{E}[I_k] = \sum_{k=0}^{\infty} P(X(t_k) = s_j). \tag{12}$$

In the context of lateral movement, N_j may represent, for example, the number of occurrences of the credential acquisition phase, remote authentication, or administrative activity before the attack ends in compromise or detection. Thus, the model does not need to assume that the attacker passes through each phase only once. Some activities may occur repeatedly.

If the chain is in the transient state s_i at time t_0, then the probability that it is in the transient state s_j after k steps is

$$P(X(t_k) = s_j \mid X(t_0) = s_i) = (\mathbf{Q}^k)_{ij}. \tag{13}$$

The element $(\mathbf{Q}^k)_{ij}$ therefore represents the probability that the process starting in state s_i will be in state s_j after k steps and that absorption has not yet occurred during these steps.

The expected number of visits to state s_j, provided that the chain was in state s_i at time t_0, is denoted by n_{ij}:

$$n_{i,j} = \mathbb{E}[N_j \mid X(t_0) = s_i] = \sum_{k=0}^{\infty} (\mathbf{Q}^k)_{ij}. \tag{14}$$

Expanding the series gives:

$$n_{ij} = \delta_{ij} + (\mathbf{Q})_{ij} + (\mathbf{Q}^2)_{ij} + \cdots , \tag{15}$$

where δ_{ij} is the Kronecker delta.

The matrix of expected visits n_{ij} is called the fundamental matrix of the Markov chain and is denoted by $\mathbf{N}$:

$$\mathbf{N} = \{n_{ij}\} = \mathbf{N} = \mathbf{I} + \mathbf{Q} + \mathbf{Q}^2 + \mathbf{Q}^3 + \cdots . \tag{16}$$

This is a matrix geometric series which, due to the properties of the Markov chain, converges, [8], and the fundamental matrix can be expressed in closed form as

$$\mathbf{N} = (\mathbf{I} - \mathbf{Q})^{-1}. \tag{17}$$

In the description of lateral movement, n_{ij} can be used to quantify how many times, on average, an attack starting from a given phase reaches another selected phase before it terminates. Higher values may indicate phases that recur during the progression, for example, repeated authentication attempts or repeated credential acquisition.

C. Expected Number of Steps to Absorption

Using the fundamental matrix, the expected number of steps required to reach one of the absorbing states can be determined.

Let $\mathbf{1}$ be a column vector of ones. Define

$$\mathbf{t} = \mathbf{N1} \quad \Longrightarrow \quad t_i = \sum_{\forall j} n_{ij}. \tag{18}$$

The value t_i represents the expected number of steps to absorption, assuming that the process starts in the transient state s_i.

In the lateral movement model, t_i can be interpreted as the expected number of additional transitions between attack phases remaining until the observed trajectory terminates. Such termination may correspond, for example, to the compromise of a critical system or to the detection and termination of the attack.

If the value of t_i is high, a longer subsequent progression can be expected from the given state. Conversely, a low value of t_i means that the process is, on average, closer to one of the final outcomes.

It is important to distinguish between the number of steps and physical time. If individual steps of the Markov chain represent security events or changes in attack phases, the value t_i does not directly represent time in seconds or minutes, but rather the expected number of additional state transitions.

D. Matrix of Absorption Probabilities

In addition to the expected number of steps to absorption, it is also possible to determine the probability that the process terminates in each of the absorbing states.

$$\mathbf{B} = \mathbf{NR}. \tag{19}$$

The element b_{ij} represents the probability that a process starting in the transient state s_i will eventually be absorbed in the j-th absorbing state.

Substituting the definition of the fundamental matrix gives

$$\mathbf{B} = \mathbf{NR} = (\mathbf{I} + \mathbf{Q} + \mathbf{Q}^2 + \cdots)\mathbf{R} = \\ = \mathbf{R} + \mathbf{QR} + \mathbf{Q}^2\mathbf{R} + \cdots . \tag{20}$$

The element R_{ij} represents the probability of a transition from the transient state s_i directly to the j-th absorbing state in the next step.

Analogously, the element $(\mathbf{Q}^k\mathbf{R})_{ij}$ represents the probability that the process performs k transitions between transient states and subsequently moves to the j-th absorbing state.

$$b_{ij} = \sum_{k=0}^{\infty} (\mathbf{Q}^k\mathbf{R})_{ij}. \tag{21}$$

The value b_{ij} therefore accounts for all possible trajectory lengths through which the process can reach the corresponding absorbing state from state s_i.

In the lateral movement model, we consider two absorbing states, s_C - system compromise and s_D - attack detection. For any transient state s_i, we can determine the probabilities

$$b_{iC} = P(X = s_C \mid X(t_0) = s_i) \tag{22}$$

$$b_{iD} = P(X = s_D \mid X(t_0) = s_i). \tag{23}$$

The matrix $\mathbf{B}$ therefore provides directly interpretable information about the further evolution of the observed progression. For each current phase, it is possible to determine the probability that the observed trajectory will lead to the compromise of a critical system and the probability that the attack will be detected and terminated before this outcome occurs.

VI. Methodology for Constructing the Attack Progression Model

The basic idea is to transform a sequence of real security events recorded in system, network, or SIEM logs into a sequence of Markov chain states. The resulting state sequence represents the observed progression of lateral movement and subsequently makes it possible to quantify the probability of its further development.

A. Definition of Target Outcomes

In the proposed model, we consider two absorbing states S_C and S_D. They represent the final outcomes of the observed trajectory, after which no further progression is considered within the model.

State S_C represents the successful achievement of the attacker's objective, for example, access to a domain controller, database server, file server, or another critical asset.

State S_D represents a situation in which the attack progression is detected and subsequently stopped, for example, by means of a SIEM or EDR system, by blocking a user account, terminating a remote session, or isolating a compromised device.

This clearly specifies which probabilities the model is ultimately intended to quantify. For each current transient state, we aim to determine the probability that further progression will lead to the compromise of a critical system or, alternatively, to the detection and termination of the attack.

B. Definition of Transient Phases

Transient states are intended to represent observable phases through which an attacker may progress during lateral movement. When defining these states, it is appropriate to base them on activities that can be identified in real system and network events.

For the purposes of a simple and easily interpretable model, we consider the following states:

TABLE I
States of the Lateral Movement Progression Model

State	Interpretation
S_1	initial compromise of a workstation
S_2	network reconnaissance and discovery of available devices
S_3	acquisition or use of authentication credentials
S_4	remote authentication to another device
S_5	establishment of a remote administrative session
S_6	privilege escalation
S_7	compromise of a critical system
S_8	detection and termination of the attack

States $S_1, \ldots, S_6$ are transient and represent individual phases of the ongoing attack. States S_7 and S_8 are absorbing and represent two possible final outcomes.

Such a representation does not assume that the attacker must pass through all states exactly once. Some phases may be repeated. For example, the attacker may repeatedly perform network reconnaissance, test different accounts, or authenticate to multiple devices. Similarly, the attack may be detected at virtually any phase of its progression.

C. Event Mapping and Construction of State Sequences

The model input consists of real security events obtained, for example, from Windows Event Log, Sysmon, EDR, SIEM, or network monitoring systems.

An observed event is represented as a heterogeneous vector

$$e_k = (t_k, u_k, h_k^{src}, h_k^{dst}, q_k, a_k), \tag{24}$$

- t_k is the time of occurrence of the event,
- u_k is a user or system account,
- h_k^{src} is the source device,
- h_k^{dst} is the destination device,
- q_k represents the event type or identifier,
- a_k contains additional event attributes.

The additional attributes a_k may include the logon type, network port number, process name, the service used, authentication result, or information about assigned privileges, the source IP address, or the destination IP address.

We define a mapping function that assigns a particular security event to the corresponding system state:

$$g(e_k) = S_i, \tag{25}$$

An example of mapping real events is shown in Table II.

TABLE II
EXAMPLE OF MAPPING SECURITY EVENTS TO STATES

State	Examples of Observable Events
S_1	initial compromise of a workstation
S_2	Sysmon Event ID 1, 3, or 22; execution of commands `ping`, `nslookup`, `net`, `nltest`; communication with multiple devices
S_3	Windows Event ID 4648 or 4776; explicit use of credentials or user account authentication
S_4	Windows Event ID 4624; successful remote logon
S_5	RDP, WinRM, SMB, SSH, WMI, or PsExec; establishment of a remote administrative session
S_6	Windows Event ID 4672 or 4688; Sysmon Event ID 1;
S_7	access to a critical server or another protected asset
S_8	SIEM/EDR alert, session blocking, account blocking, or device isolation

A single isolated event does not necessarily indicate lateral movement. For example, a successful remote logon is a common event in an enterprise network. Its security relevance arises primarily in combination with events that preceded or followed it.

For example, the following event sequence (Event ID according to Windows Security Event Log):

$$\texttt{ping} \rightarrow 4648 \rightarrow 4624_{\text{type=10}} \rightarrow 4672 \rightarrow 4688 \tag{26}$$

may indicate the following sequence of activities: network reconnaissance, use of authentication credentials, remote logon, acquisition of privileged permissions, and subsequent process execution. After applying the mapping function $g(.)$, we obtain the state sequence:

$$S_2 \rightarrow S_3 \rightarrow S_4 \rightarrow S_6 \rightarrow S_6. \tag{27}$$

With an appropriately selected mapping, a large number of heterogeneous log events can be reduced to a smaller number of security-interpretable states.

The events must be organized into common sequences based on their logical and temporal relationships, while taking into account event attributes such as the user account, source and destination devices, and the type of activity performed. For each identified incident, a time-ordered sequence of events e_k is thus created and mapped into a state sequence

$$g(e_1, e_2, \ldots, e_n) = (S_{i_1}, S_{i_2}, \ldots, S_{i_n}) \tag{28}$$

1) Successful lateral movement progression

After the initial compromise, the attacker performs network reconnaissance, obtains credentials, logs on to another device, establishes an administrative session, gains elevated privileges, and subsequently reaches the critical system:

$$S_1 \rightarrow S_2 \rightarrow S_3 \rightarrow S_4 \rightarrow S_5 \rightarrow S_6 \rightarrow S_7. \tag{29}$$

2) Unsuccessful progression with early detection

After the initial compromise of the workstation, network reconnaissance is observed, followed by an attempt to use credentials. This sequence of events is evaluated by the security system as suspicious, and the attack is stopped:

$$S_1 \rightarrow S_2 \rightarrow S_3 \rightarrow S_8. \tag{30}$$

3) Unsuccessful progression with late detection

After successful authentication, the attacker establishes an administrative session and performs privileged activity, which is subsequently detected by an EDR or SIEM system:

$$S_1 \rightarrow S_2 \rightarrow S_3 \rightarrow S_4 \rightarrow S_5 \rightarrow S_6 \rightarrow S_8. \tag{31}$$

The examples above show that attack sequences do not have to be of the same length or pass through all transient states. However, each trajectory ultimately leads to one of the defined outcomes of the model.

D. Estimation of the Transition Matrix

After constructing a sufficiently large number of state sequences, the transition probabilities between individual states can be estimated. Let N_{ij} denote the number of observed transitions from state S_i to state S_j. The maximum likelihood estimate of the transition probability p_{ij} is

$$\hat{p}_{ij} = \frac{N_{ij}}{\sum_k N_{ik}}, \qquad \hat{p}_{ij} \geq 0, \qquad \sum_j \hat{p}_{ij} = 1. \tag{32}$$

The transition matrix constructed in this way, $\mathbf{P} = \{\hat{p}_{ij}\}$, no longer describes only a single trajectory, but rather the statistical behavior of the entire set of observed attacks.

VII. ILLUSTRATIVE EXAMPLE

For the eight-state Markov chain defined in Table I, we specify the transition probability matrix $\mathbf{P} = \begin{pmatrix} \mathbf{Q} & \mathbf{R} \\ \mathbf{0} & \mathbf{I} \end{pmatrix} =$

$$= \left(\begin{array}{cccccc|cc} 0.25 & 0.55 & 0 & 0 & 0 & 0 & 0 & 0.20 \\ 0.10 & 0.20 & 0.50 & 0 & 0 & 0 & 0 & 0.20 \\ 0 & 0.10 & 0.20 & 0.50 & 0 & 0 & 0 & 0.20 \\ 0 & 0 & 0.10 & 0.20 & 0.50 & 0 & 0 & 0.20 \\ 0 & 0 & 0 & 0.10 & 0.20 & 0.50 & 0 & 0.20 \\ 0 & 0 & 0 & 0 & 0.10 & 0.15 & 0.55 & 0.20 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right).$$

We calculate the fundamental matrix $\mathbf{N} = (\mathbf{I} - \mathbf{Q})^{-1} =$

$$\begin{pmatrix} 1.4819 & 1.1139 & 0.7611 & 0.5195 & 0.3505 & 0.2062 \\ 0.2025 & 1.5190 & 1.0379 & 0.7084 & 0.4779 & 0.2811 \\ 0.0277 & 0.2076 & 1.5084 & 1.0296 & 0.6946 & 0.4086 \\ 0.0038 & 0.0283 & 0.2059 & 1.5057 & 1.0157 & 0.5975 \\ 0.0005 & 0.0038 & 0.0278 & 0.2031 & 1.4862 & 0.8743 \\ 0.0001 & 0.0004 & 0.0033 & 0.0239 & 0.1749 & 1.2793 \end{pmatrix}.$$

We calculate the expected number of steps to absorption $\mathbf{t}$ and the matrix of absorption probabilities $\mathbf{B}$:

$$\mathbf{t} = \mathbf{N1} = \begin{pmatrix} 4.4331 \\ 4.2269 \\ 3.8764 \\ 3.3569 \\ 2.5958 \\ 1.4819 \end{pmatrix} \qquad \mathbf{B} = \mathbf{NR} = \begin{pmatrix} 0.1134 & 0.8866 \\ 0.1546 & 0.8454 \\ 0.2247 & 0.7753 \\ 0.3286 & 0.6714 \\ 0.4808 & 0.5192 \\ 0.7036 & 0.2964 \end{pmatrix}.$$

If the process is in state S_1, the expected number of steps until termination is 4.43, while the probability of compromise of the critical system is only $11.34\,\%$. In state S_4, the expected number of remaining steps decreases to approximately 3.36, while the probability of compromise increases to $32.86\,\%$.

In the illustrative model, the transition from state S_5 to state S_6 can be considered an important threshold. In state S_5, the probability of compromise is still slightly lower than the probability of detection, namely $48.08\,\%$ compared with $51.92\,\%$. After reaching state S_6, however, this ratio changes substantially. The probability of compromise increases to $70.36\,\%$, while the probability of detection decreases to $29.64\,\%$.

State S_6, representing privilege escalation, therefore appears to be a critical phase in the progression of lateral movement in the considered model. If the attacker reaches this phase, it becomes substantially more likely that the process will end in the compromise of the critical system rather than in detection and termination of the attack.

The results also show that detection is most important in the earlier phases of the progression. While the probability of detection in state S_1 is $88.66\,\%$, it decreases to $29.64\,\%$ in state S_6.

These observations follow from the illustrative transition matrix and therefore cannot be interpreted as general probabilities of a real attack. However, the numerical experiment demonstrates what information can be obtained from an absorbing Markov chain after the model has been calibrated using real data.

VIII. Discussion

The main advantage of the Markov model is its interpretability. The probability of compromise has a direct security interpretation, while the fundamental matrix provides additional information on the expected number of visits to individual phases and on the expected time until the process terminates.

The main limitation is the first-order Markov property. In real attack scenarios, the progression of an attack may depend on a longer history of events as well as on additional attributes. Therefore, future research will focus on extending the proposed approach, for example, by incorporating higher-order Markov models and Hidden Markov Models.

IX. Conclusion

In this paper, we presented a basic approach to the use of absorbing Markov chains for modeling and detecting lateral movement. The theoretical modeling procedure was demonstrated using an illustrative example. The resulting material can also serve as an educational resource suitable for integration into the Information Network Theory course, providing students with an introduction to current research trends pursued at the department.

Markov chains represent only one of several tools suitable for lateral movement detection. Successful detection therefore requires their integration with other mathematical and computational approaches, such as graph-based models, multivariate correlation analysis, and machine learning methods.

Acknowledgment

Co-financed by the European Union through the Slovakia Programme under project No. NFP401101C360: Research and development of advanced artificial intelligence solutions for the detection of cyber threats and defense against sophisticated attacks

References

[1] W.-H. Ju and Y. Vardi, "A Hybrid High-Order Markov Chain Model for Computer Intrusion Detection," *Journal of Computational and Graphical Statistics*, vol. 10, no. 2, pp. 277–295, 2001. doi: 10.1198/10618600152628068.

[2] X. Tian, M. Duan, C. Sun, and W. Li, "Intrusion Detection Based on System Calls and Homogeneous Markov Chains," *Journal of Systems Engineering and Electronics*, vol. 19, no. 3, pp. 598–605, 2008. doi: 10.1016/S1004-4132(08)60126-7.

[3] K. Pei, Z. Gu, B. Saltaformaggio, S. Ma, F. Wang, Z. Zhang, L. Si, X. Zhang, and D. Xu, "HERCULE: Attack Story Reconstruction via Community Discovery on Correlated Log Graph," in *Proceedings of the 32nd Annual Conference on Computer Security Applications (ACSAC 2016)*, pp. 583–595, 2016. doi: 10.1145/2991079.2991122.

[4] B. Tynymbayev, "Applying Hidden Markov Models for User and Entity Behavioural Analytics Model," *Systems and Soft Computing*, vol. 8, p. 200467, 2026. doi: 10.1016/j.sasc.2026.200467.

[5] K. Janková, S. Kilianová, P. Brunovský and P. Bokes, *Markovove reťazce a ich aplikácie*. Bratislava: EPOS, 2015.

[6] J. Kalas, *Markovove reťazce – skriptum*. Bratislava: Polygrafické stredisko UK, 1993.

[7] J. Smieško, *Operačná analýza II. Základy teórie hromadnej obsluhy*. Žilina: MC Energy s.r.o., 1999.

[8] C. M. Grinstead and J. L. Snell, *Introduction to Probability*, 2nd ed., American Mathematical Society, Providence, RI, 1997.

[9] A. Junius, "AnoMark – Anomaly Detection in Command Lines with Markov Chains," *FIRST Conference 2023*, ANSSI – French National Cybersecurity Agency, 2023.

[10] D. P. Bertsekas, R. G. Gallager, *Data Networks*, 2nd ed. Englewood Cliffs, NJ: Prentice Hall, 1992. ISBN 0-13-200916-1.