Un processus décisionnel d'authentification multi-agent basé sur la confiance pour l'Internet des objets

Marc Saideh, Jean-Paul Jamont, Laurent Vercouter

Un processus décisionnel d'authentification multi-agent basé sur la confiance pour l'Internet des objets

Marc Saideh[a] marc.saideh@insa-rouen.fr
Jean-Paul Jamont[b] jean-paul.jamont@univ-grenoble-alpes.fr
Laurent Vercouter[a] laurent.vercouter@insa-rouen.fr

[a]INSA Rouen Normandie, Normandie Univ, LITIS UR 4108, 76000 Rouen, France

[b]LCIS, Univ. Grenoble Alpes, 26000 Valence, France

Résumé

De nombreuses applications de l'Internet des Objets reposent sur des environnements ouverts et dynamiques composés d'objets hétérogènes. Lors du déploiement d'un système multi-agent dans ce type d'environnement, les agents sont amenés à interagir avec de nouveaux agents et à exploiter les informations et les services qu'ils offrent. Ces interactions et les dépendances qui en découlent introduisent une vulnérabilité face à des comportements malveillants et nécessitent l'usage d'un système de gestion de confiance pour s'en protéger. Les modèles multi-agents de gestion de la confiance reposent sur des observations du comportement des autres agents qui doivent être identifiés. Or, les systèmes d'authentification traditionnels présentent des limites importantes lorsqu'il faut prendre en compte les contraintes matérielles d'un Internet des Objets. Cet article propose un nouveau processus décisionnel adaptatif d'authentification multi-agents basé sur la confiance. Il permet de prendre des décisions d'authentification en fonction du contexte et du niveau de confiance accordé à l'agent à authentifier. Notre proposition aide ainsi à trouver un compromis entre l'utilisation des ressources allouées à l'authentification et la sécurité.

Mots-clés : *Systèmes Multi-Agents, Internet des Objets, Authentification, Confiance, Sécurité*

Abstract

Many applications of the Internet of Things rely on open and dynamic environments composed of heterogeneous objects. When deploying a multi-agent system in such an environment, the agents are led to interact with new agents and to leverage the information and services they offer. These interactions and the resulting dependencies introduce a vulnerability to malicious behaviors and necessitate the use of trust management systems for protection. Multi-agent trust-management models are based on observations of the behavior of other agents who must be identified. However, traditional authentication systems have significant limitations when it comes to accommodating the hardware constraints of the Internet of Things. This article proposes a new adaptive multi-agent trust-based authentication decision-making process. It allows making authentication decisions based on the context and the level of trust assigned to the agent being authenticated. Our proposal thus helps to find a tradeoff between the use of resources allocated for authentication and security.

Keywords: *Multi-Agent Systems, Internet of Things, Authentication, Trust, Security*

1 Introduction

Le déploiement de Systèmes Multi-Agents (SMA) dans le contexte de l'Internet des Objets (IoT) implique des agents qui soient capables d'agir de façon autonome malgré des ressources limitées et une connaissance partielle de leur environnement. Ces contraintes, induisent nécessairement une dépendance des agents vis à vis des services et ressources proposées par les autres agents pour atteindre leurs objectifs. L'incertitude quant à la fiabilité des autres agents, qui peuvent ne pas suivre le même ensemble de règles et directives ou agir de manière malhonnête, complexifie la prise de décision d'un agent en situation de dépendance. Ce constat souligne l'importance de l'évaluation de la confiance et de la prise en compte des risques liés à l'interaction avec d'autres agents.

Une relation de confiance implique deux rôles : le *truster*, l'agent qui dépend d'un autre agent pour un service ou une information, et le *trustee*, l'agent fournissant le service au *truster*. La confiance en elle même correspond alors à la

croyance que le *truster* a en la capacité, la compétence ou l'intention du *trustee* d'agir d'une manière profitable au *truster* [12, 17]. Dans notre contexte d'étude, les systèmes de gestion de la confiance s'imposent comme des composants essentiels pour assurer la coopération, le partage d'informations et la prise de décision. En effet, les agents bénéficiant d'un tel système privilégient les interactions avec les agents en qui ils ont confiance, et peuvent détecter puis isoler les agents ayant un comportement malveillant.

Un agent *truster* devant prendre une décision qui dépend des informations fournies par un agent *trustee* s'appuie sur la confiance qu'il accorde à l'identité revendiquée par ce dernier. De ce fait, la relation de confiance établie est vulnérable aux attaques d'authentification, surtout dans les cas où un agent malveillant parvient à usurper l'identité d'un agent digne de confiance. L'authentification assure que la communication se déroule entre des agents dont l'identité est certifiée, et que seuls les agents autorisés accèdent aux services et aux données, maintenant l'intégrité et la confidentialité du système.

Si l'authentification permet en effet de s'assurer de l'identité des agents en interaction, cette solution se confronte à plusieurs défis majeurs lorsqu'il s'agit de l'appliquer dans les environnements IoT. En effet, les environnements IoT impliquent des interactions entre des appareils aux caractéristiques très hétérogènes : depuis les appareils informatiques à haute puissance jusqu'aux capteurs à faible puissance fonctionnant sous de strictes contraintes d'énergie, de coût et de temps. Le système doit alors permettre la gestion et l'adaptation de la communication entre une large diversité d'éléments aux capacités variées [15] et assurer un passage à l'échelle du modèle qui soit efficace. Les schémas d'authentification traditionnels reposent souvent sur des approches statiques, utilisant toujours les mêmes facteurs d'authentification sans tenir en compte de la nature dynamique des environnements IoT [3]. Cela limite leur capacité à s'adapter aux spécificités des agents hétérogènes impliqués dans chaque interaction, ainsi qu'à estimer et ajuster le niveau de sécurité nécessaire à l'authentification.

Cet article propose un nouveau processus décisionnel d'authentification multi-agent basé sur la confiance pour l'échange d'informations dans l'IoT. Dans ce modèle, la confiance représente à la fois une mesure de la fiabilité des agents et un déterminant de la stratégie d'authentification employée. En évaluant la confiance des agents basée sur leur comportement et leur historique d'interaction, le mécanisme peut adapter les exigences d'authentification, optimisant les mesures de sécurité à chaque cas de figure.

La section 2 fournit un bref état de l'art sur les méthodes d'authentification adaptatives dans l'IoT et les systèmes de gestion de confiance dans les SMA embarqués. La section 3 propose une explication complète et détaillée du modèle proposé qui est utilisé dans les simulations présentées en section 4. Enfin, nous concluons en section 5 sur les avantages du modèle proposé et présentons nos pistes de recherches pour de futurs travaux.

2 État de l'art

L'objectif de cette section est de présenter les techniques existantes pour l'authentification dans l'IoT et les systèmes de gestion de confiance dans les SMA embarqués afin de mettre en évidence les limites des solutions actuelles ainsi que les caractéristiques indispensables à l'élaboration d'un processus d'authentification basé sur la confiance.

2.1 Authentification dans l'IoT

L'expansion rapide de l'IoT a présenté des défis de sécurité significatifs, particulièrement dans le domaine de l'authentification. De nombreuses recherches ont visé l'identification de ces problèmes de sécurité et la recherche de moyens pour se protéger contre les attaques [2, 8]. Les avancées récentes mettent fortement l'accent sur des mécanismes d'authentification multifacteur (MFA) [10], adaptatifs et conscients du contexte [1] pour renforcer la sécurité des environnements IoT. Par exemple, certaines études ont exploré l'utilisation des Fonctions Physiquement Non-clonables (PUFs) [7] fondées sur les propriétés physiques uniques des composants matériels pour générer des clés cryptographiques. Dans [9], les auteurs ont proposé une méthode d'authentification qui prend en compte le contexte de l'environnement dans lequel les dispositifs IoT sont authentifiés. L'authentification basée sur la localisation [18] implique l'utilisation de la localisation de l'entité, comme les coordonnées GPS, pour vérifier leur identité.

2.2 La gestion de la confiance dans les SMA embarqués

La confiance peut être évaluée à partir de retours directs ou indirects basés sur les interactions. La confiance directe est celle qu'un *truster* a sur un *trustee* à partir de leurs interactions directes, tandis que la confiance indirecte est un retour que le *truster* obtient d'une tierce partie à propos du *trustee*. La littérature révèle un intérêt croissant pour la gestion de la confiance comme aspect fondamental de la sécurité de l'IoT. Les études [14, 11] soulignent le rôle critique de la confiance dans la gestion de la complexité et des vulnérabilités inhérentes aux réseaux IoT. Ces travaux démontrent la nécessité d'évoluer au-delà des modèles de sécurité statiques vers des cadres plus adaptatifs et informés par le contexte, capables de répondre dynamiquement à des conditions changeantes et aux menaces. Toutefois, bien que ces recherches constituent un fondement pour la sécurité axée sur la confiance, elles ne fournissent pas de détails sur les mécanismes permettant une prise de décision adaptée au contexte lors des processus d'authentification.

Les SMA embarqués, comme décrits dans [4], sont confrontés à des défis particuliers, tels que la gestion des ressources énergétiques limitées, et la nécessité de maintenir des propriétés robustes de confiance et de sécurité. L'importance d'avoir un processus d'authentification fiable pour s'appuyer sur un système de gestion de la confiance a été souligné dans [16], déjà dans un contexte de SMA embarqué. Ce travail avait alors attaché une mesure de confiance à un identifiant, plutôt qu'à l'agent qu'il est censé représenter, pour contourner cette difficulté.

Bien qu'il y ait eu plusieurs schémas d'authentification adaptative proposés, à notre connaissance, il y a eu peu d'études qui exploitent les valeurs de confiance entre les agents pour informer les décisions d'authentification. Le processus d'authentification adaptative proposé introduit la confiance comme un concept à deux facettes : elle est à la fois une mesure de croyance dans la fiabilité des informations et aussi un déterminant de la stratégie d'authentification employée.

3 Authentification adaptative basée sur la confiance

Nous présentons ici le processus décisionnel utilisé pour sélectionner les agents à authentifier et pour déterminer le niveau de sécurité requis pour chaque authentification en sélectionnant les facteurs à utiliser. L'IoT présente de nombreux avantages et opportunités, notamment en offrant une diversité de facteurs d'authentification. Par exemple, les capteurs IoT, en recueillant des données en temps réel sur leur environnement et sur d'autres objets sur lesquels sont déployés d'autres agents, fournissent des informations précieuses qui peuvent être exploitées pour l'authentification. Nous avons illustré la pertinence de l'utilisation opportuniste de capteurs déployés dans des systèmes connexes pour fiabiliser une authentification basée sur un seul tag RFID dans le contexte du contrôle d'accès à un parking [13]. Les données collectées par les capteurs peuvent ainsi représenter des facteurs d'authentification. Nous proposons de développer une stratégie pour choisir les facteurs d'authentification les plus appropriés en fonction de critères spécifiques.

3.1 Architecture générale

Nous introduisons des composants spécifiques pour l'authentification basée sur la confiance, destinés à être intégrés dans des agents applicatifs au sein d'un SMA embarqué (Figure 1). Chaque agent est équipé de capteurs, et/ou d'actionneurs, leur permettant de percevoir leur environnement, de réaliser des actions et de communiquer les uns avec les autres. Les agents varient en termes de puissance de calcul, de capacité de stockage et de ressources énergétiques, reflétant ainsi la diversité des environnements IoT.

L'environnement dans lequel les agents évoluent est caractérisé par sa nature dynamique et l'apparition d'événements imprévisibles. Nous nous focalisons sur les types d'environnements où les agents peuvent être amenés à recevoir simultanément le même type d'informations issu de plusieurs agents. Cependant, la véracité de ces informations est parfois variable et peut indiquer un comportement malveillant ou une tentative d'attaque de la part d'un ou plusieurs agents.

Un système de gestion de la confiance est un composant essentiel de notre modèle, permettant aux agents d'évaluer et de mettre à jour leurs valeurs de confiance qu'ils attribuent aux autres agents en se basant sur les interactions passées et la qualité des informations partagées. Bien que le choix du système de gestion de la confiance ne constitue pas l'élément central de notre article, il représente une décision importante à prendre lors de l'implémentation de l'agent applicatif.

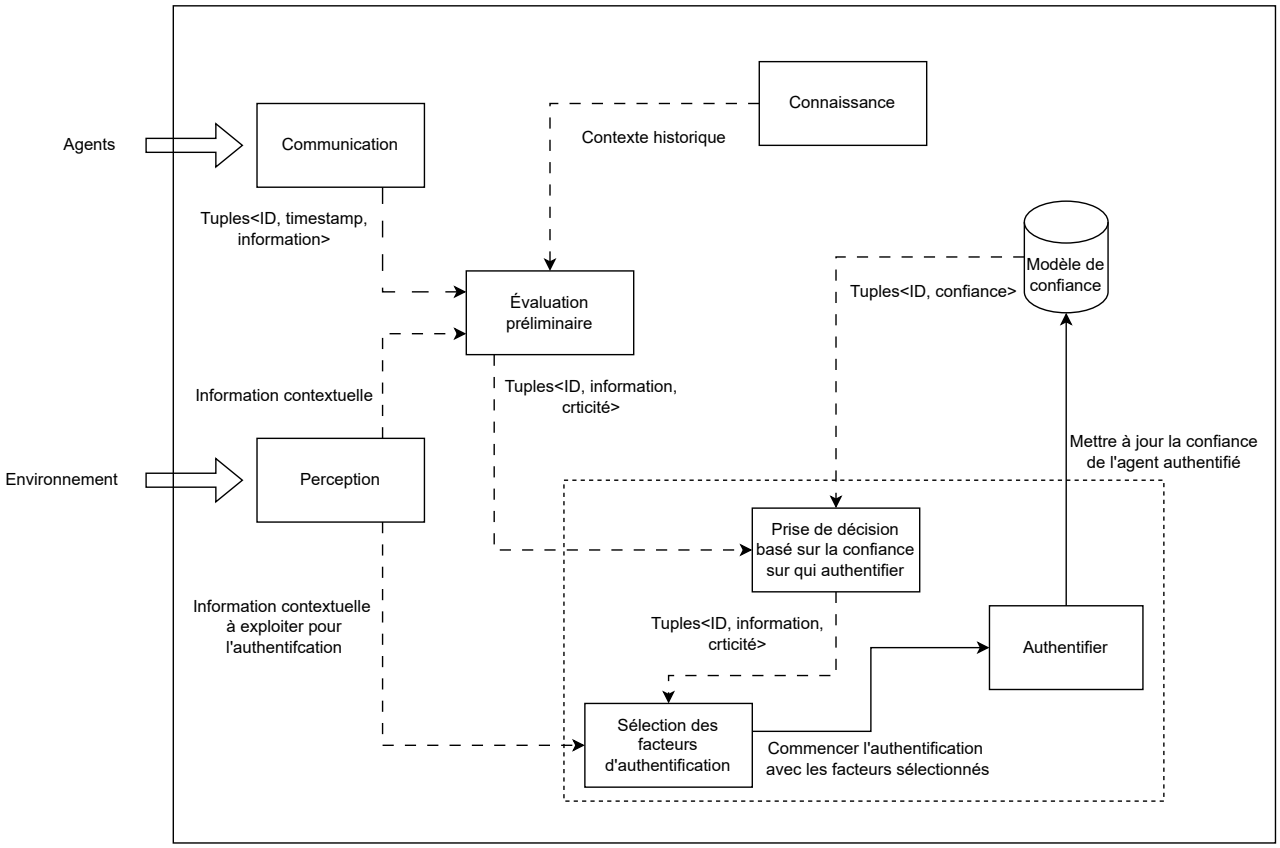

FIGURE 1 – Composants liés à l'authentification et à la gestion de la confiance

Le processus décisionnel proposé dans cet article permet aux agents de prendre en compte ou non les messages reçus de la part d'autres agents, liant la confiance accordée à l'identité d'un agent à la rigueur de son processus d'authentification. Nous considérons qu'une authentification a un coût que notre processus prend en compte pour décider d'authentifier un agent uniquement si cela en vaut la peine, c'est-à-dire que le risque encouru justifie la dépense en énergie, en temps de calcul, etc. En cela, notre approche est adaptée aux contraintes des environnements IoT, où l'optimisation des ressources de calcul et de communication est importante. Cela permet d'équilibrer efficacement les besoins de sécurité avec les contraintes de ressources.

Dans ce modèle, l'authentification vise précisément à vérifier l'identité de l'agent envoyant le message. Chaque message envoyé par un agent inclut des informations essentielles telles que l'identifiant unique de l'agent (un identifiant déclaré), un marqueur temporel indiquant le moment de l'envoi, et le contenu des données qui varie selon l'objectif de l'agent et la nature des informations partagées.

3.2 Modèle d'attaque

Nous nous intéressons ici aux attaques par usurpation d'identité (Impersonation). Dans une attaque par usurpation d'identité, un agent malveillant revendique l'identité d'un autre agent légitime pour interférer dans les communications et les interactions entre agents. En utilisant une identité digne de confiance, l'agent malveillant peut manipuler les flux de données, injecter de fausses informations, perturbant ainsi l'intégrité et la fiabilité des communications. Pour se défendre contre ces attaques, le système IoT doit mettre en œuvre des mécanismes d'authentification robustes capables de détecter et de mitiger l'usurpation d'identité et les abus de multiples identités.

3.3 Processus décisionnel d'authentification basé sur la confiance

Le processus décisionnel présenté ici a pour objectif de réaliser une authentification par un agent qui aura donc le rôle de *truster* afin de confirmer ou d'infirmer l'identité d'un autre agent.

Il se déroule en cinq étapes, chacune pouvant comprendre plusieurs sous-étapes, détaillées ci-dessous. La Figure 2 illustre ce processus de prise de décision composé des étapes suivantes :

Réception de messages. Le processus débute lorsqu'un agent *truster* reçoit des messages émis par d'autres agents. Ces messages peuvent être traités par l'agent *truster* avant l'authentification de leurs expéditeurs. [1]

Évaluation de la confiance. Nous définissons deux seuils de confiance : un seuil minimum de confiance, Θ_{min}, à partir duquel l'agent *truster* accepte de déployer des ressources pour l'authentification, et un seuil de confiance élevée, Θ_{high}, à partir duquel nous considérons que l'identité est digne de confiance. Pour chaque message reçu, trois scénarios sont envisagés en fonction de la confiance accordée à l'identité revendiquée :

- Si l'identité revendiquée est celle d'un agent digne de confiance (niveau de confiance supérieur à Θ_{high}), l'agent *truster* effectue une évaluation préliminaire de la criticité des informations reçues et les compare, le cas échéant, à d'autres messages reçus dans le même contexte émanant d'autres agents revendiquant des identités dignes de confiance. Cette comparaison d'informations est intrinsèquement liée à l'application spécifique dans laquelle les agents sont déployés, soulignant l'importance d'une approche méthodologique adaptée.
- Si l'identité revendiquée est celle d'un agent en qui le truster n'a pas confiance (niveau de confiance inférieur à Θ_{min}), il est possible de passer outre le processus d'authentification, puisque l'agent *truster* ne considérera pas l'information partagée comme fiable, faute de confiance en son émetteur.
- Si le niveau de confiance attaché à l'identité revendiquée est incertain (niveau de confiance entre Θ_{min} et Θ_{high}), du à un manque d'interactions directes ou de retours de tiers, un niveau de sécurité moyen est appliqué pour la vérification de l'identité. Alternativement, il est possible de négliger l'authentification si d'autres messages sur la même information provenant d'identités dignes de confiance sont disponibles.

1. Ce pré-traitement peut être justifié par exemple lorsque la latence est une contrainte critique et que la vérification immédiate pourrait retarder des réponses urgentes nécessaires au fonctionnement du système. Dans notre étude, ce pré-traitement est principalement utilisé pour évaluer le niveau de criticité de l'information partagée.

Vérification de la cohérence. Cette étape est essentielle lorsque l'agent *truster* reçoit plusieurs messages portant sur la même information, émanant d'agents revendiquant des identités dignes de confiance, et est particulièrement liée à l'application spécifique. Par exemple, la réception de plusieurs messages indiquant la température dans un lieu spécifique. Si les informations ne sont pas cohérentes, il y a une suspicion d'attaque possible, ce qui conduit à l'authentification de tous les agents. Si les informations sont cohérentes, l'agent *truster* procède à la sélection d'un sous-groupe d'agents pour réaliser une authentification approfondie. Nous supposons qu'il est hautement improbable que tous les agents du groupe initial soient compromis en même temps tout en partageant des informations cohérentes, ce qui permet de réduire le nombre d'agents nécessaires pour l'authentification sans impacter de manière significative la sécurité.

Authentification. Pour chaque agent du sous-groupe sélectionné, un niveau de sécurité approprié est choisi pour l'authentification. Ce niveau est déterminé en fonction de plusieurs critères clés, notamment le degré de confiance associé à l'identité revendiquée et la criticité de l'information partagée. Nous supposons qu'un ensemble diversifié de facteurs d'authentification est disponible, chacun offrant un compromis spécifique entre coût énergétique, robustesse de la sécurité et le taux d'acceptation des faux positifs (FAR). L'objectif ici est donc de sélectionner la meilleure combinaison de facteurs selon les critères donnés. Pour cela, nous définissons :

- $Conf$: La confiance en l'identité déclarée par l'agent cherchant l'authentification, $Conf : id \rightarrow [\Theta_{min}, 1]$, où Θ_{min} est le seuil minimum de confiance pour justifier une authentification, et 1 représente le niveau maximal de confiance.
- $Crit$: Le niveau de criticité de l'information partagée, $Crit : info \rightarrow [\tau_{min}, 1]$, où τ_{min} est le seuil minimum de criticité pour justifier une authentification, et 1 est le niveau maximal de criticité.
- w_{FAR} et w_{CE} : Les poids pour le taux d'acceptation des faux positifs et le coût énergétique, calculés comme suit :

$$\begin{aligned} w_{FAR} &= \min(P_{FAR}, a \cdot Conf + b \cdot Crit) \\ w_{CE} &= 1 - w_{FAR} \end{aligned} \tag{1}$$

où $a + b = 1$, P_{FAR} est le plafond du poids attribué à w_{FAR}, a et b sont des coefficients ajustables

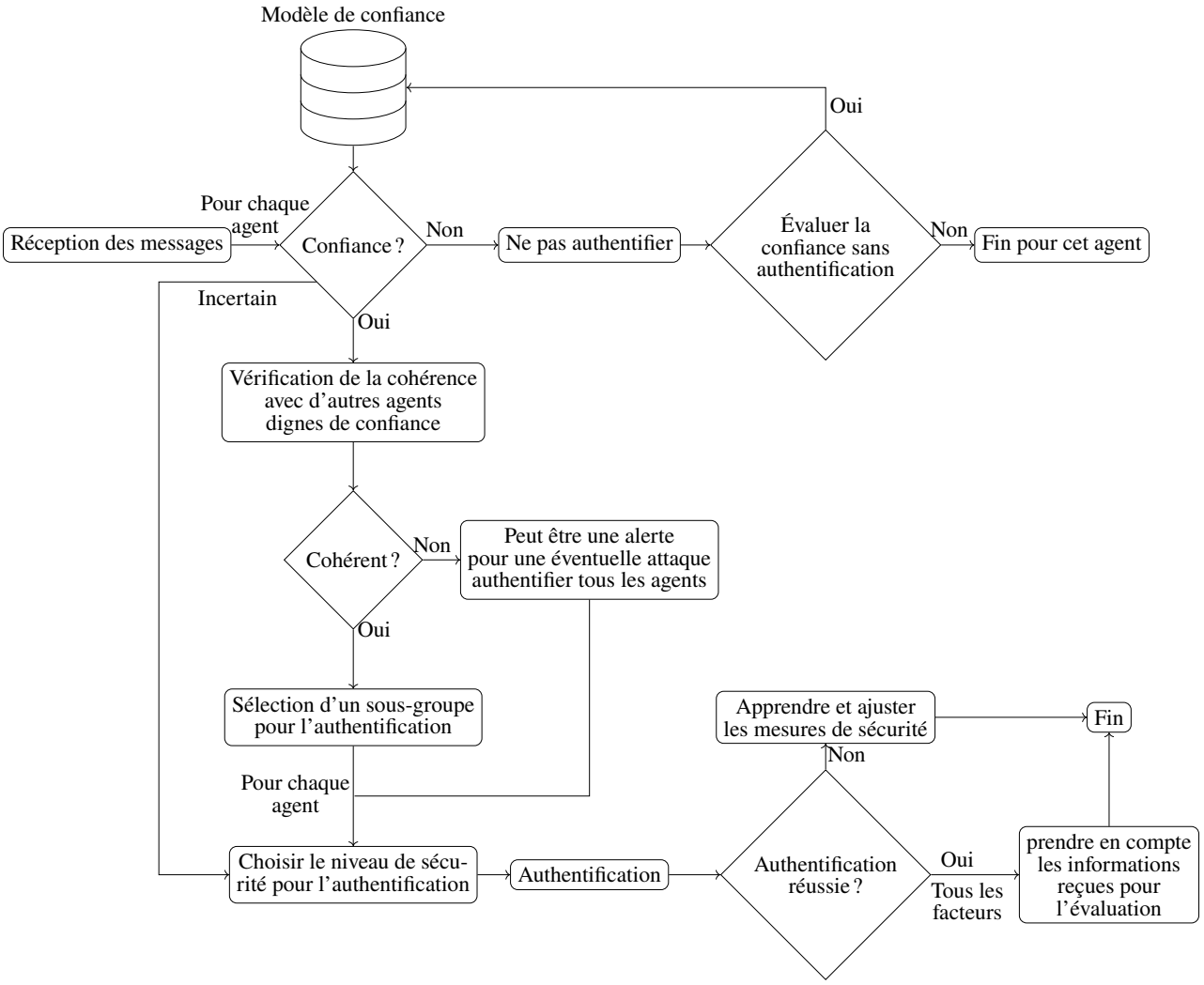

FIGURE 2 – Schéma du processus décisionnel d'authentification

pour équilibrer l'influence de $Conf$ et $Crit$ sur la sécurité et le coût.

- Score$_{FAR}$: Calculé comme la moyenne pondérée des FAR de tous les facteurs utilisés.

$$\text{Score}_{FAR} = \sum_{i=1}^{n} w_i \cdot FAR_i \tag{2}$$

où $\sum_{i=1}^{n} w_i = 1$, FAR_i est le FAR du i-ème facteur d'authentification dans la combinaison, et w_i sont les poids attribués à chaque facteur, qui pourraient être égaux ou varier selon d'autres critères.
- Score$_{CE}$: Calculé comme la somme des coûts de tous les facteurs utilisés.

$$\text{Score}_{CE} = \sum_{i=1}^{n} \text{coût}_i \tag{3}$$

où coût$_i$ représente le coût énergétique du i-ème facteur d'authentification dans la combinaison. Ce score doit être normalisé pour garantir que tous les composants contribuent de manière équilibrée à l'évaluation globale.
- Score$_{Global}$: Le score global donné à l'ensemble de facteurs choisis.

$$\text{Score}_{Global} = w_{FAR} \cdot \text{Score}_{FAR} + w_{CE} \cdot \text{Score}_{CE} \tag{4}$$

L'objectif est de minimiser ce score global. Un Score$_{Global}$ bas indique une combinaison efficace de faible FAR et de coût énergétique bas, signifiant une performance optimale du système d'authentification en termes de sécurité et d'efficacité énergétique.

Évaluation de l'authentification. Si l'authentification réussit, l'agent *truster* prend alors en compte les informations reçues pour une évaluation future et une mise à jour éventuelle du niveau de confiance.

4 Mise en œuvre et évaluation

Pour tester notre modèle, nous avons mis en œuvre une simulation d'un environnement IoT reflétant un scénario de navigation multi-agents. Ce scénario facilite l'évaluation de notre mécanisme en raison de la nature dynamique de l'environnement et de la nécessité pour les agents d'obtenir des informations des autres agents pour naviguer efficacement. La mise en place du scénario a été réalisée en utilisant le framework basé sur les agents MESA [6]. Le mécanisme proposé, incluant le modèle d'évaluation de la confiance et le processus d'authentification adaptatif, a été intégré dans la simulation. Chaque appareil IoT est représenté comme un agent capable d'évaluer dynamiquement les niveaux de confiance et de prendre des décisions d'authentification basées sur les critères de notre modèle.

4.1 Scénario de navigation multi-agents

Environnement. L'espace de navigation est représenté par une grille 2D qui représente une carte, introduisant un contexte spatial pour les mouvements des agents. Des obstacles sont placés stratégiquement ou aléatoirement dans la carte, marquant des positions que les agents ne peuvent pas franchir. La présence d'événements dynamiques, tels que des changements de position des obstacles ou l'introduction de nouveaux obstacles, contribue à l'incertitude de l'environnement.

Agents. Le SMA est ouvert, permettant l'entrée et la sortie dynamiques d'agents. Nous distinguons deux types d'agents :

1. **Navigateurs.** Un agent *navigateur* est un agent autonome placé aléatoirement sur la carte et doté de capacités de navigation. Il a pour objectif d'atteindre une destination spécifique qu'il ne connaît pas tout en minimisant la distance de navigation. Il possède une connaissance limitée de la carte, ne pouvant détecter que son environnement proche, qui inclut toutes les cellules adjacentes à celle où il se situe dans la carte.
2. **Guides.** Un agent *guide* est un agent autonome qui n'a pas de présence physique sur la carte mais qui possède une connaissance globale de la carte, incluant la position des obstacles et les destinations des *navigateurs*. Il a pour objectif de gérer le comportement global du système multi-agents en communicant avec les *navigateurs* pour envoyer des informations essentielles sur la carte.

Interaction et collaboration. Les *guides* communiquent aux *navigateurs* l'emplacement des obstacles sur la carte et les destinations à atteindre pour chaque *navigateur*. Ces derniers, dépendant de cette interaction pour obtenir les renseignements nécessaires à la navigation, évaluent les informations reçues en fonction de leur confiance dans les *guides* afin de prendre des décisions sur leur parcours sur la carte. Ainsi, des informations au sujet d'un même objet (carte et destinations) sont reçues simultanément de la part de différents *guides*.

Confiance. Dans notre simulation, les *navigateurs* utilisent le système de gestion de confiance Beta Reputation System (BRS) [5] pour évaluer la fiabilité des *guides* sur la base de leurs actions passées [2]. BRS utilise les résultats positifs et négatifs des interactions précédentes pour calculer la probabilité qu'un agent agisse de manière fiable dans le futur. Mathématiquement, la valeur de confiance d'un agent *trustee* dans BRS est calculée à l'aide de la formule suivante :

$$Conf = \frac{\alpha}{\alpha + \beta} \tag{5}$$

$$\alpha = r + 1 \text{ et } \beta = s + 1 \tag{6}$$

où r et s représentent respectivement le nombre d'interactions positives et négatives qu'un agent *truster* a eues avec le trustee en question. Cette formule fournit une estimation de la probabilité que l'agent se comporte de manière honnête dans une interaction future. Une valeur proche de 1 indique une haute fiabilité, tandis qu'une valeur proche de 0 suggère une faible fiabilité. Dans notre scénario, une interaction négative représente une fausse information sur la carte, telle que de mauvaises positions des obstacles ou de fausses destinations, tandis qu'une interaction positive représente une bonne carte partagée avec les bonnes positions des obstacles et les bonnes destinations. Les *navigateurs* pouvant détecter les fausses positions des obstacles plus rapidement que les fausses destinations, nous introduisons un poids w_β à β pour pénaliser plus fortement les *guides* partageant de fausses destinations.

2. D'autres modèles de gestion de confiance peuvent être utilisés, le choix du modèle de confiance n'étant pas l'apport central de notre article.

Facteur	Coût Énergétique (mJ)	Niveau de Sécurité	TNR	FAR
1	0.2	Faible	0.85	0.15
2	3.0	Élevé	0.98	0.02
3	1.5	Moyen	0.92	0.08
4	2.6	Élevé	0.97	0.03
5	0.8	Moyen	0.89	0.11
6	0.6	Faible	0.88	0.12
7	2.0	Élevé	0.95	0.05
8	1.2	Moyen	0.90	0.10

TABLE 1 – Facteurs d'authentification artificiels

Authentification. Les agents *navigateurs* utilisent le modèle proposé en section 3.3 pour authentifier les agents *guides*. Nous avons défini, dans le tableau 1, plusieurs facteurs d'authentification pour la simulation. Chacun de ces facteurs est représenté de manière abstraite, défini par son coût énergétique, le niveau de sécurité qu'il procure, et le Taux de Vrais Négatifs (TNR) et $FAR = 1 - TNR$. Nous avons choisi de classer la sécurité sur trois niveaux : faible, moyen et élevé. Nous présentons les facteurs de manière qu'ils augmentent en coût énergétique proportionnellement au niveau de sécurité. Un agent *navigateur* sélectionne un ou plusieurs facteurs pour l'authentification en fonction de la stratégie adoptée.

4.2 Résultats et évaluation

Nous décrivons ici les résultats obtenus en lançant notre simulation sur 200 épisodes. Chaque épisode commence par l'initialisation de l'environnement et le placement des agents *navigateurs* sur la carte, et se termine lorsque tous les agents *navigateurs* ont atteint leurs destinations. Dans chaque épisode, les agents *guides* fournissent aux *navigateurs* des informations sur la carte. Ces derniers authentifient les messages reçus et évaluent et mettent à jour les valeurs de confiance pendant la navigation. Nous avons simulé 3 agents *navigateurs*, chacun adoptant une stratégie d'authentification différente, et 10 agents *guides* dont 6 malveillants partageant des informations erronées sur la carte. Les trois stratégies d'authentification utilisées dans notre simulation :

- Authentification Statique (AS) : une méthode basée sur les deux mêmes facteurs pour tous les agents. Le choix des deux facteurs suit une approche classique, combinant un facteur de sécurité faible et un facteur de sécurité élevée.
- Authentification Adaptative basée sur la Criticité de l'information partagée (AAC) : une méthode adaptative qui sélectionne les facteurs à utiliser selon le niveau de criticité mais qui n'exploite pas les valeurs de confiance.
- Authentification Adaptative basée sur la Confiance et la Criticité (AACoC) : une méthode qui représente notre processus d'authentification, utilisant la confiance pour choisir les identités à authentifier ainsi que la confiance et la criticité pour sélectionner les facteurs à utiliser.

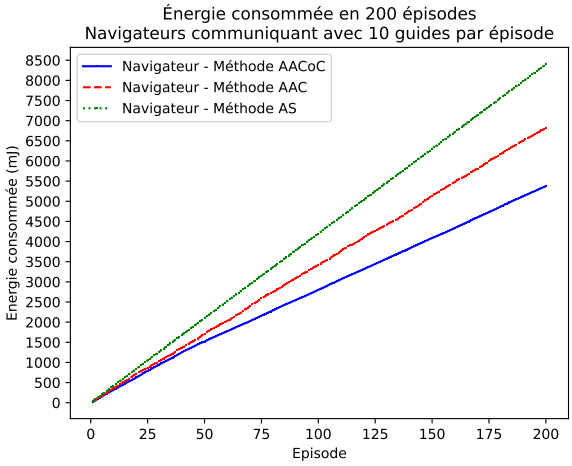

FIGURE 3 – Énergie consommée pour l'authentification en 200 épisodes

L'efficacité des ressources. Le graphique présenté dans la Figure 3 illustre la consommation énergétique cumulée sur les 200 épisodes avec les trois stratégies d'authentification pour un *navigateur* communiquant avec 10 *guides* par épisode.

Le processus d'authentification que nous proposons (AACoC) réduit la consommation énergétique de 19% par rapport à la méthode AAC, qui ne prend pas en compte la confiance, et de 37% par rapport à la méthode AS, qui authentifie

	Méthode AACoC	Méthode AAC	Méthode AS
Nombre d'attaques réussies	9	14	17
Taux d'attaques réussies	2.25%	3.5%	4.25%
Moyenne des pas par épisode (20 étant l'optimal)	22	25	27

TABLE 2 – Nombre d'attaques réussies et moyenne des pas par épisode sur 200 épisodes

systématiquement tous les agents et qui entraîne une consommation énergétique linéaire en raison de l'utilisation répétée des mêmes facteurs pour chaque authentification.

En évitant l'authentification d'agents avec qui les interactions précédentes ont été suffisantes mais non concluantes en termes de confiance, et en adaptant les facteurs d'authentification utilisés en fonction de la confiance établie et de la criticité des informations échangées, nous améliorons l'efficacité énergétique. L'authentification n'est donc effectuée que si le risque encouru justifie la dépense en énergie. Cette approche permet ainsi de concentrer les ressources là où elles apportent le plus de valeur, contribuant directement aux économies d'énergie observées.

Impact sur la sécurité. Nous avons simulé des attaques par usurpation d'identité en nous appuyant sur les FAR des facteurs d'authentification artificiels (tableau 1). Sur 200 épisodes, 2000 interactions au total dont 400 non légitimes ont été enregistrées. La simulation a été structurée pour que les attaquants essaient d'usurper l'identité des agents *guides* dignes de confiance. Chaque tentative d'attaque réussie permet à l'attaquant de partager des informations erronées de la carte avec les *navigateurs*, induisant ces derniers en erreur dans leurs trajets. Le tableau 2 résume le nombre d'attaques réussies et l'impact correspondant de celles-ci sur les temps de parcours des *navigateurs*. Plus précisément, lorsqu'un *navigateur* accepte une carte incorrecte envoyée par un attaquant, le nombre de pas nécessaires pour atteindre la destination peut augmenter jusqu'à plus de 50. Cet effet n'est pas toujours évident lorsqu'on examine la moyenne des pas par épisode, en raison du nombre relativement faible d'attaques réussies comparé au nombre total d'interactions. Notre modèle présente de meilleures performances en termes de détection d'attaques par agents malveillants puisqu'il déjoue 97,75 % des attaques contre 96.5% et 95.75% pour les modèles concurrents (tableau 2).

5 Conclusion

Dans ce travail, nous avons présenté un nouveau processus décisionnel d'authentification adaptative basé sur la confiance, conçu spécifiquement pour les environnements dynamiques et hétérogènes de l'Internet des Objets. Ce processus permet, dans un contexte d'échange d'informations dans des SMA embarqués, d'ajuster le niveau de sécurité requis pour l'authentification en fonction de la confiance accordée à l'identité revendiquée par l'émetteur et de la criticité de l'information transmise. En effet, l'évaluation de la confiance et la criticité permet de sélectionner les identités à authentifier et la meilleure approche d'authentification à travers une combinaison de facteurs d'authentification optimisant les ressources dépensées et minimisant le taux de faux positifs.

L'efficacité de notre modèle a été démontrée à travers les résultats obtenus dans les simulations de navigation multi-agents précédemment présentées : seulement 2.25% d'attaques par agents malveillants réussies contre 3.5% et 4.25% pour d'autres modèles moins adaptatifs. De plus, le coût énergétique de notre proposition est significativement réduit, de l'ordre de 19% à 37%, par rapport à celui de méthodes moins adaptatives. Ainsi, nous démontrons que notre stratégie d'authentification adaptative permet non seulement de déjouer davantage d'attaques notamment en renforçant l'authentification des agents *trustee* dignes de confiance mais aussi d'optimiser l'utilisation des ressources en réduisant la nécessité d'authentifications inutiles.

Nos futurs travaux se concentrent sur les trois axes suivants : la validation de notre modèle avec des facteurs d'authentification réels plutôt qu'artificiels, le développement d'un système de gestion de confiance proposant une stratégie plus fine pour la sélection des facteurs d'authentification, et enfin l'extension de notre modèle pour la gestion d'autres types d'attaques liées à l'identité. Ces améliorations permettront une plus grande robustesse et flexibilité du modèle

face à un éventail plus large de menaces, tout en optimisant le processus d'authentification des agents et leurs relations de confiance de manière dynamique dans un environnement IoT.

Remerciements. Ce travail est soutenu par l'Agence Nationale de la Recherche (ANR) dans le cadre du projet MaestrIoT ANR-21-CE23-0016.

Références

[1] Patricia Arias-Cabarcos, Christian Krupitzer, and Christian Becker. A survey on adaptive authentication. *ACM Computing Surveys (CSUR)*, 52(4) :1–30, 2019.

[2] Leonardo Babun, Kyle Denney, Z Berkay Celik, Patrick McDaniel, and A Selcuk Uluagac. A survey on iot platforms : Communication, security, and privacy perspectives. *Computer Networks*, 192 :108040, 2021.

[3] Mohammed El-Hajj, Ahmad Fadlallah, Maroun Chamoun, and Ahmed Serhrouchni. A survey of internet of things (iot) authentication schemes. *Sensors*, 19(5) :1141, 2019.

[4] Jean-Paul Jamont and Michel Occello. Meeting the challenges of decentralised embedded applications using multi-agent systems. *International Journal of Agent-Oriented Software Engineering*, 5(1) :22–68, 2015.

[5] Audun Josang and Roslan Ismail. The beta reputation system. In *Proceedings of the 15th Bled Electronic Commerce Conference*, volume 5, pages 2502–2511, 2002.

[6] Jackie Kazil, David Masad, and Andrew Crooks. Utilizing python for agent-based modeling : The mesa framework. In *Social, Cultural, and Behavioral Modeling : 13th International Conference, SBP-BRiMS 2020, Washington, DC, USA, October 18–21, 2020, Proceedings 13*, pages 308–317. Springer, 2020.

[7] Priyanka Mall, Ruhul Amin, Ashok Kumar Das, Mark T Leung, and Kim-Kwang Raymond Choo. Puf-based authentication and key agreement protocols for iot, wsns, and smart grids : a comprehensive survey. *IEEE IoT Journal*, 9(11) :8205–8228, 2022.

[8] Francesca Meneghello, Matteo Calore, Daniel Zucchetto, Michele Polese, and Andrea Zanella. Iot : Internet of threats ? a survey of practical security vulnerabilities in real iot devices. *IEEE Internet of Things Journal*, 6(5) :8182–8201, 2019.

[9] Markus Miettinen, Thien Duc Nguyen, Ahmad-Reza Sadeghi, and N Asokan. Revisiting context-based authentication in iot. In *Proceedings of the 55th Annual Design Automation Conference*, pages 1–6, 2018.

[10] Aleksandr Ometov, Sergey Bezzateev, Niko Mäkitalo, Sergey Andreev, Tommi Mikkonen, and Yevgeni Koucheryavy. Multi-factor authentication : A survey. *Cryptography*, 2(1) :1, 2018.

[11] Behrouz Pourghebleh, Karzan Wakil, and Nima Jafari Navimipour. A comprehensive study on the trust management techniques in the internet of things. *IEEE Internet of Things Journal*, 6(6) :9326–9337, 2019.

[12] Jordi Sabater-Mir and Laurent Vercouter. *Trust and Reputation in Multi-Agent Systems*, pages 381–419. Number 9. MIT Press, g. weiss edition, 2013.

[13] Marc Saideh, Jean-Paul Jamont, and Laurent Vercouter. Opportunistic sensor-based authentication factors in and for the internet of things. *Sensors*, 24(14), 2024.

[14] Avani Sharma, Emmanuel S Pilli, Arka P Mazumdar, and Poonam Gera. Towards trustworthy internet of things : A survey on trust management applications and schemes. *Computer Communications*, 160 :475–493, 2020.

[15] CC Sobin. A survey on architecture, protocols and challenges in iot. *Wireless Personal Communications*, 112(3) :1383–1429, 2020.

[16] Laurent Vercouter and Jean-Paul Jamont. Lightweight trusted routing for wireless sensor networks. *Progress in Artificial Intelligence*, 1 :193–202, 2012.

[17] Han Yu, Zhiqi Shen, Cyril Leung, Chunyan Miao, and Victor R Lesser. A survey of multi-agent trust management systems. *IEEE Access*, 1 :35–50, 2013.

[18] Feng Zhang, Aron Kondoro, and Sead Muftic. Location-based authentication and authorization using smart phones. In *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, pages 1285–1292. IEEE, 2012.