


# Trust-Based Multi-Agent Authentication Decision Process for the Internet of Things

Marc Saideh<sup>1</sup> <sup>a</sup>, Jean-Paul Jamont<sup>2</sup> <sup>b</sup> and Laurent Vercouter<sup>1</sup> <sup>c</sup>

<sup>1</sup>INSA Rouen Normandie, Normandie Université, LITIS UR 4108, 76000 Rouen, France

<sup>2</sup>Université Grenoble Alpes, LCIS, 26000 Valence, France

{marc.saideh, laurent.vercouter}@insa-rouen.fr; jean-paul.jamont@univ-grenoble-alpes.fr

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

**Abstract:** In the Internet of Things (IoT), systems often operate in open and dynamic environments composed of heterogeneous objects. Deploying a multi-agent system in such environments requires agents to interact with new agents and use their information and services. These interactions and resulting dependencies create vulnerabilities to malicious behaviors, highlighting the need for a robust trust management system. Multi-agent trust management models rely on observations of the behavior of other agents who must be authenticated. However, traditional authentication systems face significant limitations in adapting to diverse contexts and addressing the hardware constraints of the IoT. This paper proposes a novel trust-based multi-agent adaptive decision-making process for authentication in the IoT. Our approach dynamically adjusts authentication decisions based on the context and trustworthiness of the agent being authenticated, thereby balancing resource use for authentication with security needs and ensuring a more adaptable authentication process. We evaluate our model in a multi-agent navigation simulation, demonstrating its effectiveness for security and resource efficiency.

## 1 INTRODUCTION


The deployment of Multi-Agent Systems (MAS) in the context of the Internet of Things (IoT) requires agents to be able to act autonomously despite limited resources and partial knowledge of their environment. These constraints necessarily lead to dependence on the services and resources offered by other agents to achieve their goals. The uncertainty regarding the reliability of other agents, who may not follow the same set of rules and guidelines or act dishonestly, complicates the decision-making of an agent in a situation of dependence. This emphasizes the importance of assessing trust and taking into account the risks involved in interacting with other agents.


A trust relationship involves two roles: a *truster*, the agent who depends on another agent for a service or information, and a *trustee*, the agent providing the service to the *truster*. Trust in itself then corresponds to the belief that the *truster* has in the *trustee*'s ability, competence or intention to act in a way that ben-


efits the *truster* (Sabater-Mir and Vercouter, 2013; Yu et al., 2013). Agents benefiting from trust management systems prioritize interactions with those they trust, enabling them to detect and isolate any exhibiting malicious behavior. In our study context, these systems are essential components for ensuring cooperation, information sharing, and effective decision-making.

When a *truster* agent has to make a decision based on information provided by a *trustee* agent, it relies on the trust it estimates in the latter's claimed identity. As a result, the trust relationship established is vulnerable to authentication attacks, especially if a malicious agent manages to impersonate the identity of a trusted one. The potential risk to the *truster* is significant when they communicate with a compromised trusted agent, as they will rely on the false information or malicious services provided by the impersonated identity. Authentication ensures that communication occurs between agents with verified identities, and that only authorized agents access services and data, maintaining the integrity and confidentiality of the system.

While authentication ensures the identity of interacting agents, it encounters several major challenges

<sup>a</sup>  <https://orcid.org/0009-0007-5406-8149>

<sup>b</sup>  <https://orcid.org/0000-0002-0268-8182>

<sup>c</sup>  <https://orcid.org/0000-0002-0918-8033>

when applied in IoT environments. IoT interactions involve devices with highly heterogeneous characteristics, ranging from high-powered computing devices to low-powered sensors operating under strict energy, cost, and time constraints. The system must be able to manage and adapt communication between a wide variety of objects with varying capabilities and ensure efficient scalability (Sobin, 2020). Traditional authentication schemes often rely on static approaches, always using the same authentication factors without considering the dynamic nature of IoT environments (El-Hajj et al., 2019). This restricts their ability to adapt to the specific requirements of the heterogeneous agents involved in each interaction, as well as to estimate and adjust the level of security needed for authentication.

This paper proposes a new multi-agent Adaptive Authentication decision process based on Trust (AAT) for information exchange in the IoT. While trust helps assess agent reliability, we recognize that authentication strengthens the certainty of that trust. However, authentication comes with costs, especially in resource-constrained IoT environments. In AAT, we exploit trust both to assess agent reliability and to determine the authentication factors to be used for each authentication, dynamically adapting security measures based on the trust level of agents. This dynamic selection of authentication factors ensures that the level of security is directly proportional to the trustworthiness of the agents involved. Given the limited resources in IoT environments, the objective of AAT is to ensure that resources for authentication are used only when necessary. We validate our model through a multi-agent navigation scenario, demonstrating its efficacy and efficiency in terms of both security and energy consumption.

Section 2 provides an overview of existing adaptive authentication methods in IoT and trust management systems for security. Section 3 offers a comprehensive and detailed explanation of AAT, which is used in the simulations presented in section 4. Finally, we conclude in section 5 on the advantages of the proposed model and present our avenues for future research.

## 2 BACKGROUND

The aim of this section is to present existing techniques for authentication in the IoT and trust management systems in order to highlight the limitations of current solutions as well as the essential features for the development of a trust-based authentication process.

### 2.1 Authentication in IoT

The rapid expansion of the IoT has presented significant security challenges, particularly in the area of authentication. As billions of devices become interconnected, ensuring secure and reliable authentication methods becomes paramount to protect sensitive data and prevent unauthorized access. Much research has focused on identifying these security issues and finding ways to protect against attacks (Jahangeer et al., 2023; Kaur et al., 2023; Babun et al., 2021; Meneghello et al., 2019).

One of the primary methods explored is Multi-Factor Authentication (MFA), which combines two or more independent credentials typically categorized into three main groups: what the entity knows (password), what the entity has (security token), and what the entity is (biometric verification) (Ometov et al., 2018). Recent advancements in MFA mechanisms emphasize the integration of adaptive and context-aware approaches to enhance the security of IoT environments (Ometov et al., 2018; Arias-Cabarcos et al., 2019; Miettinen et al., 2018). For instance, adaptive MFA systems can adjust the required authentication factors based on the risk level of the access attempt. Context-aware models have been largely used to secure authentication mechanisms, adding an additional layer of security by evaluating variables such as context of interaction, time, location, and behavior patterns (Khanpara et al., 2023; Ryu et al., 2023; Arfaoui et al., 2019). For example, location-based authentication involves using the entity's geographical location, verified through GPS coordinates, to authenticate their identity (Zhang et al., 2012). Additionally, innovative techniques like Physically Unclonable Functions (PUFs) leverage the unique physical properties of hardware components to generate cryptographic keys, providing a robust solution against cloning attacks (Mall et al., 2022).

### 2.2 Trust Management for Security

Trust management is a critical aspect of security in IoT, where agents often operate with limited computational and energy resources. Trust can be assessed from direct or indirect feedback based on interactions. Direct trust is the trust that a *truster* has in a *trustee* based on their direct interactions, while indirect trust is built by feedback that the *truster* receives from third parties about the *trustee* (Pinyol and Sabater-Mir, 2013).

The literature reveals a growing interest in trust management as a fundamental aspect of IoT security. Studies (Koohang et al., 2022; Sharma et al., 2020;

Pourghbleh et al., 2019) highlight the critical role of trust in managing the complexity and vulnerabilities inherent in IoT networks. These works demonstrate the need to move beyond static security models towards more adaptive, context-informed frameworks capable of responding dynamically to changing conditions and threats. Adaptive trust management systems can adjust their trust assessments based on real-time information, ensuring a more resilient and flexible security posture (Pham and Yeo, 2018). Similarly, (Feng et al., 2023) incorporate trust and reputation mechanisms in their authentication scheme for the Internet of Vehicles, highlighting the importance of these elements in ensuring secure and reliable communications.

Embedded MAS face particular challenges such as managing limited energy resources and maintaining robust trust and security properties (Sahoo et al., 2019; Jamont and Ocello, 2015). These systems require efficient and lightweight trust management and authentication protocols that do not overly burden their limited resources. The importance of having a reliable authentication process that relies on a trust management system was highlighted by (Vercouter and Jamont, 2012), specifically in an embedded MAS context. This work proposed attaching a measure of trust to an identifier rather than to the agent it is supposed to represent, circumventing the difficulty of directly assessing an agent's trustworthiness.

In addition to trust management, adaptive selection of authentication factors has been explored as a means to enhance security. For example, (Dasgupta et al., 2016) proposed an adaptive strategy for selecting authentication factors based on the selection of devices, media, and surrounding contexts. This approach dynamically adjusts the factors used, such as passwords or biometric data, according to performance metrics and contextual information gathered during the authentication process. Such strategies aim to optimize security while accommodating the varying capabilities of devices and the specific requirements of different environments.

While existing studies lay a foundation for trust-based security and adaptive selection of authentication factors, they generally overlook how trust relationships between agents can inform decision-making during authentication processes. Although trust metrics are used to evaluate the reliability of agents, there is a need for frameworks that dynamically adjust authentication requirements based on these trust levels. Our proposed adaptive authentication decision process introduces trust as a two-faceted concept: it serves both as a measure of belief in the reliability of information and as a determinant of the authenti-

cation strategy employed. This dual-role of trust enables a more nuanced and context-sensitive approach to security, allowing authentication protocols to be dynamically adjusted based on the trustworthiness of the agents involved.

### 3 ADAPTIVE TRUST-BASED AUTHENTICATION

In this section, we present the decision-making process used to select the agents to be authenticated, and to determine the level of security required for each authentication by selecting the factors to be used. The IoT offers a diversity of authentication factors; for instance, IoT sensors can collect real-time data from their environment and other objects where agents are deployed, providing valuable information that can be leveraged for authentication. (Saideh et al., 2024) have illustrated the relevance of opportunistic use of sensors deployed in related systems to make authentication based on a single RFID tag more reliable in the context of access control to a parking lot. Data collected by sensors can thus represent authentication factors. We propose to develop a strategy for selecting the most appropriate authentication factors according to specific criteria.

#### 3.1 General Architecture

We introduce specific components for trust-based authentication, designed to be integrated into application agents within an embedded MAS, as shown in Figure 1. Each agent is equipped with sensors and/or actuators, enabling it to perceive its environment, perform actions and communicate with others. Agents vary in terms of computing power, storage capacity and energy resources, reflecting the diversity of IoT environments.

The environment in which agents evolve is characterized by its dynamic nature and the occurrence of unpredictable events. We focus on the types of environment where agents can be led to simultaneously receive the same type of information from several agents. However, the veracity of this information is sometimes variable and may indicate malicious behavior or an attack attempt by one or more agents.

A trust management system enables agents to evaluate and update the trust values they assign to other agents, based on past interactions and the quality of shared information. Although the choice of trust management system is not the main focus of our paper, it does represent an important decision to be made when implementing the application agent.

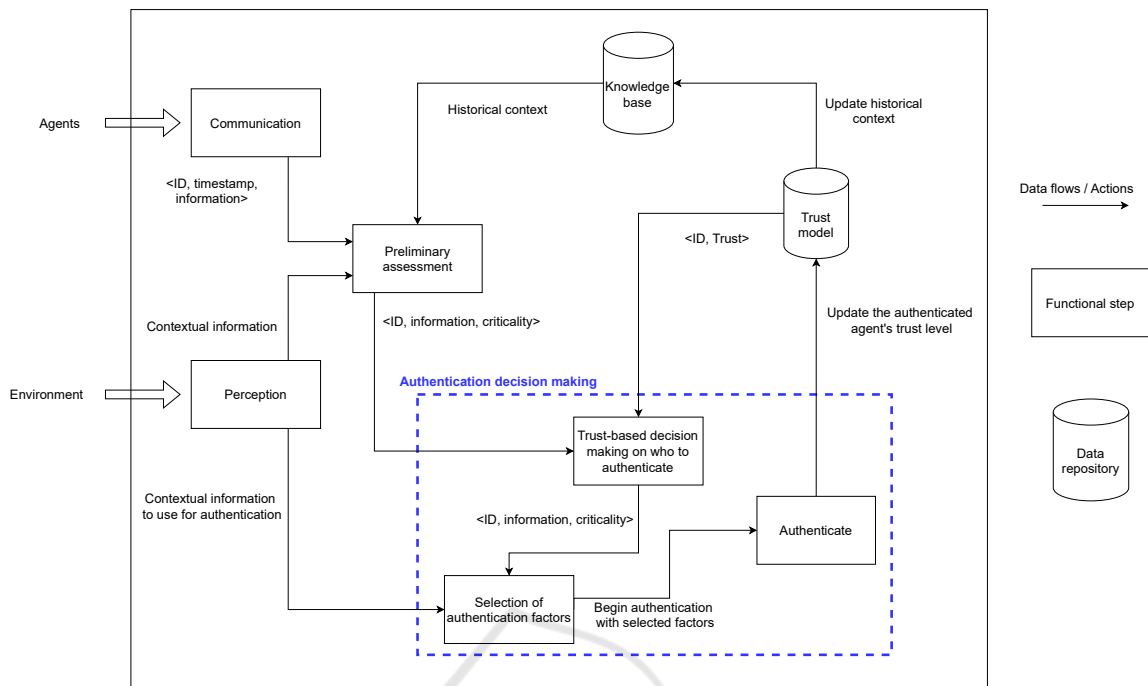


Figure 1: Components related to authentication and trust management.

The decision-making process proposed in this article enables agents to evaluate the trustworthiness of messages based on the trust assigned to the sender’s identity, dynamically adjusting the authentication rigor accordingly. By considering the risk and resource requirements, the process ensures that agents are authenticated only when necessary, balancing security with the need to optimize energy, computation, and communication resources. This approach is designed to meet the specific constraints of IoT environments, providing an efficient solution that maintains security while minimizing resource consumption.

In this model, authentication specifically aims to verify the identity of the agent sending the message. Each message sent by an agent includes essential information such as the agent’s unique identifier (a declared identifier), a timestamp indicating when the message was sent, and the data content, which varies according to the agent’s purpose and the nature of the information being shared.

### 3.2 Attack Model

In our study, we focus on impersonation attacks, a critical security concern in multi-agent systems and IoT environments. An impersonation attack occurs when a malicious agent pretends to be a legitimate agent by claiming its identity. This type of attack undermines the trust model by allowing the attacker to

exploit the trusted identity of another agent. The consequences of successful impersonation attacks are severe:

- **Data manipulation:** the attacker can alter or inject false information, leading to incorrect data being propagated through the system.
- **Communication disruption:** by pretending to be a legitimate agent, the attacker can interfere with or disrupt ongoing communications and transactions.
- **Reputation damage:** the trustworthiness of legitimate agents can be compromised, damaging their reputation and the overall integrity of the system.

To counter impersonation attacks, IoT systems must implement robust authentication mechanisms capable of detecting and mitigating identity theft and the abuse of multiple identities.

### 3.3 Trust-Based Authentication Decision-Making Process

The purpose of the decision-making process presented here is for an agent to perform authentication, thereby assuming the role of the *truster* to confirm or deny the identity of another agent. All parameters and functions used in the AAT model are summarized in Table 1. This process unfolds in five steps, each of

which may contain several sub-stages, as detailed below. Figure 2 illustrates this decision-making process, which comprises the following stages:

1. **Receiving Messages.** The process starts when a *truster* agent receives messages from other agents. These messages can be pre-processed by the *truster* agent before authenticating their senders. This pre-processing can be justified, for example, when latency is a critical constraint and immediate verification could delay urgent responses required for system operation. In our study, this pre-processing is mainly used to assess the criticality level of shared information.
2. **Trust Evaluation.** We define two trust thresholds: a minimum trust threshold,  $\Theta_{min}$ , at which the *truster* agent accepts to deploy resources for authentication, and a high trust threshold,  $\Theta_{high}$ , at which we consider the agent to be trustworthy. For each message received, three scenarios are considered based on the level of trust placed in the claimed identity:
  - If the claimed identity is that of a trustworthy agent (trust level greater than  $\Theta_{high}$ ), the *truster* agent performs a preliminary assessment of the criticality of the information received. It then compares this information, where appropriate, with other messages received in the same context from other agents claiming trustworthy identities. This comparison of information is intrinsically linked to the specific application in which the agents are deployed, underlining the importance of an adapted methodological approach.
  - If the claimed identity is that of an agent the *truster* does not trust (trust level below  $\Theta_{min}$ ), the authentication process can be bypassed. This is because the *truster* agent would not consider the shared information reliable regardless, due to the insufficient trust in the sender's claimed identity.
  - If the level of trust attached to the claimed identity is uncertain (trust level between  $\Theta_{min}$  and  $\Theta_{high}$ ) due to a lack of direct interactions or third-party feedback, a medium security level is applied for identity verification. Alternatively, authentication can be disregarded if other messages on the same information from trustworthy identities are available.
3. **Consistency Check.** This step is essential when the *truster* agent receives multiple messages about the same information from agents claiming trustworthy identities, and is particularly relevant to the specific application. For example, consider re-

Table 1: Overview of parameters and functions in the authentication decision process.

Parameter/Function	Description
$\Theta_{min}$	Minimum trust threshold to justify an authentication.
$\Theta_{high}$	High trust threshold indicating a trustworthy agent.
$\tau_{min}$	Minimum criticality threshold to justify an authentication.
$Trust$	Trust value in the claimed identity of the sender.
$Crit$	Criticality level of shared information.
$w_{FAR}$	Weight for False Acceptance Rate (FAR).
$w_{EC}$	Weight for Energy Cost (EC).
$M_{FAR}$	Maximum allowable weight for $w_{FAR}$ .
$a, b$	Coefficients balancing the impact of $Trust$ and $Crit$ .
$Score_{FAR}$	Weighted average FAR across utilized factors.
$Score_{EC}$	Sum of energy costs of all utilized factors.
$Score_{Global}$	Overall score for the selected set of factors.

ceiving several messages indicating the temperature at a specific location. If the information is inconsistent, there is a suspicion of a possible attack, leading to the authentication of all agents. If the information is consistent, the *truster* agent selects a subgroup of agents for thorough authentication. We assume that it is highly unlikely that all agents in the initial group are compromised simultaneously while sharing consistent information, thus reducing the number of agents needed for authentication without significantly impacting security.

4. **Authentication.** For each agent in the selected group, following the trust evaluation and consistency check phases, an appropriate security level is determined for authentication. This level is determined based on several key criteria, including the level of trust associated with the claimed identity and the criticality of the shared information. We assume the availability of a diverse set of authentication factors, each offering specific trade-offs between energy cost, security robustness, and False Acceptance Rate (FAR). The objective here is to select the optimal combination of factors according to these criteria. To achieve this, we define :
  - *Trust*: Trust value in the claimed identity by the agent seeking authentication,  $Trust : id \rightarrow [\Theta_{min}, 1]$ , where  $\Theta_{min}$  is the minimum trust threshold to justify authentication, and 1 represents the maximum trust level.
  - *Crit*: The criticality level of the shared information,  $Crit : info \rightarrow [\tau_{min}, 1]$ , where  $\tau_{min}$  is the minimum criticality threshold to justify authentication, and 1 is the maximum criticality level.
  - $w_{FAR}$  and  $w_{EC}$ : Weights for FAR and Energy

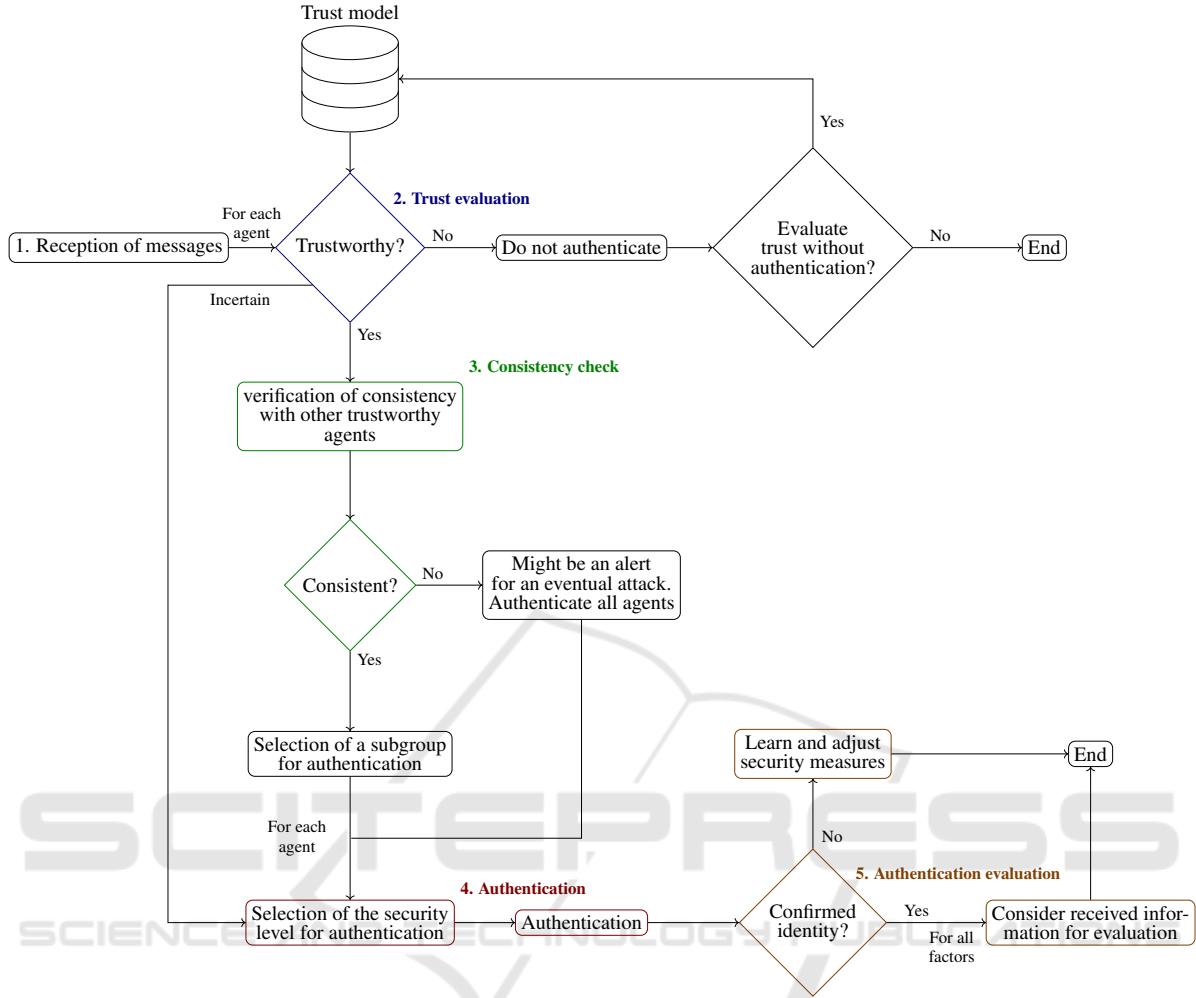


Figure 2: Diagram of authentication decision-making process.

Cost (EC), calculated as follows:

$$w_{FAR} = \min(M_{FAR}, a \times Trust + b \times Crit) \quad (1)$$

$$w_{EC} = 1 - w_{FAR} \quad (2)$$

where,  $a + b = 1$ ,  $M_{FAR}$  denotes the maximum allowable weight for  $w_{FAR}$ , while  $a$  and  $b$  serve as adjustable coefficients aimed at balancing the impact of  $Trust$  and  $Crit$  on both security and cost considerations.

- $Score_{FAR}$ : Calculated as the weighted average FAR across all utilized factors.

$$Score_{FAR} = \sum_{i=1}^n w_i \times FAR_i \quad (3)$$

where  $\sum_{i=1}^n w_i = 1$ ,  $FAR_i$  is the FAR of the  $i$ -th authentication factor in the combination, and  $w_i$  are the weights assigned to each factor, which may be equal or vary according to other criteria.

- $Score_{EC}$ : Calculated as the sum of the energy costs of all utilized factors.

$$Score_{EC} = \sum_{i=1}^n cost_i \quad (4)$$

where  $cost_i$  represents the energy cost of the  $i$ -th authentication factor in the combination. These scores must be normalized to ensure that all components contribute in a balanced way to the overall evaluation.

- $Score_{Global}$ : The overall score assigned to the selected set of factors.

$$Score_{Global} = w_{FAR} \times Score_{FAR} + w_{EC} \times Score_{EC} \quad (5)$$

The objective is to minimize the global score  $Score_{Global}$ . A low  $Score_{Global}$  indicates an effective combination of low FAR and low energy cost, demonstrating optimal performance of the authentication system in terms of security and energy efficiency.

5. **Authentication Evaluation.** In this phase, after selecting the authentication factors to verify the agent's identity, we assess whether the agent has successfully responded to all chosen factors. If the agent meets the authentication requirements, the *truster* accepts the claimed identity sent at the beginning of the interaction as authentic. Consequently, the information shared in the message is considered valid and is used for further evaluation and updates to the trust level. If the agent fails to respond to the required authentication factors, the identity is deemed unverified, and the received information is disregarded. This ensures that only authenticated agents can influence the decision-making process and trust assessments.

## 4 IMPLEMENTATION AND EVALUATION

To validate our AAT model, we implemented a simulation of an IoT environment that represents a multi-agent navigation scenario. This scenario is ideal for evaluating our mechanism due to the dynamic nature of the environment, where agents rely on information from other agents to navigate efficiently. The simulation was developed using the MESA agent-based framework (Kazil et al., 2020). AAT, which includes a trust evaluation model and an adaptive authentication process, has been fully integrated into this simulation. Each IoT device is represented as an autonomous agent capable of dynamically evaluating trust levels and making authentication decisions based on the criteria in our model.

### 4.1 Multi-Agent Navigation Scenario

#### 4.1.1 Environment

The navigation space is represented as a 2D grid that serves as a map, providing a spatial framework for the agents' movements. Obstacles are strategically or randomly placed on the map, marking positions that agents cannot cross. The environment is characterized by dynamic events, including shifts in obstacle positions or the introduction of new obstacles, which contribute to its inherent uncertainty.

#### 4.1.2 Agents

The MAS is open, allowing dynamic entry and exit of agents. We distinguish two types of agent in our simulation:

1. **Navigators.** A *navigator* agent is an autonomous agent randomly placed on the map and endowed with navigation capabilities. Its objective is to reach a specific, unknown destination while minimizing the navigation distance. It has limited knowledge of the map, being able to detect only its immediate surroundings, which includes all the cells adjacent to the one where it is located on the map.
2. **Guides.** A *guide* agent is an autonomous agent that has no physical presence on the map, but has global knowledge of the map, including the position of obstacles and the destinations of the *navigators*. The guides communicate with navigators, transmitting essential information such as the locations of obstacles and the designated destinations, helping them navigate the map more efficiently and safely.

### 4.2 Interaction and Collaboration

The *guides* communicate the location of obstacles on the map and the destinations to be reached to each *navigator*. The *navigators*, relying on this interaction to obtain the necessary information for navigation, evaluate the information received based on their trust in the *guides* to make decisions about their route on the map. Consequently, information about the same object (map and destinations) is received from different *guides*.

#### 4.2.1 Trust

In our simulation, *navigators* use the Beta Reputation System (BRS) (Josang and Ismail, 2002) to evaluate the trustworthiness of *guides* based on their past actions. Other trust management models can be used, as the choice of trust model is not the central contribution of our article. BRS uses the positive and negative results of previous interactions to calculate the probability that an agent will act reliably in the future. Mathematically, the trust value of an agent in BRS is calculated using the following formula:

$$Trust = \frac{\alpha}{\alpha + \beta} \quad (6)$$

$$\alpha = r + 1 \text{ and } \beta = s + 1 \quad (7)$$

where  $r$  and  $s$  respectively represent the number of positive and negative interactions an agent *truster* has had with the trustee in question. This formula provides an estimate of the probability that the agent will behave honestly in a future

Table 2: Artificial authentication factors.

Factor	Energy cost (mJ)	Security level	TNR	FAR
1	0.2	Low	0.85	0.15
2	3.0	High	0.98	0.02
3	1.5	Medium	0.92	0.08
4	2.6	High	0.97	0.03
5	0.8	Medium	0.89	0.11
6	0.6	Low	0.88	0.12
7	2.0	High	0.95	0.05
8	1.2	Medium	0.90	0.10

interaction. A value close to 1 indicates high reliability, while a value close to 0 suggests low reliability.

In our scenario, a negative interaction occurs when a *navigator* receives incorrect information about the map from a *guide*. For instance, if the map provided by the *guide* contains inaccuracies, such as erroneous obstacle positions or incorrect destinations, this constitutes a negative interaction. Such inaccuracies can significantly impact the *navigator's* ability to navigate effectively, leading to a negative evaluation of the *guide's* trustworthiness.

Conversely, a positive interaction is characterized by accurate information—where the map reflects the correct positions of obstacles and destinations, allowing the *navigator* to proceed. The trust level of a guide is thus influenced by the quality of the information they provide.

Given that *navigators* can detect inaccuracies in obstacle positions more rapidly than errors in destination information, we introduce a weight  $w_\beta$  to the parameter  $\beta$  to more strongly penalize *guides* who provide incorrect destination information. This weighting reflects the greater impact of destination inaccuracies on navigation effectiveness and trust. By applying this penalty, we aim to prevent *guides* from maintaining a high trust score if they provide accurate obstacle information but frequently share incorrect destination details.

#### 4.2.2 Authentication

*Navigator* agents use the AAT model proposed in section 3 to authenticate *guide* agents. We have defined several artificial authentication factors for the simulation in Table 2. Each factor is abstractly represented by its energy cost, the level of security it provides, and the True Negative Rate (TNR), with  $FAR = 1 - TNR$ . Security levels are classified into three categories: low, medium, and high. The factors are defined such that their energy cost increases proportionally with the level of security. Depending on the adopted strategy, an agent selects authentication

factors in various ways from the available options. The three authentication strategies used in our simulation are:

- Static Authentication (SA): this method uses the same two factors for all agents. The selection of these factors follows a traditional approach, combining a low-security factor with a medium or a high-security factor.
- Adaptive Authentication based on the Criticality of Shared Information (AAC): an adaptive method that selects authentication factors based on the level of criticality of the shared information, without incorporating trust values.
- Adaptive Authentication based on Trust and criticality (AAT): This method, which represents our authentication decision-making process, utilizes trust levels to decide which identities to authenticate and combines trust and criticality values to select appropriate authentication factors.

### 4.3 Results and Evaluation

We describe here the results obtained by running our simulation over 200 episodes. Each episode begins with the initialization of the environment and the placement of the *navigators* on the map, and ends when all the *navigators* have reached their destinations. In each episode, the *guides* provide the *navigators* with information about the map. The latter authenticate the messages received and evaluate and update the trust values during navigation. We simulated 3 *navigator* agents, each adopting a different authentication strategy among the three strategies detailed previously, and 10 *guide* agents, 6 of them malicious, sharing erroneous map information.

#### 4.3.1 Resource Efficiency

Figure 3 illustrates the cumulative energy consumption over 200 episodes using the three authentication strategies for a *navigator* communicating with 10 *guides* per episode.



Table 3: Number of successful attacks and average steps per episode over 200 episodes.

	AAT	AAC	SA
<b>Number of successful attacks</b>	9	14	17
<b>Successful attack rate</b>	2.25%	3.5%	4.25%
<b>Average steps per episode (20 being the optimal)</b>	22	25	27

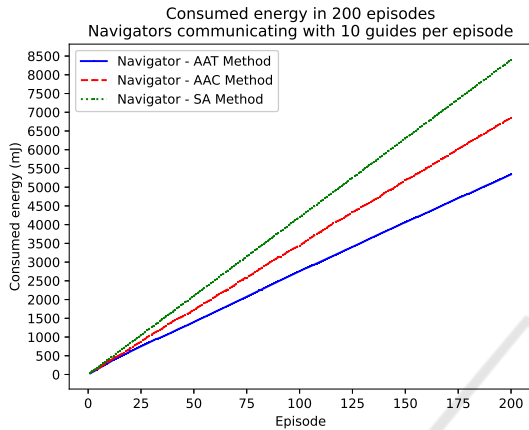


Figure 3: Energy consumed for authentication in 200 episodes.

Our proposed trust-based authentication decision process AAT reduces energy consumption by 19% compared with the AAC method, which does not consider trust, and by 37% compared with the SA method, which employs static authentication for all agents, resulting in linear energy consumption due to repeated use of the same factors at each authentication.

By avoiding authentication of agents with whom previous interactions have provided sufficient but inconclusive trust information, and by adapting authentication factors based on established trust and the criticality of exchanged information, we enhance energy efficiency. Authentication occurs only when the risk justifies the energy expenditure. This approach allows resources to be focused where they provide the most value, directly contributing to observed energy savings.

#### 4.3.2 Impact on Security

We simulated identity impersonation attacks based on the FARs of the artificial authentication factors (Table 2). Over 200 episodes, a total of 2,000 interactions were recorded, including 400 unauthorized attempts. The simulation was structured to evaluate attackers' attempts to impersonate trusted *guide* agents. Each successful attack attempt allows the

attacker to transmit erroneous map information to the *navigators*, leading to misguided paths. Table 3 summarizes the number of successful attacks and their corresponding impact on the number of steps required for *navigators* to reach their destinations. Specifically, when a *navigator* accepts an incorrect map sent by an attacker, the number of steps required to reach the destination can increase to over 50. This impact may not always be apparent in the average steps per episode, due to the relatively small number of successful attacks compared to the total interactions. Overall, AAT performs better in terms of detecting malicious agent attacks, preventing 97.75% of them, compared with 96.5% and 95.75% for competing models (Table 3).

The complementary nature of resource efficiency and security in our proposed AAT framework highlights its overall effectiveness. By significantly reducing energy consumption while maintaining a high level of security, AAT demonstrates that efficient resource usage does not come at the expense of security integrity. The ability to adaptively authenticate based on trust not only conserves resources but also enhances the system's resilience against impersonation attacks. This dual benefit underscores the value of our approach, illustrating how optimizing one aspect can simultaneously bolster another, ultimately leading to a more robust and sustainable multi-agent system in IoT environments. Specifically, only 2.25% of malicious agent attacks were successful in AAT, compared with 3.5% and 4.25% for other less adaptive models. Furthermore, AAT significantly reduces energy costs, achieving savings of 19% to 37% compared to less adaptive methods.

To further enhance the effectiveness and applicability of the AAT framework, future experiments could focus on testing its performance across diverse contexts and applications. For instance, evaluating the system in varying IoT environments, such as industrial, healthcare, and smart home settings, could provide deeper insights into its adaptability and reliability. Additionally, the computational cost of the decision process algorithm should be rigorously ana-

lyzed to ensure that the benefits of resource efficiency do not come at the expense of scalability or real-time responsiveness. Another critical avenue for improvement involves developing and simulating strategic attack methods, such as coordinated multi-agent impersonation or evolving adversarial strategies, to test the resilience of the framework. These refinements would not only validate the robustness of the AAT model but also identify potential areas for optimization, allowing more comprehensive and future-proof solutions.

## 5 CONCLUSIONS

In this paper, we presented a novel trust-based adaptive authentication decision process designed for the dynamic and heterogeneous environments of the Internet of Things. Specifically developed for information exchange within embedded MAS, this process dynamically adjusts the required security level for authentication based on both the trustworthiness of the claimed identity by the sender and the criticality of the transmitted information. By evaluating trust levels and criticality, the process selects which identities to authenticate and employs the most effective combination of authentication factors. This approach optimizes resource allocation while minimizing the false positive rate.

The effectiveness of our model is demonstrated by the results obtained in the multi-agent navigation simulations, which showed a significant reduction in the success rate of malicious agent attacks compared to other, less adaptive models. Additionally, our approach demonstrates a marked improvement in resource efficiency, allowing for the intelligent use of energy and computational resources. This highlights that our adaptive authentication strategy not only enhances security by foiling more attacks — particularly by strengthening authentication for trustworthy agents — but also optimizes resource utilization by minimizing unnecessary authentications.

The integration of trust management and adaptive authentication mechanisms in IoT and embedded MAS represents a promising direction for enhancing security. By leveraging the strengths of both approaches, it is possible to create systems that are more resilient to attacks and better suited to the dynamic and resource-constrained environments typical of IoT and MAS. Our future work will focus on the following three main areas: validating our model using real rather than artificial authentication factors, developing a trust management system with a more sophisticated strategy for selecting authentication factors, and expanding our model to address other types of

identity-related attacks. These improvements will enhance the model's robustness and flexibility against a broader range of threats, while dynamically optimizing agent authentication processes and trust relationships in IoT environments.

## ACKNOWLEDGEMENTS

This work is supported by the French National Research Agency (ANR) in the framework of the project MaestrIoT ANR-21-CE23-0016.

## REFERENCES

- Arfaoui, A., Cherkaoui, S., Kribeche, A., Senouci, S. M., and Hamdi, M. (2019). Context-aware adaptive authentication and authorization in internet of things. In *ICC 2019-2019 IEEE International Conference on Communications (ICC)*, pages 1–6. IEEE.
- Arias-Cabarcos, P., Krupitzer, C., and Becker, C. (2019). A survey on adaptive authentication. *ACM Computing Surveys (CSUR)*, 52(4):1–30.
- Babun, L., Denney, K., Celik, Z. B., McDaniel, P., and Uluagac, A. S. (2021). A survey on iot platforms: Communication, security, and privacy perspectives. *Computer Networks*, 192:108040.
- Dasgupta, D., Roy, A., and Nag, A. (2016). Toward the design of adaptive selection strategies for multi-factor authentication. *computers & security*, 63:85–116.
- El-Hajj, M., Fadlallah, A., Chamoun, M., and Serhrouchni, A. (2019). A survey of internet of things (iot) authentication schemes. *Sensors*, 19(5):1141.
- Feng, X., Wang, X., Cui, K., Xie, Q., and Wang, L. (2023). A distributed message authentication scheme with reputation mechanism for internet of vehicles. *Journal of Systems Architecture*, 145:103029.
- Jahangeer, A., Bazai, S. U., Aslam, S., Marjan, S., Anas, M., and Hashemi, S. H. (2023). A review on the security of iot networks: From network layer's perspective. *IEEE Access*, 11:71073–71087.
- Jamont, J.-P. and Ocelllo, M. (2015). Meeting the challenges of decentralised embedded applications using multi-agent systems. *International Journal of Agent-Oriented Software Engineering*, 5(1):22–68.
- Josang, A. and Ismail, R. (2002). The beta reputation system. In *Proceedings of the 15th Bled Electronic Commerce Conference*, volume 5, pages 2502–2511.
- Kaur, B., Dadkhah, S., Shoeleh, F., Neto, E. C. P., Xiong, P., Iqbal, S., Lamontagne, P., Ray, S., and Ghorbani, A. A. (2023). Internet of things (iot) security dataset evolution: Challenges and future directions. *Internet of Things*, 22:100780.
- Kazil, J., Masad, D., and Crooks, A. (2020). 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.
- Khanpara, P., Lavingia, K., Trivedi, R., Tanwar, S., Verma, A., and Sharma, R. (2023). A context-aware internet of things-driven security scheme for smart homes. *Security and Privacy*, 6(1):e269.
- Koohang, A., Sargent, C. S., Nord, J. H., and Paliszkiwicz, J. (2022). Internet of things (iot): From awareness to continued use. *International Journal of Information Management*, 62:102442.
- Mall, P., Amin, R., Das, A. K., Leung, M. T., and Choo, K.-K. R. (2022). Puf-based authentication and key agreement protocols for iot, wsns, and smart grids: a comprehensive survey. *IEEE IoT Journal*, 9(11):8205–8228.
- Meneghello, F., Calore, M., Zucchetto, D., Polese, M., and Zanella, A. (2019). Iot: Internet of threats? a survey of practical security vulnerabilities in real iot devices. *IEEE Internet of Things Journal*, 6(5):8182–8201.
- Miettinen, M., Nguyen, T. D., Sadeghi, A.-R., and Asokan, N. (2018). Revisiting context-based authentication in iot. In *Proceedings of the 55th Annual Design Automation Conference*, pages 1–6.
- Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., and Koucheryavy, Y. (2018). Multi-factor authentication: A survey. *Cryptography*, 2(1):1.
- Pham, T. N. D. and Yeo, C. K. (2018). Adaptive trust and privacy management framework for vehicular networks. *Vehicular Communications*, 13:1–12.
- Pinyol, I. and Sabater-Mir, J. (2013). Computational trust and reputation models for open multi-agent systems: a review. *Artificial Intelligence Review*, 40(1):1–25.
- Pourghbleh, B., Wakil, K., and Navimipour, N. J. (2019). A comprehensive study on the trust management techniques in the internet of things. *IEEE Internet of Things Journal*, 6(6):9326–9337.
- Ryu, R., Yeom, S., Herbert, D., and Dermoudy, J. (2023). A comprehensive survey of context-aware continuous implicit authentication in online learning environments. *IEEE Access*, 11:24561–24573.
- Sabater-Mir, J. and Vercouter, L. (2013). *Trust and Reputation in Multi-Agent Systems*, pages 381–419. Number 9. MIT Press, g. weiss edition.
- Sahoo, S. S., Veeravalli, B., and Kumar, A. (2019). A hybrid agent-based design methodology for dynamic cross-layer reliability in heterogeneous embedded systems. In *Proceedings of the 56th Annual Design Automation Conference 2019*, pages 1–6.
- Saideh, M., Jamont, J.-P., and Vercouter, L. (2024). Opportunistic sensor-based authentication factors in and for the internet of things. *Sensors*, 24(14):4621.
- Sharma, A., Pilli, E. S., Mazumdar, A. P., and Gera, P. (2020). Towards trustworthy internet of things: A survey on trust management applications and schemes. *Computer Communications*, 160:475–493.
- Sobin, C. (2020). A survey on architecture, protocols and challenges in iot. *Wireless Personal Communications*, 112(3):1383–1429.
- Vercouter, L. and Jamont, J.-P. (2012). Lightweight trusted routing for wireless sensor networks. *Progress in Artificial Intelligence*, 1:193–202.
- Yu, H., Shen, Z., Leung, C., Miao, C., and Lesser, V. R. (2013). A survey of multi-agent trust management systems. *IEEE Access*, 1:35–50.
- Zhang, F., Kondoro, A., and Muftic, S. (2012). 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.