



HAL
open science

Accelerating Trust Convergence in IIoT: A ML Approach for Dynamic Network Conditions

Aymen Bouferroum, Valeria Loscri, Abderrahim Benslimane

► To cite this version:

Aymen Bouferroum, Valeria Loscri, Abderrahim Benslimane. Accelerating Trust Convergence in IIoT: A ML Approach for Dynamic Network Conditions. IEEE Global Communications Conference (GLOBECOM) 2025, Dec 2025, Taipei, Taiwan. pp.4427-4432, <10.1109/GLOBECOM59602.2025.11431874>. <hal-05235093v2>

HAL Id: hal-05235093

<https://hal.science/hal-05235093v2>

Submitted on 18 Jun 2026

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Copyright - All rights reserved

Accelerating Trust Convergence in IIoT: A ML Approach for Dynamic Network Conditions

Aymen Bouferroum
Inria Lille-Nord Europe
Lille, France
aymen-salah-eddine.bouferroum@inria.fr

Valeria Loscri
Inria Lille-Nord Europe
Lille, France
valeria.loscri@inria.fr

Abderrahim Benslimane
LIA/CERI University of Avignon
Avignon, France
abderrahim.benslimane@univ-avignon.fr

Abstract—In Industrial Internet of Things (IIoT) environments, trust management plays a vital role in securing systems, especially when dealing with resource-constrained devices. Traditional trust models often overlook the impact of fluctuating network quality, leading to slower trust convergence and inaccurate assessments. In this paper, we propose a dynamic trust management solution, known as the Trust Convergence Acceleration (TCA) approach, which integrates Machine Learning (ML) to accelerate trust convergence under poor network conditions. Our model predicts the number of time units needed for trust convergence based on key network metrics and dynamically adapts transition probabilities in the trust model to enhance convergence speed. Using a simulation framework that incorporates realistic Wi-Fi channel conditions based on the IEEE 802.11 standard, we demonstrate the effectiveness of the TCA-based approach, achieving up to a 28.6% reduction in trust convergence time under challenging conditions. Furthermore, the proposed solution exhibits resilience in scenarios involving malicious nodes, improving trust evaluation accuracy. This work provides a scalable and adaptive trust framework for IIoT systems in dynamic industrial environments, ensuring robust performance under varying network conditions.

Index Terms—Internet of Things (IoT), Industrial IoT (IIoT) Networks, Trust Management, Machine Learning (ML), Network Quality.

I. INTRODUCTION

The rapid advancement of the Industrial Internet of Things (IIoT) has transformed industrial sectors through Industry 4.0 [1], integrating cyber-physical systems, cloud computing, and artificial intelligence into manufacturing processes to enhance operational efficiency and decision-making capabilities [2]. This evolution, however, introduces significant security challenges as IIoT networks grow increasingly complex, particularly in resource-constrained environments where traditional encryption-based security proves impractical [3]. The heterogeneous nature of these devices, with their limited computational and energy resources, has led to the emergence of trust management systems as a viable alternative for securing industrial operations. These systems [3] continuously monitor device behavior, assigning and updating trust levels based on interactions and performance [4], enabling effective detection and isolation of potentially compromised devices.

Trust management approaches can be categorized into centralized, distributed, and hybrid models [2], [5], [6]. Centralized

models provide global network visibility but face scalability challenges. Distributed models offer improved scalability but require significant energy consumption and time to achieve trust convergence [7], which is problematic in resource-constrained environments. Hybrid models, such as the H-IIoT architecture [2], combine the strengths of both approaches by organizing IIoT devices into industrial communities managed by trusted leaders, balancing localized trust management with a global perspective.

In operational IIoT environments, network quality is subject to continuous variations caused by electromagnetic interference, device mobility, and network congestion. These fluctuations significantly impact trust management systems, as network metrics such as availability, throughput, and delay influence the effectiveness of trust evaluations [8]. While some researchers have employed recommendation filtering algorithms to address varying contextual factors [9] or introduced fixed probability models for network constraints [2], these approaches often fail to capture the nuanced impact of dynamic network quality on trust evaluation. Consequently, trust management systems lacking real-time adaptation risk delayed detection of malicious activities and inaccurate assessments of device trustworthiness.

To address these challenges, we propose the Trust Convergence Acceleration (TCA), a novel trust management solution designed to enhance trust metric convergence by predicting and optimizing the trust evaluation process under varying network conditions. Our TCA integrates the Random Forest algorithm, which offers optimal performance with limited data, making it particularly suitable for resource-constrained IIoT environments. Empirical evaluations confirm its superior performance in terms of prediction accuracy and convergence speed. Integrated within the H-IIoT architecture [2] and leveraging Wi-Fi 6 (IEEE 802.11ax) technology [10], [11], our framework provides an adaptive, scalable, and robust solution that significantly improves performance under fluctuating network conditions. Our work makes the following key contributions:

- Development of a trust management model that integrates real-time network channel conditions into trust evaluations, capturing the inherent variability of IIoT environments.
- Design and implementation of a Machine Learning (ML) framework to accelerate trust convergence under varying

network conditions, ensuring rapid and reliable system performance.

- Demonstration of enhanced robustness against malicious nodes, showcasing the resilience of our approach against adversarial behaviors.

The rest of this paper is organized as follows: Section II introduces the system model and problem formulation. Section III details our ML-enhanced trust management solution. Section IV evaluates the performance of our approach. Finally, Section V concludes and outlines future research directions.

II. SYSTEM MODEL AND PROBLEM FORMULATION

Our proposed trust management approach requires a formal characterization of the IIoT environment to address the challenges of dynamic industrial networks. We establish a comprehensive framework encompassing network architecture, trust formulation mechanisms, and an analysis of how varying network quality influences trust convergence in operational settings.

A. Network Architecture

Our system model builds upon an enhanced version of the Hybrid Industrial Internet of Things (H-IIoT) architecture [2], integrating Wi-Fi 6 technology to meet the demands of modern industrial environments. The architecture organizes IIoT devices into managed industrial communities, providing a foundation for efficient trust management in large-scale deployments.

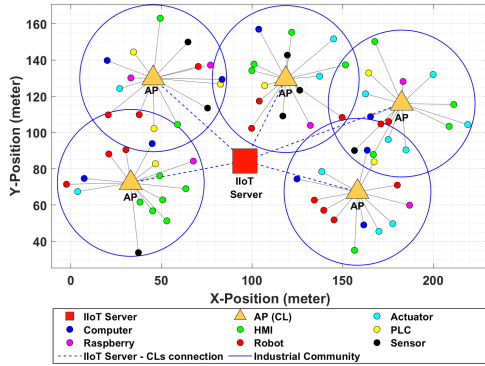


Fig. 1: Network architecture.

The network consists of K Community Leaders (CLs) and L Member Nodes (MNs), denoted by $CL_j | j \in \{1, 2, \dots, K\}$ and $MN_i | i \in \{1, 2, \dots, L\}$, respectively. The main components include:

- 1) **IIoT Server**: A cloud-based central authority that aggregates global trust metrics and ensures consistent trust evaluation across the network.
- 2) **CLs**: Wi-Fi 6 Access Points (APs) serving as trusted supervisors for industrial communities, each managing a Basic Service Set (BSS) of devices.
- 3) **MNs**: Various IIoT devices (sensors, robots, actuators, PLCs, HMIs) organized into communities based on proximity and operational roles.

- 4) **Industrial Communities**: Functional groupings of MNs managed by a single CL, corresponding to a BSS in Wi-Fi terminology, enabling localized trust management and reduced communication overhead.

For simulation purposes, our environment comprises a total of 200 nodes distributed across a 200 x 200 m² area representing an industrial facility. From these, 10 nodes function as CLs, while the remaining 190 operate as MNs with varying industrial roles. This scale was selected to reflect realistic industrial deployments while remaining computationally feasible for detailed network quality analysis. Fig. 1 provides a simplified visualization of this architecture. The hierarchical structure created by these components enables efficient trust evaluation through a balance of localized management and global coordination. CLs monitor their associated nodes while communicating with the IIoT server to maintain network-wide trust consistency, significantly reducing overhead in large-scale deployments. Our implementation leverages IEEE 802.11 standards due to their widespread adoption in industrial settings, technical maturity, and robust performance in challenging electromagnetic environments. Specifically, we selected Wi-Fi 6 for its advanced capabilities that address critical IIoT requirements [10]. These include Orthogonal Frequency Division Multiple Access (OFDMA) for improved multi-device communication, Multi-User Multiple Input Multiple Output (MU-MIMO) for enhanced throughput, BSS coloring to reduce interference in dense deployments, and Target Wake Time (TWT) for energy efficiency. While our current implementation utilizes Wi-Fi 6, the framework's modular design ensures compatibility with emerging wireless technologies. Note that the centralized server, while enabling global coordination, represents a potential single point of failure that can be mitigated through redundancy or edge-based failover in critical deployments.

B. Trust Model Formulation

The trust model, Tm-IIoT, evaluates the trustworthiness of IIoT devices based on their behavior and interactions within the network [2]. Each node i is assigned a trust metric Tm_i , continuously updated based on these performance metrics:

- 1) **Cooperation Rate** (C_{MN_i}): Reflects the node's willingness to cooperate in network activities (e.g., forwarding messages):

$$C_{MN_i} = \frac{\sum_{i=1}^{NF} C_{mi}}{NF}, \quad (1)$$

where NF is the total number of messages transmitted to the node, and C_{mi} is 1 if message mi is forwarded correctly, 0 otherwise.

- 2) **Direct Honesty** (D_{MN_i}): Assesses how well the node's activities align with its expected operational behavior, as defined in its device configuration profile:

$$D_{MN_i} = \frac{|A(MN_i) \cap AF(MN_i)|}{|A(MN_i) \cup AF(MN_i)|}, \quad (2)$$

where $A(MN_i)$ is the set of activities the node should perform according to its operational role, and $AF(MN_i)$ is the set of activities actually performed.

- 3) **Indirect Honesty** (I_{MN_i}): Reflects the node’s reputation within its community, based on feedback from other nodes:

$$I_{MN_i} = \frac{\sum_{MN'_i=1}^N R_{MN'_i, MN_i}}{N}, \quad (3)$$

where $R_{MN'_i, MN_i}$ is the reputation given by node MN'_i to node MN_i , and N is the total number of MNs. This peer-evaluation mechanism helps identify malicious nodes that might appear legitimate in direct evaluations.

The model employs a finite-state discrete-time Markov chain with $(E + 1)$ states to represent trust evolution, where E is set to 10 in our implementation. Each state corresponds to a discrete trust value between 0 (completely untrusted) and 1 (fully trusted), with uniform increments of $\phi = 0.1$.

While continuous trust models offer more granularity, we adopt a discrete approach for three key reasons: (1) computational efficiency in resource-constrained environments, (2) increased robustness against small fluctuations in trust metrics, and (3) simplified decision-making for trust-based actions. The choice of $E=10$ states balances granularity with stability: coarser ($E=5$) and finer ($E=20$) discretizations in our tests preserved qualitative outcomes while $E=10$ minimized oscillations.

The transition matrix P of the Markov chain is defined as:

$$P = (P_{i,j}(t))_{0 \leq i,j \leq E}, \quad (4)$$

where $P_{i,j}(t)$ represents the probability of transitioning from state i to state j at time t , expressed as:

$$P_{i,j}(t) = Pr(Y_t = j | Y_{t-1} = i), \quad (5)$$

where Y_t is the random variable representing the trust metric Tm of an IIoT device at time t . The probability of being in state i at time t , given an initial state $Y_0 = 1$, is:

$$p_i(t) = \sum_{z \in \{1 \dots E\}} P_{1,z}(t_z) \cdot P_{z,i}(t). \quad (6)$$

At each time step, the trust calculation allows for five possible transitions based on the performance metrics: increasing, decreasing, remaining in the same state, reaching the maximum trust state (E), or falling to the untrusted state (0). This mechanism ensures adaptive trust assessment, enabling the model to respond to changes in node behavior over time.

C. Network Condition Modeling and Tm Convergence Analysis

The assessment of trust in Wi-Fi 6 environments necessitates consideration of Quality of Service (QoS) parameters identified in [12] as significant for network performance and trust evaluation. These parameters include: Signal-to-Noise Ratio (SNR), Packet Loss probability (PL), Jitter (J), Latency (L), Throughput (T), and Signal-to-Interference-plus-Noise Ratio (SINR). Each parameter directly influences data transmission reliability, which subsequently affects trust evaluation accuracy. Our investigation leverages MATLAB’s WLAN and Communications Toolboxes for creating this high-fidelity simulation environment, selected for their accurate implementation of IEEE

802.11ax specifications. This framework incorporates detailed physical layer characteristics, including OFDMA resource allocation and MU-MIMO transmission schemes, ensuring that network behavior faithfully represents operational conditions in industrial settings.

We conducted simulations analyzing three distinct network condition scenarios (Good, Medium, and Poor) derived from IEEE 802.11ax standard specifications and observed performance characteristics in industrial Wi-Fi 6 deployments. Table I summarizes these parameter ranges, which represent realistic operational conditions in industrial environments based on field measurements and standard performance metrics for Wi-Fi 6 networks.

TABLE I: Network condition scenarios with parameter ranges.

Parameter	Scenario 1 Good	Scenario 2 Medium	Scenario 3 Poor
SNR (dB)	30–41	20–29	10–19
Packet Loss Probability (%)	0–1	1–4	4–8
Jitter (ms)	0–2	2–10	10–30
Latency (ms)	1–5	5–20	20–50
Throughput (% of max)	80–100	50–80	<50
SINR (dB)	>25	15–25	<15

Our simulation methodology for trust convergence analysis comprised the following key steps:

- 1) **Baseline Establishment:** We first conducted baseline simulations under ideal network conditions to determine the stable trust value for each node in the network, representing its "ground truth" trustworthiness.
- 2) **Trust Perturbation:** We then artificially set the trust values of selected nodes to 0.5, deliberately deviating from their established ground truth values.
- 3) **Convergence Monitoring:** Under each network condition scenario, we measured the number of time units required for the perturbed trust values to recover and stabilize at their ground truth values.

Fig. 2 illustrates trust evolution across the three scenarios, revealing a clear correlation between network quality and trust stabilization time. Under Good conditions, trust recovers from perturbation ($Tm=0.5$) to ground truth ($Tm=0.75$) in only 4 time units, compared to 8 units in Medium conditions and 12 in Poor conditions. When trust converges under Good conditions, under Poor conditions it has only reached approximately 0.58, creating periods of uncertainty about node trustworthiness that compromise security. These findings underscore the need

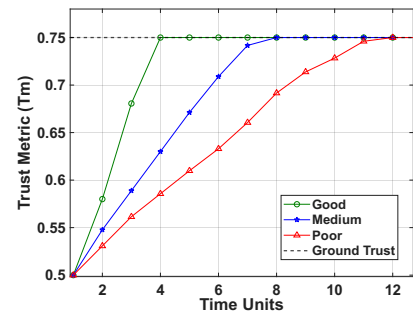


Fig. 2: Tm convergence over time under varying network conditions.

for an adaptive trust management approach that adapts to network conditions to achieve faster trust convergence without compromising evaluation accuracy.

III. PROPOSED TCA-BASED TRUST MANAGEMENT

We introduce a novel approach that integrates ML with existing trust management frameworks to address the challenges of trust convergence under varying network conditions. Our TCA solution predicts and mitigates the impact of network conditions on trust convergence. This section details our architecture, methodology, and implementation.

A. Solution Architecture

Our solution enhances trust management adaptability through the TCA module, which optimizes trust metric convergence through network condition quantification, ML prediction, and dynamic trust adjustment. Fig. 3 illustrates our approach.

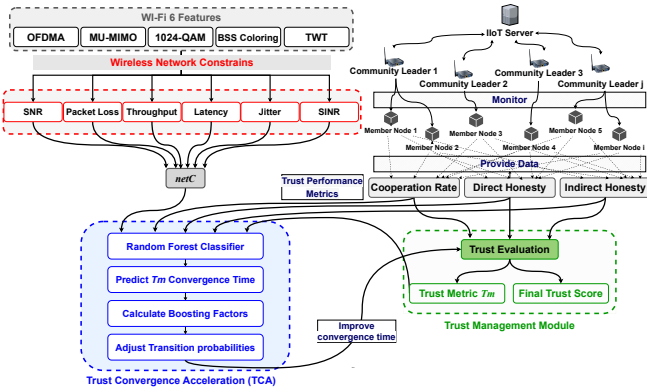


Fig. 3: Architecture of our TCA solution.

The TCA operates as an enhancement layer that integrates with existing trust frameworks, with three key components:

- 1) **Network Condition Quantification:** A comprehensive network condition parameter ($netC$) aggregates multiple quality indicators, providing real-time assessment of network health.
- 2) **ML Prediction:** A pre-trained Random Forest model predicts convergence time under specific network conditions, enabling proactive trust adjustments.
- 3) **Dynamic Trust Adjustment:** Based on predictions, the system adaptively modifies trust evaluation parameters to accelerate convergence while maintaining accuracy.

Importantly, the TCA operates predominantly offline, using pre-trained models to make predictions. This design minimizes computational overhead during operation, making it suitable for resource-constrained IIoT environments.

B. Network Condition Parameter ($netC$)

The $netC$ parameter provides a unified representation of network quality, calculated as a weighted sum of normalized network metrics:

$$netC = \alpha \cdot SNR_{norm} + \beta \cdot (1 - PL_{norm}) + \gamma \cdot (1 - J_{norm}) + \delta \cdot (1 - L_{norm}) + \tau \cdot T_{norm} + \sigma \cdot SINR_{norm}, \quad (7)$$

where the normalized metrics represent key QoS parameters, and the weights ($\alpha, \beta, \gamma, \delta, \tau, \sigma$) reflect their relative

importance. For this implementation, we assign equal weights (1/6 each) to avoid bias toward any single QoS metric without deployment-specific empirical evidence. This baseline approach demonstrated robust performance across all tested industrial scenarios. For metrics where lower values indicate better performance (PL, J, L), we use their complements to maintain consistent polarity in the calculation.

C. Dataset Generation and Preprocessing

Building upon the simulation environment introduced in Section II-C, we utilized MATLAB's WLAN and Communications Toolboxes to generate a comprehensive dataset for ML model training and evaluation. This integration ensured consistency between our network condition modeling and the subsequent ML-based trust acceleration framework, maintaining realistic IEEE 802.11ax channel characteristics throughout both analysis phases. The dataset development process involved the following steps:

- 1) **Node Selection:** MNs were randomly selected from each industrial community within the simulated environment.
- 2) **Network Condition Simulation:** Each selected node was subjected to varying network conditions, categorized as Good, Medium, and Poor, based on the parameter ranges defined in Table I.
- 3) **Trust Metric and $netC$ Calculation:** For each node and network condition, we calculated the trust performance metrics and the network condition parameter.
- 4) **Trust Convergence Simulation:** We simulated the trust convergence process for each node under the given network conditions, recording the time units required for the Tm to converge.
- 5) **Data Sample Recording:** Each simulation run generated a data sample comprising the features $X = [netC, C_{MN_i}, D_{MN_i}, I_{MN_i}, SNR, PL, J, L, T, SINR]$ and the corresponding output Y (convergence time), as illustrated in Fig. 4.

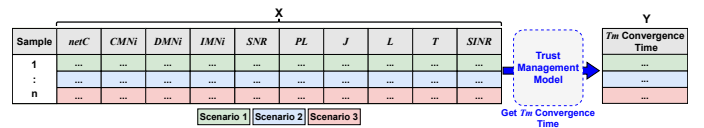


Fig. 4: Dataset input and output structure.

The initial dataset comprised approximately 35,000 samples with a wide range of convergence times. To facilitate effective model training and address the inherent variability in trust convergence times, we organized the convergence times into six distinct classes:

- Class 1 (Very Fast Convergence): $Y = 4$
- Class 2 (Fast Convergence): $Y = 5-6$
- Class 3 (Moderate Convergence): $Y = 7-9$
- Class 4 (Slow Convergence): $Y = 10-12$
- Class 5 (Very Slow Convergence): $Y = 13-15$
- Class 6 (Extremely Slow Convergence): $Y \geq 16$

We then employed random under-sampling to balance the dataset, resulting in 1,000 samples per class and a total of 6,000

samples. This balanced dataset provides a robust foundation for training and evaluating our ML model.

D. Trust Convergence Acceleration (TCA)

The TCA leverages ML to predict the convergence time of trust metrics based on network conditions and trust parameters. We evaluated several ML models, including Random Forest [13], XGBoost [14], Support Vector Machine (SVM) [15], and Logistic Regression [16]. We opted against deep learning models for several reasons specific to IIoT: their substantial computational demands render them impractical for resource-constrained devices; neural networks require significantly larger training datasets than were feasible in our context; deployment across distributed IIoT environments would introduce considerable complexity without commensurate improvements for this prediction task; and traditional ML approaches offer superior interpretability, a crucial factor in security-critical applications. The dataset was split into 70% for training, 15% for validation, and 15% for testing. Model performance was evaluated using Accuracy, Precision, Recall, and F1-score [17], as shown in Table II.

TABLE II: Comparison of ML models.

Model	Accuracy	Precision	Recall	F1-Score
Random Forest	92.66%	92.72%	92.73%	92.63%
XGBoost	91.50%	91.65%	91.58%	91.55%
SVM	89.12%	89.35%	89.20%	89.18%
Logistic Regression	85.45%	85.60%	85.52%	85.48%

Based on these results, the Random Forest classifier was selected for the TCA implementation due to its superior performance across all metrics. The Random Forest model achieved the highest accuracy (92.66%) and F1-score (92.63%), demonstrating its strong capability in accurately predicting trust convergence time ranges under varying network conditions. Additionally, Random Forest’s ensemble approach provides robustness to noise in feature data. The model’s inference complexity of $O(T \cdot d_{\max})$ (trees \times depth) enables real-time evaluation on CLs with negligible overhead.

E. Dynamic Trust Evaluation Adjustment

To enhance adaptability to varying network conditions, we introduce a boosting factor (bf) that dynamically adjusts trust convergence based on predicted convergence time and current network quality. The boosting factor is computed as:

$$bf = 1 + (1 - netC) \cdot \lambda \cdot \min\left(\frac{pc}{maxT}, 1\right), \quad (8)$$

where pc is the predicted class from the ML model, $maxT$ is the maximum convergence time units (for normalization), and λ is a scaling factor (empirically set to 0.2 for optimal convergence-stability balance). When network conditions are good ($netC \geq 0.8$), no boosting is applied ($bf = 1$).

Algorithm 1 outlines the boosting factor calculation process, which is then used to adjust transition probabilities in the Markov chain trust model, effectively accelerating trust convergence under poor network conditions while maintaining evaluation accuracy. This approach allows our system to

Algorithm 1: Boosting Factor Calculation

```

Input:  $netC, pc, maxT$ 
Output:  $bf$ 
 $classRanges \leftarrow [4, 6, 9, 12, 15, maxT]$  // Class 1 to 6 upper bounds;
 $pc \leftarrow classRanges[pc]$  // Select upper bound of predicted class range;
if  $netC \geq 0.8$  then
   $bf \leftarrow 1$  // No boosting for good network conditions;
else
   $baseFactor \leftarrow 1 + (1 - netC) \cdot \lambda$  // For  $\lambda = 0.2$ , the maximum boosting factor is 1.2;
   $classFactor \leftarrow \min\left(\frac{pc}{maxT}, 1\right)$  // Normalize predicted class range using upper bound;
   $bf \leftarrow 1 + (baseFactor - 1) \cdot classFactor$  // Adjust  $bf$ ;
return  $bf$ ;

```

distinguish between poor network conditions and malicious behavior by adjusting trust evaluation parameters based specifically on network metrics. Since trust calculations incorporate both performance metrics (cooperation, honesty) and network conditions, the system can identify when poor performance is likely due to network issues rather than malicious intent.

F. Performance Evaluation

We conducted comprehensive simulations comparing our TCA-based approach with the original Tm-IIoT model across varying network conditions and in the presence of malicious nodes. The results are presented in Fig. 5. Fig. 5a illustrates trust convergence for a monitored node, comparing TCA with the original Tm-IIoT under different network conditions. In Scenario 1 (Good network conditions), both approaches converge rapidly in approximately 4 time units, as optimal conditions facilitate efficient trust evaluation. However, TCA’s advantages become evident in challenging environments. In Scenario 2 (Medium conditions), TCA achieves convergence in about 6 time units versus 7 for Tm-IIoT, yielding a 14.3% reduction in convergence time. The improvement is most pronounced in Scenario 3 (Poor conditions), where TCA converges significantly faster, requiring approximately 10 time units compared to 14 for Tm-IIoT. This represents a substantial 28.6% reduction in convergence time, demonstrating TCA’s effectiveness in accelerating trust stabilization, particularly when network quality degrades.

To evaluate robustness against malicious behavior, we analyzed performance during bad-mouthing attacks [18], where attackers provide false negative feedback to unfairly lower legitimate nodes’ trust scores. Fig. 5b presents comparative results under poor network conditions with malicious node percentages (Pm) ranging from 20% to 50%. While convergence time increases for both models as attack intensity rises, TCA consistently demonstrates superior performance over Tm-IIoT in terms of convergence speed. At $Pm=20\%$, TCA converges significantly faster, requiring only 9 time units compared to 13 for Tm-IIoT, which represents a 30.77% reduction. This advantage persists as the percentage of malicious nodes increases: at $Pm=30\%$, TCA converges in 10 time units versus 13 for Tm-IIoT (a 23.08% improvement), and at $Pm=40\%$, it takes 11 time units for TCA compared to 14 for Tm-IIoT (a 21.43% reduction). Even under high attack intensity of $Pm=50\%$, TCA maintains a clear edge, converging in 12

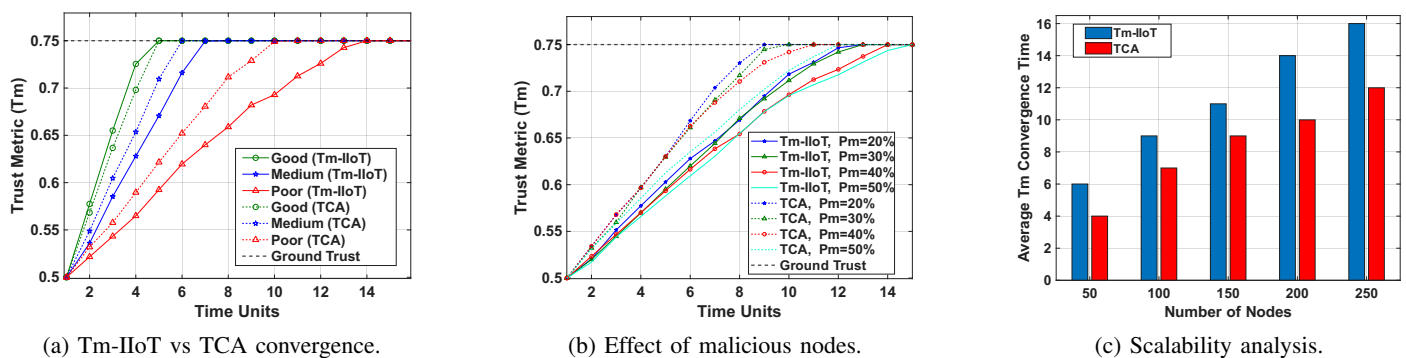


Fig. 5: Performance comparison of the TCA-based trust model.

time units while Tm-IIoT requires approximately 14.5 time units, achieving a 17.24% faster convergence. Furthermore, Fig. 5b confirms the robustness of our approach; while both models eventually converge near the ground truth (0.75), TCA reaches this level significantly faster, demonstrating that the acceleration mechanism does not negatively impact final trust evaluation accuracy, even under coordinated attack scenarios.

Finally, we evaluated scalability by analyzing the average convergence time with increasing network sizes (from 50 to 250 nodes) under poor network conditions, as depicted in Fig. 5c. The results clearly demonstrate that TCA consistently exhibits lower average convergence times across all tested network scales. For a smaller network of 50 nodes, TCA converges in approximately 4 time units compared to 6 for Tm-IIoT, achieving a significant 33% reduction. This performance advantage is maintained as the network grows. For the largest tested network of 250 nodes, TCA requires only 12 time units for convergence versus 16 for Tm-IIoT, still providing a notable 25% reduction. This confirms that TCA’s benefits in accelerating trust convergence are preserved even in large-scale IIoT deployments, highlighting its practical applicability.

IV. CONCLUSION AND FUTURE RESEARCH

This paper has presented a novel ML-enhanced trust management framework for IIoT environments that effectively addresses the challenges of varying network conditions in industrial settings. Our TCA approach achieves up to 28.6% faster trust convergence under challenging network conditions while maintaining robust accuracy in detecting malicious nodes. Experimental results demonstrate the framework’s resilience against bad-mouthing attacks and excellent scalability across networks of varying sizes, confirming its practical applicability in diverse industrial deployments. While our implementation utilizes IEEE 802.11ax as the foundational standard, the framework’s inherent adaptability enables its application across diverse network architectures, including emerging cellular infrastructures. The modular design facilitates deployment as a network layer overlay in IIoT systems, interfacing effectively with standard industrial communication protocols. Future research will focus on real-world testbed validation using standards-compliant APs as CLs and ESP32-C6 devices as MNs, enhancing threat detection capabilities for sophisticated attack scenarios, and extending support to emerging industrial

connectivity paradigms including deterministic networking approaches.

ACKNOWLEDGMENT

This work was funded by the French National Research Agency (ANR-22-PEFT-0007) as part of France 2030 and the NF-FITNESS project.

REFERENCES

- [1] A.-R. Sadeghi *et al.*, “Security and privacy challenges in industrial internet of things,” in *Proc. Annu. Des. Autom. Conf.*, (New York, NY, USA), Association for Computing Machinery, 2015.
- [2] C. Boudagdigue *et al.*, “Trust management in industrial internet of things,” *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 3667–3682, 2020.
- [3] M. Serror *et al.*, “Challenges and opportunities in securing the industrial internet of things,” *IEEE Trans. Ind. Inform.*, vol. 17, no. 5, pp. 2985–2996, 2021.
- [4] C. Boudagdigue *et al.*, “A distributed advanced analytical trust model for IoT,” in *Proc. IEEE Int. Conf. Commun.*, pp. 1–6, 2018.
- [5] M. D. Alshehri *et al.*, “Clustering-driven intelligent trust management methodology for the internet of things (CITM-IoT),” *Mob. Netw. Appl.*, vol. 23, no. 3, pp. 419–431, 2018.
- [6] I.-R. Chen *et al.*, “Trust-based service management for social internet of things systems,” *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 6, pp. 684–696, 2016.
- [7] B. Abderrahim *et al.*, “TMCoi-SIoT: A trust management system based on communities of interest for the social internet of things,” in *Proc. Int. Wirel. Commun. Mob. Comput.*, pp. 747–752, 2017.
- [8] V. Mohammadi *et al.*, “Trust-based recommendation systems in internet of things: a systematic literature review,” *Hum.-Centric Comput. Inf. Sci.*, vol. 9, no. 1, p. 21, 2019.
- [9] G. Chen *et al.*, “An adaptive trust model based on recommendation filtering algorithm for the internet of things systems,” *Comput. Netw.*, vol. 190, p. 107952, 2021.
- [10] M. Smith *et al.*, “Wi-Fi 6/6E for industrial IoT,” white paper, Wireless Broadband Alliance, 2022. [Online]. Available: <https://wballiance.com/resource/wi-fi-6-6e-for-industrial-iiot/>. Accessed: February 4, 2025.
- [11] D.-J. Deng *et al.*, “IEEE 802.11ax: Next generation wireless local area networks,” in *Proc. Int. Conf. Heterog. Netw. Qual. Reliab. Secur. Robust.*, pp. 77–82, 2014.
- [12] W. Sugeng *et al.*, “The impact of QoS changes towards network performance,” in *Int. J. Comput. Netw. Commun. Secur.*, 2015.
- [13] L. Breiman, “Random forests,” *Mach. Learn.*, vol. 45, pp. 5–32, 2001.
- [14] T. Chen *et al.*, “XGBoost: A scalable tree boosting system,” in *Proc. ACM SIGKDD Int. Conf. Knowl. Discov. Data Min.*, pp. 785–794, 2016.
- [15] C. Cortes *et al.*, “Support-vector networks,” *Mach. Learn.*, vol. 20, pp. 273–297, 1995.
- [16] J. Peng *et al.*, “An introduction to logistic regression analysis and reporting,” *J. Educ. Res.*, vol. 96, pp. 3–14, 2002.
- [17] D. Chicco and G. Jurman, “The advantages of the matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation,” *BMC Genomics*, vol. 21, no. 1, p. 6, 2020.
- [18] A. Buja *et al.*, “Enhancing cyber security in industrial internet of things systems: An experimental assessment,” in *Proc. Mediterran Conf Embed Comput.*, pp. 1–5, 2023.