Adaptive Authentication Factor Selection in the Internet of Things: A Trust-Based Multi-Objective Optimization Approach

Marc Saideh
INSA Rouen Normandie, Normandie Université, LITIS UR 4108
76000 Rouen, France
marc.saideh@insa-rouen.fr

Jean-Paul Jamont
Université Grenoble Alpes, LCIS
26000 Valence, France
jean-paul.jamont@lcis.grenoble-inp.fr

Laurent Vercouter
INSA Rouen Normandie, Normandie Université, LITIS UR 4108
76000 Rouen, France
laurent.vercouter@insa-rouen.fr

ABSTRACT

Multi-Agent Systems (MAS) deployed in the Internet of Things (IoT) face significant security challenges due to device heterogeneity and dynamic environments. Traditional authentication mechanisms often fail to address the various trade-offs that arise in resource-constrained environments, which are critical for IoT systems. To address this, we propose a trust-based, multi-objective optimization framework for adaptive authentication factor selection in IoT. Our approach leverages the Non-Dominated Sorting Genetic Algorithm II (NSGA-II) to optimize the security, energy efficiency, and delay of the authentication factors. Trust is integrated into the optimization model as a guiding parameter to enable a more adaptive and context-aware selection process, ensuring that requirements and resource consumption are tailored to the specific context of each authentication instance. Simulation results demonstrate that our framework enhances security while optimizing resource consumption.

KEYWORDS

Multi-Agent Systems, Internet of Things, Authentication, Trust, Multi-Objective Optimization

1 INTRODUCTION

The rapid expansion of the Internet of Things (IoT) has introduced significant challenges in security, scalability, and decision-making. IoT environments consist of a vast number of interconnected devices, ranging from simple sensors to edge computing nodes, operating in highly dynamic and resource-constrained environments. These constraints, such as limited processing power, energy, and communication bandwidth, necessitate adaptive and efficient security mechanisms. However, conventional security solutions designed for traditional networks are often not well suited for IoT, as they impose excessive computational overhead and fail to adapt to the heterogeneous and evolving nature of IoT systems. To address these limitations, this paper proposes a framework that dynamically optimizes authentication decisions in IoT by integrating trust-based reasoning with multi-objective resource management.

A fundamental challenge in securing IoT environments lies in the decision-making process governing authentication and trust management [32]. In distributed IoT networks, Multi-Agent Systems (MAS) offer a promising approach to model interactions among autonomous devices [10, 13]. Each agent can represent an IoT object capable of making decisions, exchanging information, and collaborating with other agents to achieve specific goals. However, the decentralized nature of MAS introduces risks. For instance, agents relying on peer-provided data or services must efficiently decide before engaging in interactions: Can I trust this agent? Is it who it claims to be? This makes trust a critical component in managing security and cooperation in MAS. It enables agents to assess the reliability of other agents based on past interactions, observed behavior, or shared reputations [29]. However, relying solely on trust for decision-making is insufficient if malicious agents can exploit trust by impersonating high-trust agents and compromising the security of the system. To mitigate this risk, authentication mechanisms are required to validate the identity of agents, ensuring that trust is assigned to legitimate agents and interactions remain secure.

Traditional authentication schemes often rely on static methods that apply fixed security measures without considering the dynamic and heterogeneous nature of IoT environments [8]. Such static approaches are inefficient and fail to address the trade-offs inherent in IoT systems, where authentication must balance conflicting objectives, such as security, energy consumption and quality of service [23]. These trade-offs are particularly significant in resource-constrained environments, where unnecessary authentication overhead can drain device resources or disrupt real-time applications. The interdependence between trust and authentication has been highlighted in [31], demonstrating how authentication strengthens trust relationships while trust can guide authentication decisions. By leveraging this feedback loop, adaptive authentication strategies can be designed to dynamically select authentication factors based on contextual trust values, optimizing security while minimizing resource consumption.

This paper introduces a novel framework that integrates Multi-Objective Optimization (MOO) with trust-based decision-making to optimize authentication strategies in resource-constrained and dynamic IoT environments. The proposed approach formulates authentication as a multi-objective problem, where security, energy consumption, and delay are optimized simultaneously. Using trust as a guiding parameter, the framework dynamically selects authentication factors, ensuring that authentication decisions adapt to the heterogeneous and resource-constrained nature of IoT environments.

The main contributions of this work are as follows:

(1) Proposing a dynamic framework for multi-objective optimization of authentication factor selection, balancing security, energy consumption, and delay using the elitist Non-dominated Sorting Genetic Algorithm (NSGA-II).
(2) Integrating trust as a guiding parameter in decision-making to dynamically select optimal authentication solutions.

Proc. of the Adaptive and Learning Agents Workshop (ALA 2025), Avalos, Aydeniz, Müller, Mohammedalamen (eds.), May 19 – 20, 2025, Detroit, Michigan, USA, ala-workshop.github.io. 2025.

The rest of this paper is organized as follows. Section 2 reviews existing work on security in IoT, trust management, and multi-objective optimization. Section 3 describes the optimization model in details, including the optimization flow and the nature of authentication factors before formalizing the problem. Section 4 presents the simulation setup, results, and performance analysis. Finally, Section 5 concludes with insights into the contributions and outlines directions for future research.

2 BACKGROUND AND RELATED WORK

This section outlines the security challenges in IoT, emphasizing the need for adaptive authentication mechanisms. We review trust management systems as a foundation for context-aware security decisions and explore multi-objective optimization techniques to address conflicting objectives. Table 1 groups and summarizes the main lines of related research in IoT security, trust management, and multi-objective optimization, highlighting their collective approaches and contributions.

2.1 Security in IoT

Security in IoT is inherently a multi-objective problem, requiring a trade-off between security, efficiency, and usability [23]. Among the various security mechanisms, authentication plays a crucial role in ensuring that interactions occur between legitimate entities while minimizing overhead on resource-constrained IoT devices [19]. Unlike traditional computing environments, IoT devices operate under strict energy, processing, and latency constraints, making static authentication approaches impractical [8].

Extensive research has explored these security challenges and proposed protective measures to mitigate threats [4, 12, 14, 19]. A widely studied approach is Multi-Factor Authentication (MFA), which strengthens security by combining two or more independent authentication factors. These factors are generally categorized into knowledge-based (e.g., passwords), possession-based (e.g., security tokens), and inherent characteristics (e.g. biometric verification) [21].

To further enhance security while maintaining efficiency, recent MFA advancements have focused on adaptive and context-aware authentication [3, 20, 21]. Adaptive MFA dynamically adjusts authentication requirements based on the assessed risk level of an access attempt, reducing unnecessary overhead while maintaining security. Similarly, context-aware models incorporate additional information such as user behavior, time, location, and interaction history to refine authentication decisions [2, 16, 28]. Moreover, the potential of IoT in enabling opportunistic authentication factors based on available sensors and contextual data was highlighted in [30]. This underscores the need for adaptive techniques capable of dynamically selecting the most appropriate authentication mechanisms.

2.2 Trust Management in IoT for Security

Trust management plays a critical role in securing IoT systems, where agents interact while facing constraints in computational and energy resources. In a trust relationship, there are two roles: the truster, who relies on information or service provided by another agent, and the trustee, the agent who provides the service or action to the truster [29]. Trust can be evaluated using direct or indirect feedback derived from interactions. Direct trust refers to the trust that a truster places in a trustee based on their own interactions, while indirect trust is formed through feedback the truster receives from third parties about the trustee [26].

The literature demonstrates increasing attention to trust management as a key element of IoT security. Studies [17, 27, 32] emphasize the crucial role of trust in addressing the complexities and vulnerabilities present in IoT networks. These works underline the need to move away from static security models and adopt more adaptive, context-aware frameworks that can respond dynamically to evolving threats and conditions. Adaptive trust management systems, for example, can adjust trust assessments in real-time, enhancing security flexibility and resilience [25]. Similarly, authors in [9] integrate trust and reputation mechanisms into their authentication scheme for the Internet of Vehicles, stressing the importance of these factors in ensuring secure and reliable communication.

2.3 Multi-Objective Optimization for Security

MOO has emerged as a powerful tool for addressing the conflicting requirements of IoT systems, such as balancing security, resource consumption and quality of service. Given the resource constraints in IoT environments, optimizing these trade-offs is crucial for maintaining efficiency and robustness [23]. Unlike single-objective optimization, which yields a single optimal solution, MOO produces a set of Pareto-optimal solutions, each representing a unique trade-off between the objectives. A solution is said to be Pareto-optimal if no objective can be improved without worsening at least one other objective. The set of all Pareto-optimal solutions forms the *Pareto front* that represents the set of non-dominated solutions in the objective space. By examining the Pareto front, decision-makers can select a solution that best aligns with system constraints and priorities.

Traditional methods for solving MOO problems, such as the weighted sum method, aggregate multiple objectives into a single weighted function [18]. While this method is computationally efficient, it requires precise weight tuning and may struggle to capture the full spectrum of trade-offs, especially in dynamic and uncertain IoT environments. This approach also necessitates a predefined trade-off, which may not generalize well across different scenarios.

In contrast, evolutionary algorithms, such as Genetic Algorithms (GA) and Particle Swarm Optimization (PSO), have been widely used to solve multi-objective problems in IoT [1, 5, 11]. These algorithms generate a set of Pareto-optimal solutions without requiring explicit weight assignments, enabling decision-makers to select the most appropriate trade-off. Several comparative studies of different multi-objective optimization methods [24, 33] have demonstrated that the Non-dominated Sorting Genetic Algorithm II (NSGA-II) [6] outperforms other methods by maintaining a well-distributed set of trade-off solutions and achieving better convergence towards the true Pareto front.

3 SYSTEM MODEL

The core problem addressed in this work is the challenge of selecting appropriate authentication factors in IoT environments while balancing conflicting requirements. In such environments,

Table 1: Grouped summary of related work in IoT security, trust management, and multi-objective optimization

Focus Area / Group	Representative Works	Approach/Method	Key Contributions/Insights
IoT Authentication & Security	[4, 8, 12, 14, 19]	Surveys and analysis of IoT authentication mechanisms	Overview of authentication challenges and solutions for resource-constrained IoT devices
Multi-Factor & Context-Aware Authentication	[2, 3, 16, 20, 21, 28, 30]	Adaptive/context-aware MFA, opportunistic authentication	Adaptive models leveraging context (user behavior, location, sensors) for enhanced security and usability
Trust Management in IoT	[9, 17, 25–27, 29, 32]	Trust modeling, adaptive trust management, reputation systems	Trust frameworks and adaptive mechanisms to improve security and reliability in IoT interactions
Multi-Objective Optimization	[1, 5, 6, 11, 18, 24, 33]	Weighted sum, evolutionary algorithms (GA, PSO, NSGA-II)	Application of MOO techniques to balance security, efficiency, and resource use in IoT environments

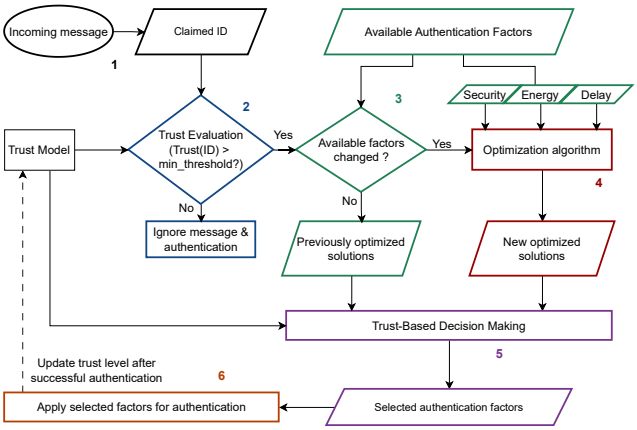


Figure 1: Optimization model workflow

devices exhibit diverse capabilities, and excessive authentication costs can degrade performance or even exhaust the resources of low-power devices. Conversely, choosing weak or minimal authentication undermines security. This creates the need for adaptive decision-making that considers both security requirements and resource constraints.

We consider a heterogeneous set of agents representing IoT objects, ranging from low-power sensors to more complex devices. Each agent is assigned a unique identifier (ID) and is capable of sending and receiving messages. For simplicity, we assume that received messages follow the format `(claimed_ID, content)`. The focus of the authentication process is on verifying the claimed identity within the message. Agents maintain and update trust values assigned to other agents through a trust management system, reflecting past interactions and the quality of exchanged information. Each agent independently evaluates trust levels, assesses authentication requests, and makes decisions based on its local knowledge and the optimization framework. While the specific choice of trust management system is beyond the scope of this paper, it remains an important design consideration when deploying the proposed framework.

3.1 Authentication Factors Attributes

The selection of authentication factors plays a critical role in balancing security, energy consumption, and delay. Each authentication factor impacts these objectives differently, and its selection is influenced by system constraints as well as the dynamic trust levels of agents.

We consider a diverse set of authentication factors, each characterized by three key attributes:

- Security Level (SL): Represents the robustness of the authentication factor against potential attacks. Higher values indicate stronger security.
- Energy Cost (E): Measures the total energy consumed when employing the authentication factor.
- Authentication Delay (D): Reflects the time required to complete the authentication process using the factor.

3.2 Authentication Process Workflow

The goal of the proposed optimization model is to dynamically select the most suitable authentication factors for each authentication while balancing multiple conflicting objectives: security, energy consumption and latency. Our framework leverages MOO to identify the different optimal trade-offs among possible authentication solutions, while trust-based decision-making determines both which agents should be authenticated and which trade-off to select. This aims to ensure that authentication resources are allocated efficiently, maintaining strong security while minimizing unnecessary overhead.

Figure 1 illustrates the workflow of the proposed optimization model, outlining the sequence of operations for adaptively selecting authentication factors. In the context of trust management, two agent roles are distinguished: the truster (who evaluates trust and makes authentication decisions) and the trustee (who provides a service and must be authenticated), as defined in Section 2. The optimization is performed from the truster's perspective, who must decide whether to authenticate a potential trustee and, if so, which combination of authentication factors to adopt. The optimization model has 3 inputs: (1.) the claimed identity to authenticate, (2.) the trust level associated with the claimed ID from the truster's perspective (retrieved from the trust model), and (3.) the set of

available authentication factors that can be used. The output of the optimization algorithm is the Pareto front of authentication solutions, where each solution represents a combination of a predefined number of authentication factors (MFA). The final decision-making step involves selecting one solution from the Pareto front, guided by trust, to authenticate the claimed ID. The key steps of the process are as follows:

1. Incoming Message: The optimization and decision-making process is triggered when an agent (truster) receives a message from another agent (potential trustee). The primary objective of authentication is to verify whether the *claimed_ID* accurately represents the sender's true identity. Upon receiving the message, the truster extracts the claimed identity and proceeds to assess whether authentication is necessary in the subsequent step.

2. Trust Evaluation: The truster evaluates the trustworthiness of the sender's `claimed_ID` based on the trust model. If the assigned trust value is below a predefined threshold Θ_{min}, the message is discarded, as interactions with untrustworthy entities are deemed unnecessary. Otherwise, authentication is initiated to verify the sender's identity before further processing the message.

3. Authentication Factor Availability Check: The truster verifies the set of available authentication factors. Since the optimization model derives a set of optimal solutions based on these factors, any change requires re-optimization. In dynamic IoT environments, factors may become unavailable due to power constraints (e.g., a biometric sensor) or new factors may emerge following device upgrades. If the set of available factors is unchanged, previously computed optimal trade-offs remain valid, allowing the process to proceed directly to trust-based decision-making. Conversely, any modification—such as a factor becoming unavailable, a new factor being introduced, or an update to an existing factor—triggers re-execution of the optimization process to generate an updated set of trade-offs.

4. Optimization Algorithm Execution: If the optimization algorithm must be executed—either during the initial run or due to changes in authentication factor availability—it takes as input the characteristics of the available authentication factors: (i) security level, (ii) energy consumption, and (iii) delay. The algorithm explores the trade-offs among these metrics, producing a Pareto front of optimal authentication solutions. Each solution represents a combination of two or three factors from the available set, enabling adaptive selection that aligns with system constraints while optimizing security, energy consumption, and latency.

5. Trust-Guided Decision Making: Based on the set of optimal authentication solutions generated by the optimization algorithm, the truster selects the most appropriate solution according to the trust value associated with the `claimed_ID`. High-trust claimed identities trigger the selection of stricter authentication solutions, prioritizing security to prevent potential trust exploitation through identity spoofing. This precaution is necessary to protect trust-dependent operations, ensuring that the claimed identity corresponds to the true sender. Conversely, lower-trust identities may justify selecting more lightweight, energy-efficient solutions, as the reliance on their information is already limited. The specific details of this selection process are further explained in subsection 3.4

6. Authentication Execution: Once the authentication solution is selected, the truster verifies whether the potential trustee satisfies the requirements of the chosen authentication factors. If the authentication is successful, the `claimed_ID` is accepted as authentic, and the message content is processed, contributing to future trust evaluations and updates. If authentication fails, the `claimed_ID` is considered unverified, and the message is discarded. This ensures that only authenticated agents can influence subsequent decisions and trust assessments within the system.

3.3 Problem Formulation

We model the selection of authentication factors as a multi-objective optimization problem aimed at balancing three competing objectives: maximizing security, minimizing energy consumption, and reducing authentication delay. Let $\mathcal{F}_{\text{avail}} = \{f_1, f_2, \ldots, f_n\}$ denote the set of available authentication factors, where each factor f_i is characterized by: SL_i (Security level of factor f_i), E_i (Energy consumption of factor f_i), D_i (Authentication delay associated with factor f_i).

The optimization problem is formulated as follows: given a set of available authentication factors F_{avail}, we aim to select a subset $A \subseteq F_{\text{avail}}$ that forms an MFA scheme while optimizing the following objectives:

$$\text{Maximize } SL(A) = \sum_{f_i \in A} SL_i \tag{1}$$

$$\text{Minimize } E(A) = \sum_{f_i \in A} E_i \tag{2}$$

$$\text{Minimize } D(A) = \sum_{f_i \in A} D_i \tag{3}$$

Subject to the constraints:

- A must contain at least one authentication factor: $|A| \geq 1$.
- The number of selected factors is constrained by system resources: $1 \leq |A| \leq k_{\max}$, where $k_{\max}$ is the upper limit on the number of factors an agent can handle simultaneously.
- Each selected factor must be available in the current context: $A \subseteq \mathcal{F}_{\text{avail}}$, where $\mathcal{F}_{\text{avail}}$ can change dynamically depending on environmental conditions and device capabilities.
- Each authentication factor can be used at most once in a single authentication solution:
  A is a set, meaning $\forall f_i, f_j \in A,\ i \neq j \Rightarrow f_i \neq f_j$.

In a MOO problem, it is generally impossible to find a single solution that optimizes all objectives simultaneously. Instead, the solution space consists of a set of Pareto-optimal solutions, where improving one objective often comes at the cost of another. To navigate these trade-offs, the final decision-making process will be guided by a trust-based approach, ensuring that the selected solution aligns with contextual priorities and dynamically balances the competing factors. NSGA-II is well-suited for the authentication factor selection problem formulated in the previous subsection due to three key characteristics: (i) *fast non-dominated sorting*, which efficiently ranks solutions based on dominance relations, (ii) *elitism preservation*, ensuring high-quality solutions are retained across generations, and (iii) *crowding-distance-based diversity maintenance*, which prevents premature convergence by promoting diversity in the Pareto front. Figure 2 illustrates the NSGA-II procedure. In the

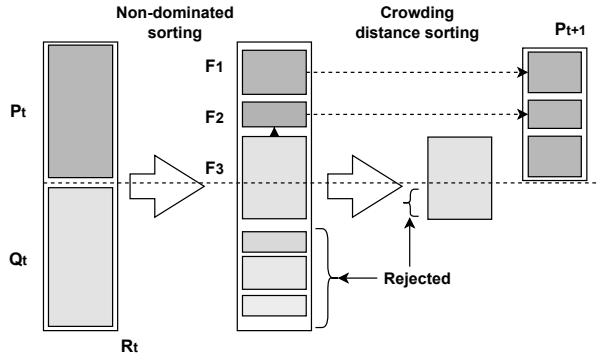


Figure 2: General structure of NSGA-II [6]

context of authentication factor selection, an individual in NSGA-II represents a specific combination of factors from $\mathcal{F}_{\text{avail}}$. Each individual is encoded as a subset $A \subseteq F_{\text{avail}}$, where the size of A corresponds to the chosen authentication scheme (e.g., two-factor or three-factor authentication). The optimization process starts with a diverse population of such subsets, and each solution is evaluated based on the three objectives: security, energy consumption, and delay, as defined in equations (1), (2), and (3). Through iterative selection, crossover, and mutation, NSGA-II refines these combinations, favoring non-dominated solutions while maintaining diversity using crowding distance. Constraints are incorporated by ensuring only feasible solutions are generated during initialization, crossover, and mutation. The process continues until a termination criterion is met, such as a fixed number of generations or convergence of the Pareto front. This enables the algorithm to efficiently explore the trade-offs between authentication factors' characteristics, ultimately generating a Pareto front of optimal authentication schemes. Once the Pareto front is obtained, trust values guide the final solution selection, as explained in the following subsection.

3.4 Trust-Based Decision Making on the Pareto Front

Given a set of non-dominated authentication solutions obtained through NSGA-II: $\mathcal{S} = \{S_1, S_2, ..., S_n\}$, the decision process involves selecting the appropriate solution S^* for a given `claimed_ID`. Let $T(\texttt{ID})$ represent the trust score assigned to the claimed identity, where $T : \texttt{ID} \rightarrow [0, 1]$.

The selection function $\mathcal{F}_{sel}$ is defined as:

$$S^* = \mathcal{F}_{sel}(\mathcal{S}, T(\texttt{ID})) \tag{4}$$

where $\mathcal{F}_{sel}$ determines the most appropriate solution S^* based on trust and the available set of non-dominated solutions $\mathcal{S}$.

High-trust claimed identities trigger the use of stricter authentication factors to prevent potential exploitation of high-trust identities by malicious actors through identity spoofing, thereby protecting trust-dependent operations. Conversely, for low-trust identities, the truster may opt for less resource-intensive authentication methods or outright rejection of the interaction to minimize risk and resource expenditure:

$$\mathcal{F}_{sel}(\mathcal{S}, T(\texttt{ID})) = \arg\max_{s \in \mathcal{S}} (\alpha \cdot \text{SL}(s) - \beta \cdot \text{E}(s) - \gamma \cdot \text{D}(s)) \tag{5}$$

where:

- $\text{SL}(s)$ is the security level of authentication solution s.
- $\text{E}(s)$ represents the energy consumption of s.
- $\text{D}(s)$ represents the delay introduced by s.
- $\text{SL}(s)$, $\text{E}(s)$, and $\text{D}(s)$ are normalized to ensure a balanced contribution to the overall evaluation.
- α, β,γ are weight coefficients that vary based on trust:

$$\alpha = \lambda \cdot \frac{1}{1 + e^{(-k \cdot (T(\texttt{ID}) - 0.5))}} \tag{6}$$

$$\beta = (1 - \alpha) \cdot \phi \tag{7}$$

$$\gamma = (1 - \alpha) \cdot (1 - \phi) \tag{8}$$

  where α is determined by a sigmoid function that depends on the trust value $T(\texttt{ID})$. This function ensures a smooth transition in the weight assigned to security as trust increases. k is a steepness parameter controlling this transition from low to high security priority as trust increases, ϕ represents the importance of energy and delay ($\phi = 0.5$ for equal importance), the coefficients satisfy $\alpha + \beta + \gamma = 1$. Additionally, $\lambda \rightarrow [0, 1]$ controls the influence of trust on the trade-off, allowing for easier integration of other contextual factors in the selection process. For example $\lambda = f(T(\texttt{ID}), C_1, C_2, ...)$ where $C1, C2...$ represent other contextual factors (e.g., device type, criticality of the operation). For now, $\lambda = 1$ as trust is the primary factor. This allows for a smooth and dynamic adjustment of priorities based on the trust value of the claimed identity.

This ensures that for high-trust identities, security takes priority, while for low-trust identities, resource efficiency is favored. To summarize, the authentication process consists of the following steps:

(1) An agent presents a `claimed_ID`.
(2) The receiving agent (truster) retrieves $T(\texttt{claimed\_ID})$ and the Pareto-optimal authentication solutions $\mathcal{S}$ from the available set of authentication factors.
(3) The function $\mathcal{F}_{sel}$ selects the most suited solution S^*.
(4) The selected authentication method is applied.

4 PERFORMANCE EVALUATION

In this section, we evaluate the performance of our proposed authentication decision-making model by analyzing its effectiveness under different conditions.

4.1 Simulation Setup:

The energy cost, delay, and security level values assigned to each authentication factor are synthetic but inspired by plausible characteristics observed in IoT authentication systems, drawn from typical energy consumption patterns, estimated processing and communication times, and multi-criteria security evaluations in the literature [7, 15, 22]. These values are intended to facilitate the exploration of trade-offs between energy efficiency, security, and delay, rather than represent any specific authentication protocols. Future work may incorporate empirical data to refine these values. The factors used in our simulation are presented in Table 2, ensuring logical consistency throughout. Specifically, we account for the inherent correlation between security and energy consumption, as stronger authentication mechanisms typically demand more

Table 2: Artificial authentication factors

Factor	Security level	Energy cost	Delay
Factor 1	2	0.1	5
Factor 2	3	0.15	15
Factor 3	2.5	0.25	10
Factor 4	4	0.2	25
Factor 5	5.5	0.5	30
Factor 6	6	0.3	40
Factor 7	6	0.65	20
Factor 8	7	0.8	45
Factor 9	7.5	1.0	50
Factor 10	7.5	1.4	35
Factor 11	8	1.3	60
Factor 12	8	1.2	65
Factor 13	8.5	1.6	75
Factor 14	9.5	2	90
Factor 15	9	2.3	75

computational resources. Each factor is characterized by three key metrics: (i) Security level (SL) $\rightarrow [1, 10]$ where higher values indicate stronger security; (ii) Energy consumption (EC) $\rightarrow [0.1, 2.5]$ measured in millijoules (mJ); (iii) Delay (D) $\rightarrow [0.1, 100]$ measured in milliseconds (ms).

To assess our model, we implemented NSGA-II algorithm to optimize the selection of two-factor and three-factor authentication schemes. The key parameters used in NSGA-II process are as follows: crossover rate p_c of 0.9 and mutation rate p_m of 0.1. The fitness evaluation considers the three objectives defined previously. The number of possible solutions for two-factor schemes is $\binom{15}{2} = 105$, while for three-factor schemes, it increases to $\binom{15}{3} = 455$.

4.2 Results and Analysis of Pareto Front

Figure 3 and Figure 4 illustrate the evolution of the optimization process using NSGA-II for two-factor and three-factor authentication schemes, respectively. The 3D plots represent security on the x-axis, energy cost on the y-axis, and delay indicated by the color-bar. In both cases, the initial population is randomly distributed across the objective space, covering diverse combinations of authentication factors with varying levels of security, energy consumption, and delay.

As the optimization progresses, the algorithm gradually refines the population towards a set of non-dominated solutions forming the Pareto front. The final Pareto fronts for two-factor and three-factor schemes highlight the fundamental trade-offs inherent in authentication scheme selection: (i) Trade-off between security, energy, and delay: increasing security generally leads to higher energy consumption and increased delay. Solutions that minimize energy consumption tend to offer lower security levels. (ii) Impact of adding a third factor: the pareto front for three-factor schemes extends beyond the two-factor front, reflecting the potential for achieving higher security. However, this comes at the cost of increased energy consumption and delay, emphasizing the growing complexity with additional factors.

The analysis of the Pareto front highlights that selecting an optimal authentication scheme requires navigating these trade-offs. The Pareto front analysis underscores the importance of balancing security, energy, and delay when selecting authentication schemes. The trust-based decision process presented in the next subsection dynamically guides this selection.

4.3 Trust-based Selection of Authentication Factors

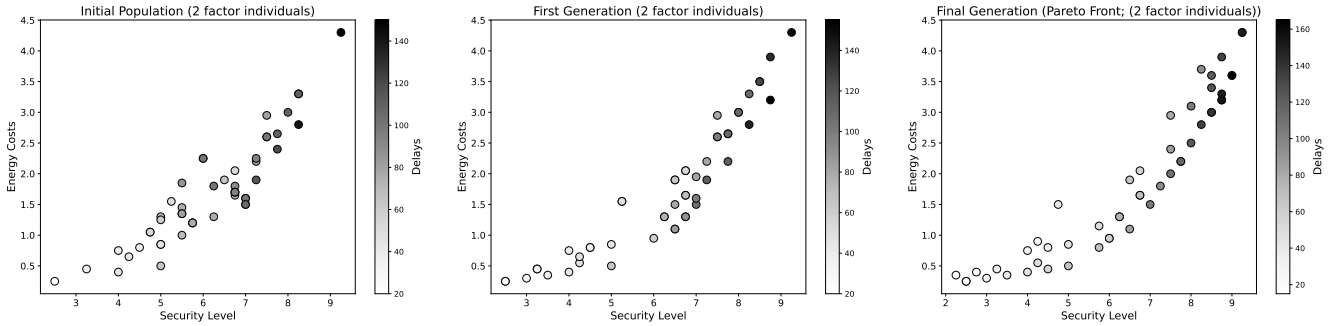
We apply a trust-based selection mechanism to the Pareto-optimal solutions obtained via NSGA-II, as described in previous sections. This mechanism adjusts the selection based on dynamic trust levels, with parameters α, β, and γ computed according to the trust value and steepness parameter k. Higher values of k make the selection more sensitive to changes in trust.

We performed a series of simulations using a range of trust values $T(\texttt{ID}) \in [0, 1]$. For each trust value, the selection process was applied to the Pareto-optimal solutions generated by NSGA-II. The impact of varying trust values on the chosen authentication solution was observed across several scenarios. Figure 5 illustrates the relationship between the trust value and the selected authentication solution. As trust increases, the selection mechanism prioritizes solutions with higher security levels, while minimizing energy consumption and delay as secondary factors. Conversely, for low-trust values, the selection process favors solutions that reduce resource consumption, opting for less secure but more energy-efficient or lower-delay authentication methods.

To further validate the effectiveness of our trust-based multi-objective optimization (TB-MOO) framework, we conducted a comparison with three alternative methods, each method includes the selection of three authentication factors:

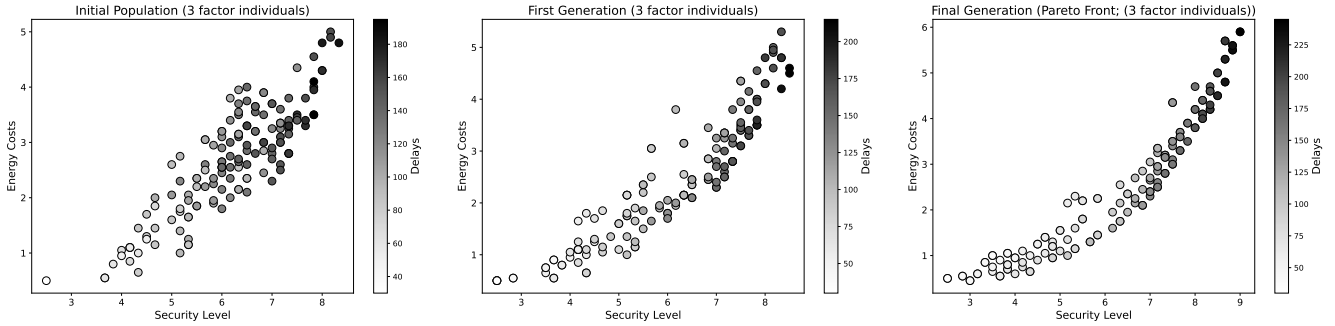
- Fixed Authentication (FixedA): Always uses the same three authentication factors while prioritizing security, providing a static baseline.
- Random Authentication (RandA): Selects factors randomly for each authentication.
- Trust Rule-based Authentication (RuleA): Adjusts factor selection based on three predefined trust thresholds (e.g., $T(\texttt{ID}) < 0.3 \rightarrow$ low energy, $0.3 < T(\texttt{ID}) < 0.7 \rightarrow$ balances objectives, $T(\texttt{ID}) > 0.7 \rightarrow$ high security).

The simulation models a direct communication process, where an agent interacts with 10 other agents, updating trust values dynamically based on predefined behaviors. For simplicity, trust values are updated after each episode in the simulation according to these behaviors, without relying on a formal trust management model. The objective is to verify how authentication factor selection adapts based on trust values. The 10 agents exhibited distinct behaviors: 3 malicious agents, 3 changing behavior agents, and 4 honest agents. Malicious agents results in a declining trust trend with occasional random fluctuations. Changing behavior agents demonstrate unpredictable trust oscillations, reflecting erratic behavior. Honest agents results in an increasing trust trend with minor noise. The simulation consisted of 1,000 episodes, with each episode involving authentication attempts for all 10 agents using the four methods: TB-MOO,



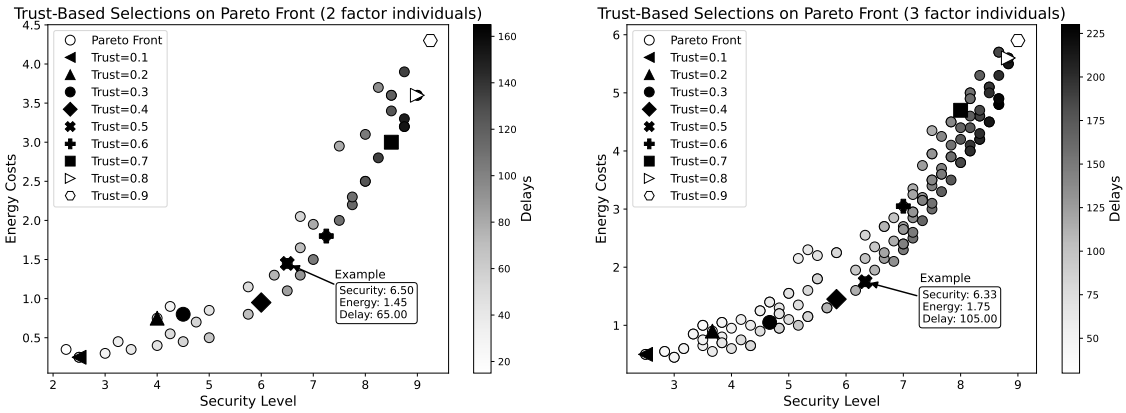
(a) Initial Population **(b) First Generation** **(c) Final Generation (Pareto Front)**

Figure 3: Results of two-factor authentication factor combinations



(a) Initial Population **(b) First Generation** **(c) Final Generation (Pareto Front)**

Figure 4: Results of three-factor authentication factor combinations

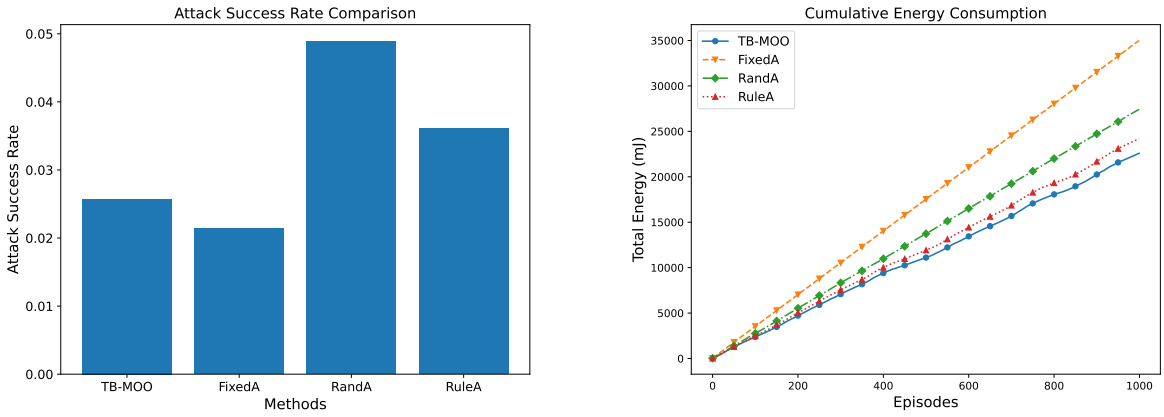


(a) Two-factor individuals **(b) Three-factor individuals**

Figure 5: Visualization of trust-driven selection on the pareto front

FixedA, RandA, RuleA. The attack success rate and cumulative energy consumption over time were measured for each method. To simulate attacks, the security level of each authentication factor, ranging from 1 to 10, is directly linked to its robustness against attacks. For example, a security level of 9 corresponds to a successful attack probability of approximately 1% $(10 - security\_level)/100$, with lower security levels increasing the likelihood of a successful attack.

The results, shown in Figure 6, illustrate the trade-offs between attack resistance and energy consumption for each method. FixedA



(a) Attack success rate

(b) Cumulative energy consumption

Figure 6: Comparison of attack rate and energy consumption on three-factor individuals

achieves the lowest attack rate at 0.0214, reflecting its strong security performance. This method was intentionally designed to prioritize security, utilizing a combination of authentication factors with an average security level of 8.1. While it minimizes the likelihood of attacks, it incurs significant energy consumption. In contrast, TB-MOO offers a balanced approach, with an attack rate of 0.0257 and the lowest cumulative energy consumption. By adapting the security requirements based on the trust level of each identity, TB-MOO efficiently allocates resources, ensuring higher security when necessary while reducing energy expenditure by ignoring low-trust claimed identities. RuleA, which relies on trust values assigned to three clusters, outperforms RandA in terms of energy efficiency, but it does not achieve the same level of balance between security and energy as TB-MOO. Unlike RuleA, RandA follows a random strategy, resulting in higher attack rates and energy consumption.

Overall, the results shows that TB-MOO achieves the best balance between security and energy efficiency, leveraging trust to adapt security requirements dynamically. FixedA may be suitable for scenarios where security is paramount, but it sacrifices energy efficiency. RuleA offers a middle ground, better than RandA, but still less adaptable than TB-MOO. By incorporating trust into the decision-making process, TB-MOO not only improves security but also optimizes the use of energy.

5 CONCLUSION

In this paper, we present a novel adaptive framework for authentication factor selection in IoT environments that balances security robustness with energy and latency efficiency. By integrating multi-objective optimization (NSGA-II) and trust-based decision-making, our approach addresses the critical challenge of balancing conflicting objectives in resource-constrained IoT systems. The framework first generates a Pareto front of non-dominated authentication solutions, capturing optimal trade-offs between the objectives. A sigmoid-like trust-weighting mechanism then dynamically prioritizes solutions from this Pareto front, favoring high-security configurations for highly trusted identities to prevent trust exploitation by identity spoofing, and energy-efficient configurations for low-trust interactions. This dual-layer optimization ensures that authentication decisions adapt to both the operational constraints of IoT devices and the evolving trustworthiness of agents.

Our simulation results demonstrate that the proposed approach effectively adapts authentication decisions based on trust levels, selecting from a Pareto front composed of two-factor and three-factor authentication solutions. The results show that our approach ensures robust security for high-trust identities while reducing authentication overhead for low-trust interactions. Comparative evaluations further highlight that our method achieves the best balance between attack resistance and energy efficiency compared to a high-security fixed approach, a three-category trust-based rule, and a random selection method.

The integration of trust management and adaptive authentication mechanisms in IoT and 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. Future work will explore the integration of additional contextual factors, such as device type, criticality of the operation, and environmental conditions, into the selection process. Furthermore, we aim to validate our approach through real-world deployments and extend it to other security-related decision-making processes in IoT systems.

ACKNOWLEDGMENTS

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

REFERENCES

[1] Hassan A Alterazi, Pravin R Kshirsagar, Hariprasath Manoharan, Shitharth Selvarajan, Nawaf Alhebaishi, Gautam Srivastava, and Jerry Chun-Wei Lin. 2022. Prevention of cyber security with the internet of things using particle swarm optimization. *Sensors* 22, 16 (2022), 6117.

[2] Amel Arfaoui, Soumaya Cherkaoui, Ali Kribeche, Sidi Mohammed Senouci, and Mohamed Hamdi. 2019. Context-aware adaptive authentication and authorization in internet of things. In *ICC 2019-2019 IEEE International Conference on Communications (ICC)*. IEEE, 1–6.

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

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

[5] Zheng-Yi Chai, Ying-Jie Zhao, and Ya-Lun Li. 2024. Multi-Task Computation Offloading Based On Evolutionary Multi-Objective Optimization in Industrial Internet of Things. *IEEE Internet of Things Journal* (2024).

[6] Kalyanmoy Deb, Amrit Pratap, Sameer Agarwal, and TAMT Meyarivan. 2002. A fast and elitist multiobjective genetic algorithm: NSGA-II. *IEEE transactions on evolutionary computation* 6, 2 (2002), 182–197.

[7] Elham Ebrahimpour and Shahram Babaie. 2024. Authentication in Internet of Things, protocols, attacks, and open issues: a systematic literature review. *International Journal of Information Security* 23, 3 (2024), 1583–1602.

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

[9] Xia Feng, Xiaofeng Wang, Kaiping Cui, Qingqing Xie, and Liangmin Wang. 2023. A distributed message authentication scheme with reputation mechanism for Internet of Vehicles. *Journal of Systems Architecture* 145 (2023), 103029.

[10] Giancarlo Fortino, Raffaele Gravina, Wilma Russo, and Claudio Savaglio. 2017. Modeling and simulating internet-of-things systems: A hybrid agent-oriented approach. *Computing in Science & Engineering* 19, 5 (2017), 68–76.

[11] Maria Habib, Ibrahim Aljarah, Hossam Faris, and Seyedali Mirjalili. 2020. Multi-objective particle swarm optimization for botnet detection in internet of things. *Evolutionary Machine Learning Techniques: Algorithms and Applications* (2020), 203–229.

[12] Asma Jahangeer, Sibghat Ullah Bazai, Saad Aslam, Shah Marjan, Muhammad Anas, and Sayed Habibullah Hashemi. 2023. A review on the security of IoT networks: From network layer's perspective. *IEEE Access* 11 (2023), 71073–71087.

[13] Tobias Jung, Payal Shah, and Michael Weyrich. 2018. Dynamic co-simulation of internet-of-things-components using a multi-agent-system. *Procedia Cirp* 72 (2018), 874–879.

[14] Barjinder Kaur, Sajjad Dadkhah, Farzaneh Shoeleh, Euclides Carlos Pinto Neto, Pulei Xiong, Shahrear Iqbal, Philippe Lamontagne, Suprio Ray, and Ali A Ghorbani. 2023. Internet of things (IoT) security dataset evolution: Challenges and future directions. *Internet of Things* 22 (2023), 100780.

[15] Umair Khalid, Muhammad Asim, Thar Baker, Patrick CK Hung, Muhammad Adnan Tariq, and Laura Rafferty. 2020. A decentralized lightweight blockchain-based authentication mechanism for IoT systems. *Cluster Computing* 23, 3 (2020), 2067–2087.

[16] Pimal Khanpara, Kruti Lavingia, Rajvi Trivedi, Sudeep Tanwar, Amit Verma, and Ravi Sharma. 2023. A context-aware internet of things-driven security scheme for smart homes. *Security and Privacy* 6, 1 (2023), e269.

[17] Alex Koohang, Carol Springer Sargent, Jeretta Horn Nord, and Joanna Paliszkiewicz. 2022. Internet of Things (IoT): From awareness to continued use. *International Journal of Information Management* 62 (2022), 102442.

[18] R Timothy Marler and Jasbir S Arora. 2010. The weighted sum method for multi-objective optimization: new insights. *Structural and multidisciplinary optimization* 41 (2010), 853–862.

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

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

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

[22] Muslum Ozgur Ozmen, Attila A Yavuz, and Rouzbeh Behnia. 2019. Energy-aware digital signatures for embedded medical devices. In *2019 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 55–63.

[23] Santosh Pattar, Rajkumar Buyya, Kuppanna Rajuk Venugopal, SS Iyengar, and LM Patnaik. 2018. Searching for the IoT resources: Fundamentals, requirements, comprehensive review, and future directions. *IEEE Communications Surveys & Tutorials* 20, 3 (2018), 2101–2132.

[24] João Luiz Junho Pereira, Guilherme Antônio Oliver, Matheus Brendon Francisco, Sebastiao Simoes Cunha Jr, and Guilherme Ferreira Gomes. 2022. A review of multi-objective optimization: methods and algorithms in mechanical engineering problems. *Archives of Computational Methods in Engineering* 29, 4 (2022), 2285–2308.

[25] Thi Ngoc Diep Pham and Chai Kiat Yeo. 2018. Adaptive trust and privacy management framework for vehicular networks. *Vehicular Communications* 13 (2018), 1–12.

[26] Isaac Pinyol and Jordi Sabater-Mir. 2013. Computational trust and reputation models for open multi-agent systems: a review. *Artificial Intelligence Review* 40, 1 (2013), 1–25.

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

[28] Riseul Ryu, Soonja Yeom, David Herbert, and Julian Dermoudy. 2023. A comprehensive survey of context-aware continuous implicit authentication in online learning environments. *IEEE Access* 11 (2023), 24561–24573.

[29] Jordi Sabater-Mir and Laurent Vercouter. 2013. Trust and reputation in multiagent systems. *Multiagent systems* (2013), 381.

[30] Marc Saideh, Jean-Paul Jamont, and Laurent Vercouter. 2024. Opportunistic Sensor-Based Authentication Factors in and for the Internet of Things. *Sensors* 24, 14 (2024), 4621.

[31] Marc Saideh, Jean-Paul Jamont, and Laurent Vercouter. 2025. Trust-Based Multi-Agent Authentication Decision Process for the Internet of Things. In *17th International Conference on Agents and Artificial Intelligence*, Vol. 1. SCITEPRESS-Science and Technology Publications, 45–55.

[32] Avani Sharma, Emmanuel S Pilli, Arka P Mazumdar, and Poonam Gera. 2020. Towards trustworthy Internet of Things: A survey on Trust Management applications and schemes. *Computer Communications* 160 (2020), 475–493.

[33] Eckart Zitzler, Kalyanmoy Deb, and Lothar Thiele. 2000. Comparison of multiobjective evolutionary algorithms: Empirical results. *Evolutionary computation* 8, 2 (2000), 173–195.