

## **Applications des automates finis dans la détection des intrusions informatiques : vers une sécurité proactive, une revue systématique (2019–2025).**

**OUEDRAOGO Mohamed**

Le département Intelligence Artificielle, à l'université de Lisala (UNILIS), République démocratique du Congo

### **RESUME**

La multiplication et la sophistication croissante des cyberattaques révèlent les limites des systèmes de détection d'intrusions traditionnels, majoritairement fondés sur des signatures statiques ou des modèles d'apprentissage automatique souvent peu explicables.

L'objectif de cette recherche est de présenter une revue systématique de la littérature portant sur les applications des automates finis dans la détection des intrusions informatiques, en mettant l'accent sur leur contribution à une sécurité proactive.

La méthodologie adoptée suit les recommandations PRISMA et couvre la période 2019–2025. Les recherches menées dans les bases de données IEEE Xplore, SpringerLink, ScienceDirect, ACM Digital Library, ArXiv, MDPI et AJOL ont permis d'identifier 54 articles, dont 10 études primaires retenues après élimination des doublons et application de critères d'inclusion et d'exclusion rigoureux.

Les résultats montrent que 34 % des travaux reposent sur des automates finis déterministes ou des machines à états finis, 33 % sur des modèles non déterministes ou probabilistes, et 33 % sur des approches hybrides combinant automates finis et apprentissage automatique. Les domaines d'application concernent les réseaux d'entreprise (45%), les systèmes critiques ICS/SCADA (22 %) et les environnements SOC (33 %).

Les travaux existants montrent des performances élevées pour la détection et l'anticipation des attaques cyber, avec des taux de détection pouvant atteindre 97 à 99 % selon les approches. Les

**À PARAÎTRE**

méthodes basées sur les automates finis non déterministe se distinguent par leur précision, tandis que les approches déterministes et hybrides permettent de prédire les actions futures de l'attaquant avec des résultats encourageants. Toutefois, des limites subsistent, notamment l'explosion du nombre d'états et la difficulté d'adaptation aux attaques inédites.

En conclusion, les automates finis apparaissent comme un socle formel explicable et robuste, favorisant l'évolution des systèmes de détection d'intrusions vers des architectures de sécurité proactive, complémentaires aux approches statistiques et neuronales.

**Mots-clés :** Automates finis ; Détection d'intrusions ; Sécurité proactive ; Attaques multi-étapes ; Cybersécurité.

**ABSTRACT**

The increasing frequency and sophistication of cyberattacks highlight the limitations of traditional intrusion detection systems, which are mainly based on static signatures or machine learning models that are often difficult to interpret. In this context, finite automata emerge as a relevant formal framework for modeling attack behaviors as sequences and for supporting a more proactive security approach.

The objective of this research is to present a systematic literature review on the applications of finite automata in intrusion detection, with a particular focus on their contribution to proactive security. The adopted methodology follows the PRISMA guidelines and covers the period 2019–2025. Searches conducted in IEEE Xplore, SpringerLink, ScienceDirect, ACM Digital Library, ArXiv, MDPI, and AJOL identified 54 articles, of which 10 primary studies were retained after duplicate removal and the application of rigorous inclusion and exclusion criteria. The results show that 34% of the studies rely on deterministic finite automata or finite-state machines, 33% on nondeterministic or probabilistic models, and 33% on hybrid approaches combining finite automata and machine learning. The main application domains include enterprise networks (45%), critical ICS/SCADA systems (22%), and SOC environments (33%). The reviewed studies report high performance in intrusion detection and attack anticipation, with

**À PARAÎTRE**

detection rates reaching 97–99% depending on the approach. However, several limitations remain, including state-space explosion and difficulties in adapting to previously unseen attacks.

In conclusion, finite automata constitute a robust and explainable formal foundation that supports the evolution of intrusion detection systems toward proactive security architectures, complementing statistical and neural-based approaches.

**Keywords** : Finite automata ; Intrusion detection ; Proactive security ; Multi-step attacks ; Cybersecurity.

---

Soumis le : 14 Mars , 2025

Publié le : 14 Mars, 2025

Auteur correspondant: Ouedraogo Mohamed

Adresse électronique : [ouedamedform@gmail.com](mailto:ouedamedform@gmail.com)

Ce travail est disponible sous la licence

Creative Commons Attribution 4.0 International.



## I. INTRODUCTION

L'évolution rapide du paysage des menaces cyber, caractérisée par la prolifération d'attaques complexes, multi-étapes et persistantes, constitue un défi majeur pour les systèmes de détection d'intrusions contemporains. Ces attaques s'appuient sur des séquences d'actions coordonnées et distribuées dans le temps, qui échappent fréquemment aux mécanismes de détection traditionnels lorsque les événements sont analysés de manière isolée.

Les systèmes de détection d'intrusions (IDS) classiques, qu'ils reposent sur des signatures ou sur des techniques d'apprentissage automatique, présentent des limites structurelles face à cette évolution des menaces. Les approches à signatures sont intrinsèquement incapables de détecter des attaques inédites, tandis que les modèles d'apprentissage automatique, bien que performants dans certains contextes, souffrent de problèmes récurrents de généralisation, de dépendance aux données d'apprentissage et de manque d'explicabilité. Ces limites entravent leur adoption dans des environnements exigeant transparence, audibilité et gouvernance des décisions de sécurité [1] [2]

Dans ce contexte, la littérature scientifique a progressivement réinvesti les modèles formels, et en particulier les automates finis, pour la modélisation et la détection des cyberattaques. Les automates finis offrent une représentation explicite des états et des transitions d'attaque, fournissant ainsi un cadre rigoureux pour la détection séquentielle, l'anticipation de la progression des attaques et, dans certains cas, la prédiction des actions futures de l'attaquant (Ning et al., 2002) [3]. Différentes variantes — déterministes, non déterministes ou probabilistes et hybride — ont été proposées afin de prendre en compte l'incertitude, la variabilité et la complexité des scénarios d'attaque réels.

Au-delà de leurs capacités de détection, les automates finis présentent un avantage déterminant en matière d'explicabilité, en offrant des mécanismes de décision transparents, traçables et interprétables. Cette propriété contraste avec l'opacité de nombreux modèles d'apprentissage

**À PARAÎTRE**

automatique et répond aux exigences croissantes en matière de confiance, de gouvernance et de conformité des systèmes de cybersécurité (Doshi-Velez & Kim, 2017) [4].

Cependant, malgré ces apports, la littérature met également en évidence plusieurs défis majeurs, notamment l'explosion de l'espace d'états, la faible adaptabilité aux attaques inédites ou évolutives, ainsi que le manque d'évaluations approfondies en environnements opérationnels réels [5]. Ces limites soulèvent des interrogations quant à la pertinence, à la scalabilité et à l'applicabilité pratique des approches fondées sur les automates finis face à l'évolution continue des menaces cyber.

Dans ce contexte, cette étude vise à présenter une revue systématique de la littérature, conduite conformément aux recommandations PRISMA, afin d'analyser les applications des automates finis dans la détection des intrusions informatiques. Cette revue couvre la période 2019–2025 et s'appuie sur des recherches menées dans plusieurs bases de données scientifiques reconnues. L'objectif est d'identifier les types d'automates utilisés, leurs domaines d'application, leurs contributions à une sécurité proactive, ainsi que les principales limites et perspectives de recherche mises en évidence par la littérature récente. Ainsi, cette revue s'articule autour de la question de recherche suivante :

Comment les automates finis sont-ils utilisés dans la littérature pour la détection proactive et explicable des attaques multi-étapes, et quelles limites et opportunités émergent des travaux existants ?

**II. État des connaissances actuelles sur le sujet**

Les automates finis constituent un cadre formel fondamental pour la modélisation de comportements séquentiels, permettant de représenter les attaques informatiques comme des suites ordonnées d'événements observables. Dans le contexte de la détection d'intrusions, un automate fini est classiquement défini par un quintuplet [6]

$$A = (Q, \Sigma, \delta, q_0, F),$$

où  $Q$  désigne l'ensemble fini des états,  $\Sigma$  l'alphabet des événements observés,  $\delta$  la fonction de transition,  $q_0$  l'état initial et  $F \subseteq Q$  l'ensemble des états acceptants correspondant à des comportements malveillants ou anormaux.

## À PARAÎTRE

Dans le cas d'un automate fini déterministe (AFD), la fonction de transition est définie par

$$\delta: Q \times \Sigma \rightarrow Q,$$

ce qui garantit une évolution unique du système pour chaque couple état–événement. Cette propriété confère aux AFD une exécution stable, prévisible et interprétable, particulièrement adaptée aux environnements temps réel et aux systèmes de détection nécessitant une traçabilité claire des décisions.

À l'inverse, un automate fini non déterministe (AFN) conserve la même structure formelle, mais sa fonction de transition est définie par

$$\delta: Q \times \Sigma \rightarrow 2^Q,$$

où  $2^Q$  présente l'ensemble des parties de  $Q$ . Cette formulation permet à l'automate d'évoluer vers plusieurs états possibles pour une même observation, traduisant la capacité du modèle à représenter des trajectoires d'attaque multiples ou ambiguës. Dans certains cas, des transitions silencieuses  $\varepsilon$  peuvent être introduites, étendant la fonction de transition à

$$\delta: Q \times (\Sigma \cup \{\varepsilon\}) \rightarrow 2^Q,$$

afin de modéliser des changements d'état implicites.

Appliqués à la détection des intrusions, ces modèles permettent d'identifier non seulement des états finaux correspondant à des attaques avérées, mais également des états intermédiaires de suspicion, ouvrant la voie à des mécanismes de sécurité proactive. Par leur explicabilité intrinsèque et leur capacité à modéliser des séquences d'actions, les automates finis constituent ainsi un socle théorique robuste et complémentaire aux approches statistiques et neuronales pour la conception des systèmes de détection d'intrusions de nouvelle génération.

L'automate hybride combine la structure formelle des automates finis avec des techniques d'apprentissage automatique. Il conserve un espace d'états explicite et interprétable (par exemple :  $q_0 \rightarrow q_1 \rightarrow q_2$ , représentant normal, suspect et intrusion), garantissant une modélisation claire des comportements.

La particularité de cette approche réside dans l'intégration d'un module ML/DL qui calcule un score de risque à partir des données observées. Ce score influence dynamiquement les transitions via une fonction paramétrée :

$$\delta_{\theta}(q,a)=\begin{cases} q' & \text{si } f_{\theta}(q,a) \geq \tau \\ q & \text{sinon} \end{cases}$$

où  $f_{\theta}(q,a)$  est une fonction de scoring issue d'un modèle d'apprentissage paramétré par  $\theta$  (appris à partir des données), et  $\tau$  un seuil adaptatif.

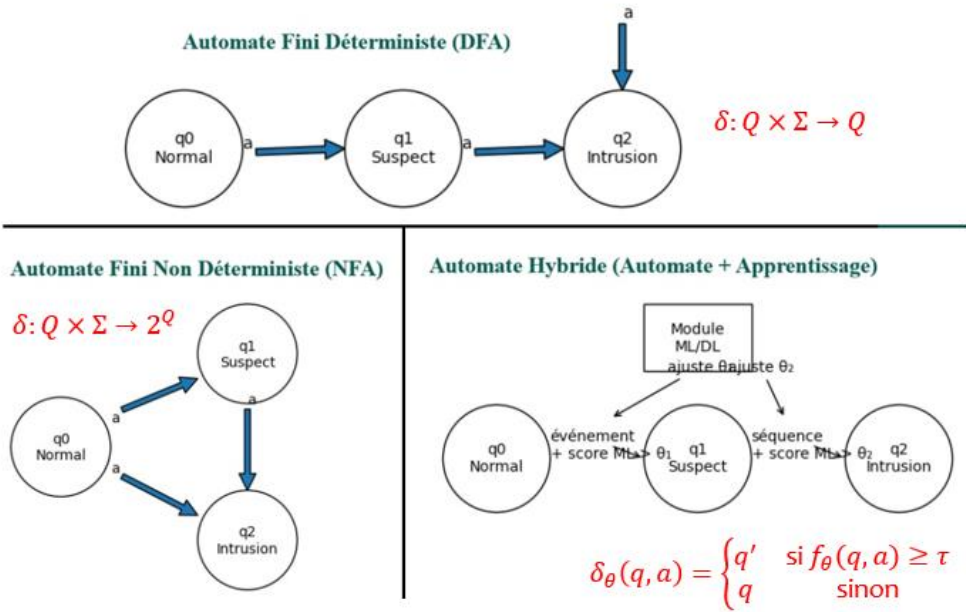


Figure 1: Les trois variétés d'automates finis  
**Source :** personnelle

Tableau 1 : Tableau comparatif des automates finis (IDS)

| Critère                  | Automate fini déterministe (DFA)         | Automate fini non déterministe (NFA)       | Automate hybride (Automate + ML)                  |
|--------------------------|------------------------------------------|--------------------------------------------|---------------------------------------------------|
| Définition formelle      | $\delta : Q \times \Sigma \rightarrow Q$ | $\delta : Q \times \Sigma \rightarrow 2^Q$ | $\delta_{\theta} : Q \times \Sigma \rightarrow Q$ |
| Transitions              | Une seule transition par événement       | Plusieurs transitions possibles            | Une seule transition dépendante d'un score appris |
| Trajectoire d'exécution  | Unique                                   | Multiple (parallèle)                       | Unique mais paramétrée                            |
| Gestion de l'incertitude | Faible                                   | Élevée                                     | Élevée + adaptative                               |
| Complexité théorique     | $O(n)$                                   | Potentiellement exponentielle              | Dépend du modèle ML                               |
| Interprétabilité         | Très forte                               | Forte                                      | Moyenne à forte                                   |

**À PARAÎTRE**

| Adaptabilité aux attaques nouvelles | Limitée                        | Moyenne                   | Élevée                                |
|-------------------------------------|--------------------------------|---------------------------|---------------------------------------|
| Usage typique en IDS                | Détection séquentielle stricte | Modélisation multi-étapes | Détection proactive et adaptative     |
| Avantage principal                  | Stabilité et simplicité        | Expressivité              | Compromis explicabilité / performance |
| Limite principale                   | Rigidité                       | Explosion d'états         | Complexité et dépendance aux données  |

***Source :** Synthèse de l'auteur à partir des études primaires incluses*

### III. Méthodologie

#### III.1. Critères d'éligibilité

Ont été incluses les études publiées entre 2019 et 2025, évaluées par les pairs, rédigées en anglais ou en français, et portant explicitement sur l'utilisation des automates finis, machines à états finis ou modèles apparentés pour la détection des intrusions informatiques. Les études devaient présenter une application concrète en cybersécurité et rapporter des résultats expérimentaux mesurables. Ont été exclues les études hors période, purement théoriques, sans lien direct avec les IDS, les doublons, ainsi que les publications ne fournissant pas d'indicateurs de performance exploitables.

#### III.2. Sources d'information

Les recherches ont été conduites dans les bases de données scientifiques internationales suivantes : IEEE Xplore, SpringerLink, ScienceDirect (Elsevier), ACM Digital Library, arXiv (Computer Science), MDPI, AJOL, HAL et Academia.

#### III.3. Stratégie de recherche

La stratégie de recherche a été définie de manière systématique en combinant des mots-clés relatifs aux automates finis et à la détection des intrusions. Les termes principaux utilisés incluent : *"finite automata"*, *"finite state machine"*, *"deterministic finite automata"*, *"non-deterministic finite automata"*, *"intrusion detection"*, *"intrusion detection system"*, *"IDS"*, *"network security"*, *"attack detection"*, *"behavioral detection"* et *"multi-step attacks"*.

## À PARAÎTRE

Ces mots-clés ont été combinés à l'aide d'opérateurs booléens selon des requêtes de type : ("finite automata" OR "finite state machine" OR "FSM") AND ("intrusion detection" OR "IDS" OR "attack detection").

Des filtres temporels (2019–2025) et disciplinaires (informatique, cybersécurité, intelligence artificielle) ont été appliqués afin de restreindre les résultats aux études pertinentes.

### III.4 Processus de sélection

Le processus de sélection a suivi les étapes recommandées par PRISMA 2020 : identification initiale des articles, suppression des doublons, criblage des titres et résumés, puis évaluation des textes intégraux pour déterminer l'éligibilité finale, tel qu'illustré dans le diagramme PRISMA.

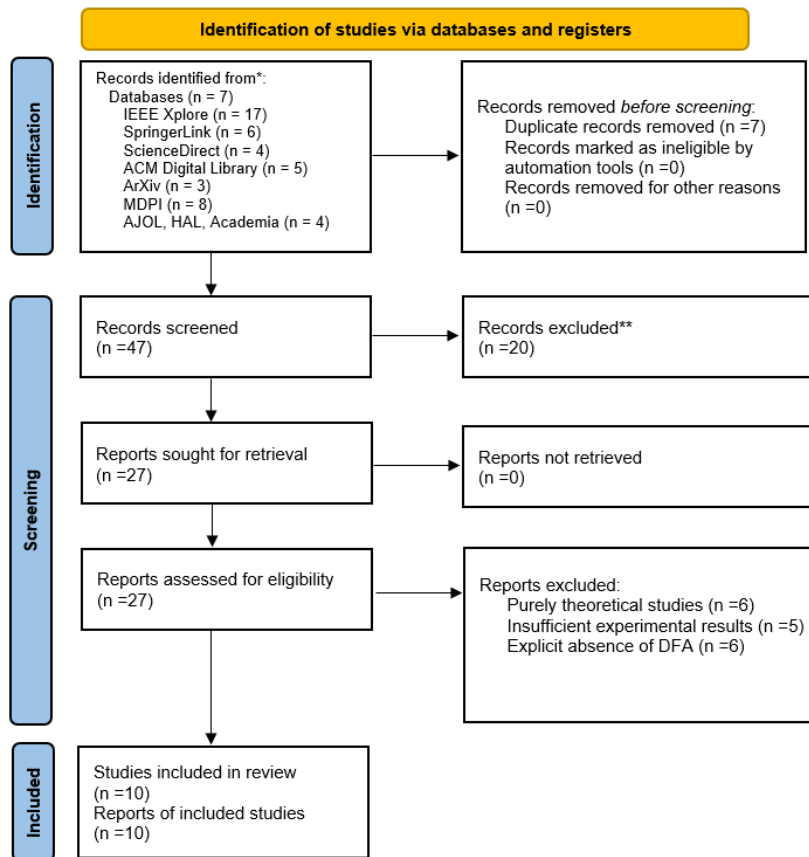


Figure 2 : PRISMA 2020 flow diagram of the literature selection process (2019–2025)

**Source** : Elaboration de l'Auteur selon les recommandations PRISMA 2020

III.5 Processus de collecte des données

Les données ont été collectées de manière standardisée à partir des études retenues à l’aide d’un tableau de synthèse, garantissant l’homogénéité et la comparabilité des informations extraites. Les éléments extraits comprennent le type d’automate utilisé, le domaine d’application, le type d’attaque ciblée, les jeux de données employés, les méthodes de comparaison, les indicateurs de performance et les principaux résultats rapportés.

IV. PRINCIPAUX RÉSULTATS DE LA RECHERCHE

IV.1 Sélection des études

La recherche documentaire a permis d’identifier 54 articles issus des bases de données sélectionnées. Après suppression de 7 doublons, 47 articles ont été examinés lors du criblage des titres et résumés. À cette étape, 20 articles ont été exclus. Les 27 articles restants ont été évalués en texte intégral. Parmi ceux-ci, 17 articles ont été exclus après lecture complète. Au total, 10 études primaires ont été incluses dans la revue systématique. Le processus de sélection est présenté dans le diagramme PRISMA 2020 (figure 3).

IV.2 Caractéristiques des études

Les 10 études incluses ont été publiées entre 2019 et 2025. Les domaines d’application identifiés portent sur les réseaux d’entreprise (45%), les systèmes industriels critiques ICS/SCADA (22 %) et les environnements SOC (33 %). Concernant les modèles utilisés, 34 % emploient des automates finis déterministes, 33% utilisent des automates non déterministes ou probabilistes, et 33 % reposent sur des approches hybrides. Les types d’attaques étudiés incluent les scans réseau, les attaques par force brute, les attaques multi-étapes et les intrusions persistantes avancées.

Tableau 1: Etudes incluses par type de modèle d’automates finis

| Rubrique | Thème | Auteurs | Titre / Référence | Commentaire (résultats) | Lacunes / Défis |
|----------|-------|---------|-------------------|-------------------------|-----------------|
|----------|-------|---------|-------------------|-------------------------|-----------------|

À PARAÎTRE

|                                                  |                                              |                                |                                                                                                                         |                                                                                                                                                                     |                                                                                                             |
|--------------------------------------------------|----------------------------------------------|--------------------------------|-------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| <b>Automates finis déterministes (DFA)</b>       | Détection multi-étapes par séquences         | S. Prithi, S. Sumathi          | <i>An Intrusion Detection System Based on Finite State Automaton</i> [6]                                                | Les attaques sont modélisées par des états et transitions déterministes, permettant la détection d'intrusions complexes par suivi séquentiel des événements réseau. | Dépendance aux scénarios prédéfinis ; difficulté face aux attaques inconnues ; explosion du nombre d'états. |
|                                                  | Détection précoce d'attaques                 | Jalindar Karande, Sarang Joshi | <i>DEDA: An Algorithm for Early Detection of Attacks</i> [7]                                                            | La reconnaissance de préfixes de séquences d'événements permet de déclencher une alerte avant la phase finale de l'attaque.                                         | Dépendance aux seuils ; absence de mécanisme d'adaptation automatique.                                      |
|                                                  | Détection d'attaques séquentielles et mixtes | Fu-I Chou et al.               | <i>Detecting Mixed-Type Intrusion in High Adaptability Using Artificial Immune System and Parallelized Automata</i> [8] | Les automates finis parallélisés détectent efficacement des attaques hétérogènes et séquentielles, avec un taux de détection supérieur à 95 %.                      | Explosion du nombre d'états ; apprentissage essentiellement hors ligne.                                     |
|                                                  | Détection haut débit                         | Laurens Le Jeune et al.        | <i>SoK – Network Intrusion Detection on FPGA</i> [9]                                                                    | Les IDS matériels exploitent des automates finis déterministes pour assurer une détection rapide et déterministe à débit filaire.                                   | Flexibilité limitée ; coûts de conception matériels élevés.                                                 |
| <b>Modèles non déterministes / probabilistes</b> | Tolérance aux intrusions                     | Fengquan Li                    | <i>A Markov-Based Intrusion Tolerance Finite Automaton</i> [10]                                                         | L'automate fini probabiliste à transitions markoviennes permet d'adapter l'état de sécurité du système face aux intrusions. Avec un taux de détection de 99 %       | Estimation complexe des probabilités ; hypothèses markoviennes restrictives.                                |
|                                                  | Anticipation des actions de l'attaquant      | Ion Băbălău et al.             | <i>Forecasting Attacker Actions using Alert-Driven Attack Graphs</i> [11]                                               | Le modèle rSPDFA prédit les actions futures de l'attaquant ; Top-3 accuracy de 67,27 % (+57,17 %).                                                                  | Dépendance aux données historiques ; complexité computationnelle.                                           |
|                                                  | Analyse comportementale adaptative           | Gaetano Pellegrino             | <i>Learning Automata for Network Behaviour Analysis</i> [12]                                                            | Les comportements réseau sont modélisés par des automates probabilistes dont les transitions sont ajustées dynamiquement par apprentissage.                         | Validation surtout théorique ; déploiement IDS non détaillé.                                                |

À PARAÎTRE

|                                                       |                                        |                           |                                                                                                                         |                                                                                                                                                                            |                                                                           |
|-------------------------------------------------------|----------------------------------------|---------------------------|-------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
|                                                       | Reconstruction de scénarios d'attaque  | Azqa Nadeem et al.        | <i>SAGE: Intrusion Alert-Driven Attack Graph Extractor [13]</i>                                                         | Les graphes d'attaque représentent plusieurs chemins d'intrusion possibles à partir d'alertes IDS corrélées. Avec 35,67 % de détection des éléments critiques de l'attaque | Absence de probabilités explicites ; dépendance à la qualité des alertes. |
| <b>Approches hybrides (automates + apprentissage)</b> | Détection adaptative d'attaques mixtes | Fu-I Chou et al.          | <i>Detecting Mixed-Type Intrusion in High Adaptability Using Artificial Immune System and Parallelized Automata [8]</i> | L'intégration d'un système immunitaire artificiel améliore l'adaptation des automates finis face aux attaques complexes.                                                   | Complexité du modèle ; coût computationnel.                               |
|                                                       | Détection d'attaques multi-étapes      | Mohammad Almseidin et al. | <i>Fuzzy Automaton as a Detection Mechanism for the Multi-Step Attack [14]</i>                                          | L'automate flou permet de gérer l'incertitude dans la progression des attaques multi-étapes. Avec taux de détection de 97,836 %                                            | Calibration empirique des règles floues ; passage à l'échelle limité.     |
|                                                       | Sécurité proactive adaptative          | Gaetano Pellegrino        | <i>Learning Automata Network Behaviour Analysis [12]</i>                                                                | Les transitions probabilistes sont ajustées par apprentissage, permettant une adaptation progressive du modèle aux comportements observés.                                 | Scalabilité et déploiement temps réel non évalués.                        |
|                                                       | Anticipation proactive des attaques    | Ion Băbălău et al.        | <i>Forecasting Attacker Actions using Alert-Driven Attack Graphs [11]</i>                                               | L'apprentissage statistique des transitions permet d'anticiper les prochaines actions de l'attaquant et d'orienter la défense proactive.                                   | Besoin de données d'apprentissage représentatives ; complexité du modèle. |

**Source :** Synthèse de l'auteur à partir des études primaires incluses

### IV.3 Risque de biais dans les études

L'évaluation du risque de biais a été réalisée de manière qualitative à l'aide d'une grille simple, adaptée aux études méthodologiques en cybersécurité. Quatre critères ont été considérés : la clarté de l'objectif, la description du modèle proposé, la méthodologie d'évaluation et la cohérence des résultats. Chaque étude a été classée selon un niveau de risque de biais faible ou modéré. Aucun biais critique n'a été identifié justifiant l'exclusion d'une étude incluse.

#### IV.4 Résultats des études individuelles

Une étude utilisant un automate flou pour la détection d'attaques DDoS multi-étapes rapporte une accuracy globale de 97,836 % [14]. Un modèle probabiliste rSPDFA, appliqué à la prédiction des actions futures de l'attaquant à partir de séquences d'alertes, atteint une Top-3 accuracy moyenne de 67,27 % [11], avec une amélioration de 57,17 % [11] par rapport aux méthodes de référence évaluées. Sur le jeu de données CPTC-2018, une méthode de corrélation et d'extraction guidée par alertes permet d'identifier, dans le meilleur cas, 28 sommets sur 70, soit 40 % d'alertes de sécurité critiques, avec une moyenne pondérée de 35,67 % de détection des éléments critiques de l'attaque [13]. Une approche citée dans une revue fondée sur un modèle de type Markov rapporte un taux de détection de 99 % [10].

#### IV.5 Résultats des synthèses

Les études retenues rapportent des accuracies allant jusqu'à 97,836 % [14] pour la détection d'attaques multi-étapes basées sur des automates flous. Les approches probabilistes orientées anticipation atteignent une Top-3 accuracy de 67,27 % pour la prédiction des actions futures de l'attaquant [11]. Les méthodes de corrélation d'alertes appliquées au jeu CPTC-2018 permettent d'identifier jusqu'à 40 % des sommets classés sévères, avec une moyenne pondérée de 35,67 % [13]. Les modèles probabilistes de type Markov rapportés dans la littérature présentent des taux de détection pouvant atteindre 99 % [10].

### V. DISCUSSION DES PRINCIPAUX RÉSULTATS

#### V.1 Analyse critique des approches fondées sur les automates finis

L'analyse des études retenues met en évidence une diversité d'approches reposant sur les automates finis, principalement réparties entre modèles déterministes, non déterministes/probabilistes et hybrides. Les approches déterministes se distinguent par leur simplicité, leur faible coût computationnel et leur forte explicabilité, ce qui facilite leur compréhension et leur adoption dans des contextes opérationnels. Toutefois, leur dépendance à des scénarios d'attaque prédéfinis limite leur capacité à détecter des attaques évolutives ou inédites.

À l'inverse, les approches non déterministes et probabilistes offrent une meilleure flexibilité dans la modélisation des comportements d'attaque, en intégrant l'incertitude et la variabilité des

**À PARAÎTRE**

séquences d'événements. Ces modèles présentent généralement de meilleures performances de détection, avec des taux d'accuracy et de recall élevés, en particulier pour les attaques multi-étapes complexes. Néanmoins, cette amélioration s'accompagne souvent d'une augmentation significative de la complexité, rendant leur maintenance et leur déploiement plus délicats.

Les approches hybrides, combinant automates finis et techniques d'apprentissage automatique, apparaissent comme une piste prometteuse pour concilier performance, adaptabilité et explicabilité. Toutefois, leur mise en œuvre reste hétérogène dans la littérature, et les critères d'évaluation ne sont pas toujours uniformes, ce qui complique les comparaisons directes entre études.

**V.2 Lacunes de la littérature**

La revue met en évidence plusieurs lacunes majeures dans les travaux existants. Tout d'abord, la majorité des études sont évaluées sur des jeux de données simulés ou contrôlés, avec une faible représentation des environnements opérationnels réels, tels que les SOC, les institutions financières ou les contextes à ressources limitées, notamment en Afrique. Cette limitation réduit la généralisabilité des résultats.

Par ailleurs, le problème de l'explosion de l'espace d'états demeure un défi central, en particulier pour les modèles non déterministes et probabilistes. Cette complexité croissante impacte la scalabilité des solutions et limite leur applicabilité dans des systèmes à grande échelle.

Enfin, de nombreuses approches présentent une faible capacité d'adaptation aux attaques inédites, car elles reposent sur des modèles ou des scénarios d'attaque construits a priori. Cette dépendance limite leur efficacité face à des attaquants adaptatifs et à l'évolution rapide des Tactiques, Techniques et Procédures (TTP).

**V.3 Perspectives de recherche**

Les constats issus de cette revue ouvrent plusieurs perspectives de recherche. Une première orientation concerne l'hybridation des automates finis avec des approches d'intelligence artificielle explicable, afin de renforcer l'adaptabilité des modèles tout en conservant leur caractère interprétable. Cette combinaison pourrait permettre de pallier les limites liées aux attaques inconnues tout en répondant aux exigences de gouvernance et de transparence.

**À PARAÎTRE**

Une seconde perspective porte sur l'évaluation des approches en environnements contraints et réels, notamment dans des SOC opérationnels, des infrastructures critiques ou des institutions financières en contexte africain. Ces contextes offrent des cas d'usage encore peu explorés et essentiels pour valider la robustesse et la pertinence pratique des modèles proposés.

Enfin, ces perspectives constituent une base solide pour des travaux de recherche futurs, notamment dans le cadre de thèses ou d'articles scientifiques, visant à proposer des modèles de référence, des cadres méthodologiques unifiés et des protocoles d'évaluation standardisés pour les systèmes de détection d'intrusions basés sur les automates finis.

**VI. CONCLUSION**

Cette revue systématique, couvrant la période 2019–2025, a analysé l'utilisation des automates finis dans la détection des intrusions informatiques. Les résultats montrent que ces modèles constituent un cadre formel efficace pour représenter les attaques séquentielles et améliorer les performances des systèmes de détection, notamment par une détection plus précoce des comportements malveillants, favorisant ainsi une sécurité proactive.

Les travaux examinés mettent en évidence la prédominance des automates finis déterministes dans les environnements temps réel, l'intérêt des modèles non déterministes et probabilistes dans les contextes incertains, ainsi que le potentiel des approches hybrides combinant automates finis et apprentissage automatique. Toutefois, des limites subsistent, en particulier la complexité des modèles, leur scalabilité et leur adaptation aux attaques émergentes.

En perspective, l'optimisation et la minimisation des automates, leur intégration dans des architectures hybrides explicables et leur validation en conditions opérationnelles réelles constituent des axes de recherche prioritaires pour la conception des systèmes de détection d'intrusions de nouvelle génération.

**VII. REFERENCES BIBLIOGRAPHIQUES**

- [1] N. SFETCU, "Les menaces persistantes avancées en cybersécurité – La guerre cybernétique," 2024.
- [2] R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," 2010.

- [3] P. Ning, Y. Cui, and D. S. Reeves, “Constructing attack scenarios through correlation of intrusion alerts,” *Association for Computing Machinery (ACM)*, Nov. 2002, pp. 245–254. doi: 10.1145/586110.586144.
- [4] F. Doshi-Velez and B. Kim, “Towards A Rigorous Science of Interpretable Machine Learning,” Mar. 2017, [Online]. Available: <http://arxiv.org/abs/1702.08608>
- [5] O. Assi and H. Hermann, “Journal of Business and Technologies Exploration des langages formels et des automates, fondamentaux pour la compréhension des systèmes informatiques et des compilateurs,” 2025, [Online]. Available: [www.jobt.org](http://www.jobt.org)
- [6] S. Prithi and S. Sumathi, “A technical research survey on bio-inspired intelligent optimization grouping algorithms for finite state automata in intrusion detection system,” *International Journal of Engineering, Science and Technology*, vol. 16, no. 2, pp. 48–67, May 2024, doi: 10.4314/ijest.v16i2.6.
- [7] J. Karande and S. Joshi, “DEDA: An algorithm for early detection of topology attacks in the internet of things,” *International Journal of Electrical and Computer Engineering*, vol. 11, no. 2, pp. 1761–1770, Apr. 2021, doi: 10.11591/ijece.v11i2.pp1761-1770.
- [8] F. I. Chou, W. H. Ho, Y. J. Chen, J. T. Tsai, and C. W. Chang, “Detecting mixed-type intrusion in high adaptability using artificial immune system and parallelized automata,” *Applied Sciences (Switzerland)*, vol. 10, no. 5, Mar. 2020, doi: 10.3390/app10051566.
- [9] L. Le Jeune, A. Sateesan, M. Rabbani, T. Goedemé, J. Vliegen, and N. Mentens, “SoK-Network Intrusion Detection on FPGA.” [Online]. Available: <https://suricata.io/>
- [10] F. Li, “A Markov-Based Intrusion Tolerance Finite Automaton,” *Journal of Computing and Information Technology*, vol. 28, no. 2, pp. 89–100, 2020, doi: 10.20532/cit.2020.1005178.
- [11] I. Băbălău and A. Nadeem, “Forecasting Attacker Actions using Alert-driven Attack Graphs,” 2018. doi: XXXXXXXX.XXXXXXX.
- [12] G. Pellegrino, “Learning Automata for Network Behaviour Analysis”, doi: 10.4233/uuid:6ea4a13b-ff8e-4c4b-866d-168cdccd880a.

- [13] A. Nadeem, S. Verwer, and S. J. Yang, “SAGE: Intrusion Alert-driven Attack Graph Extractor,” Oct. 2021, [Online]. Available: <http://arxiv.org/abs/2107.02783>
- [14] M. Almseidin, I. P. #2, M. Al-Kasassbeh, and S. Kovacs, “Fuzzy Automaton as a Detection Mechanism for the Multi-Step Attack,” vol. 9, no. 2, 2019.