UDC 004.77.056. DOI: 10.18372/2073-4751.85.21087

Alkema V. V.,
orcid.org/0009-0000-0009-8237,
vitalii.alkema@gmail.com,
Bilonenko V. U.,
orcid.org/0009-0002-7941-7249,
vladyslav.bilonenko@npp.kai.edu.ua

AN AGENT-BASED MODEL FOR THE EARLY DETECTION OF TRUST ANOMALIES IN INDUSTRIAL IOT NETWORKS

State University "Kyiv Aviation Institute"

Introduction

Industrial Internet of Things (IIoT) networks operate under dynamic conditions characterized by changing traffic patterns, heterogeneous devices, unstable communication states, and varying node behavior. In such environments, abnormal processes are not always manifested as explicit failures or sharp traffic deviations. In many cases, early warning signs appear as changes in node trust, including inconsistent data transmission, unstable interaction patterns, reduced communication reliability, or behavior that deviates from expected operational profiles. In this paper, trust anomalies are defined as abnormal deviations in trust-related indicators of IIoT nodes that may reflect compromised behavior, malfunction, false data injection, or communication disruption.

Existing anomaly detection methods in IIoT are mainly focused on traffic statistics, signature-based intrusion patterns, or centralized analytical models. However, such approaches may be insufficient for dynamic industrial environments, where early detection requires distributed observation, local adaptation, and timely interpretation of node behavior. In this context, an agent-based model is considered as a distributed structure in which autonomous agents monitor node behavior, evaluate trust-related changes, exchange local observations, and support the early identification of suspicious deviations. The aim of this study is to develop an agent-based model for the early detection of trust anomalies in Industrial IoT networks. To achieve this aim, the study focuses on defining the role of agents in distributed monitoring, determining the indicators associated with trust anomalies, and describing the interaction mechanism that enables early anomaly detection in dynamic IIoT conditions.

Problem Statement

The problem addressed in this study is the early detection of abnormal node behavior in dynamic Industrial IoT networks, where changes in trust-related characteristics may indicate compromised operation, communication instability, or data inconsistency before explicit failures occur. In distributed industrial environments, centralized monitoring is often constrained by delayed response, limited scalability, and low sensitivity to local behavioral changes. At the same time, trust anomalies are not always directly observable through conventional traffic-based indicators, since they may emerge as gradual deviations in interaction patterns, transmission reliability, or consistency of node actions. Therefore, there is a need for an agent-based monitoring structure that enables continuous distributed observation of network nodes, local evaluation of trust-related indicators, and cooperative interpretation of suspicious deviations. The task is to design such a structure for identifying trust anomalies at early stages under dynamic IIoT conditions, taking into account heterogeneous nodes, changing communication states, and the distributed nature of industrial network infrastructures.

To address this problem, an agent-based monitoring structure is proposed for distributed trust evaluation and early anomaly signaling in Industrial IoT networks.

Agent-Based Monitoring Structure

In the proposed model, the early detection of trust anomalies is performed by a set of interacting agents distributed across the Industrial IoT network. Each agent is assigned a specific monitoring and analytical role and operates on the basis of local observations and inter-agent communication. Such an organization makes it possible to detect suspicious deviations in node behavior at an early stage, without relying entirely on centralized analysis.

The model includes three main agent types. The **local monitoring agent** is associated with an individual IIoT node and continuously observes its operational and communication characteristics, such as transmission regularity, response delay, interaction stability, and data consistency. On the basis of these observations, the agent forms a local description of node behavior.

The **trust evaluation agent** processes the observed indicators and estimates the current trust state of the node. This agent identifies deviations from the expected behavioral profile and determines whether the observed changes may correspond to a trust anomaly. In this study, a trust anomaly is interpreted as an abnormal change in the trust-related characteristics of a node that may indicate compromised operation, communication disturbance, or unreliable data exchange.

The **coordination agent** integrates local signals received from several agents and supports the final interpretation of suspicious states at the network level. Its role is especially important in dynamic IIoT conditions, where isolated local deviations may not always be sufficient for anomaly confirmation, while a combination of several weak signals may indicate an emerging abnormal process.

The interaction of these agents forms the basis of the proposed detection algorithm. At the first stage, the local monitoring agent collects current node indicators. At the second stage, the trust evaluation agent transforms these indicators into a trust-related assessment and compares the result with the expected operating profile. At the third stage, if the deviation exceeds the admissible level, the corresponding signal is transmitted to the coordination agent. At the final stage, the coordination agent aggregates local anomaly signals and generates an early warning about a possible trust anomaly in the Industrial IoT network.

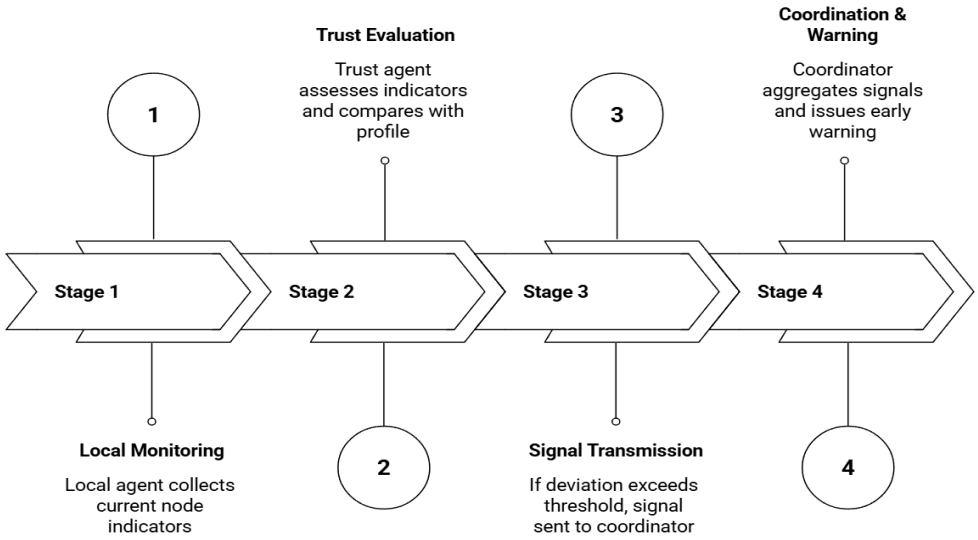

Fig 1. Main Stages of the Proposed Agent Based Trust Anomaly Detection Algorithm

Trust Indicators and Decision Rule

After the agent-based monitoring stages are completed, the node state is assessed using a compact set of trust-related indicators, including data consistency, communication stability, packet delivery regularity, response delay, and interaction reliability. These indicators characterize the stability and reliability of node behavior in the Industrial IoT network. A trust anomaly is assumed when one or more of these indicators exhibit a persistent deviation from the expected operating profile.

To obtain an integral estimate of node trust, the following expression is used:

$$T_i = \sum_{k=1}^{m} w_k \, x_{ik}, \qquad (1)$$

where $T_i$denotes the trust score of node i, $x_{ik}$are normalized values of trust-related indicators, and $w_k$are their corresponding weights. Based on the calculated trust score, the anomaly decision is made according to the rule

$$A_i = \begin{cases} 1, & \text{if } T_i < \theta, \\ 0, & \text{otherwise}, \end{cases} \qquad (2)$$

where $A_i$indicates the presence of a trust anomaly and $\theta$is the detection threshold. Thus, the proposed rule makes it possible to transform locally observed deviations into a compact decision criterion that can be used by agents for the early identification of suspicious node behavior.

According to (1), the trust score is formed as a weighted combination of normalized indicators, while rule (2) is used to generate the anomaly flag when the score falls below the specified threshold.

Illustrative Scenario

To illustrate the operation of the proposed model, a synthetic monitoring scenario was considered for an Industrial IoT network with a sensor node observed over a sequence of time windows. Since the study is focused on the conceptual validation of the agent-based detection logic, the input data were generated synthetically in order to reproduce typical node behavior under normal, degraded, and anomalous operating conditions. For each observation window, a set of trust-related indicators was formed, including data consistency, communication stability, packet delivery regularity, response delay, and interaction reliability. The generated values reflect gradual changes in node behavior rather than abrupt failures, which is consistent with the objective of early anomaly detection.

At the initial stage of the scenario, the node operates in a normal mode, characterized by stable communication, regular packet exchange, low delay, and consistent transmitted data. Under these conditions, the local monitoring agent records indicator values close to the expected operating profile, and the calculated trust score remains above the detection threshold. At the next stage, the node enters a degraded state, in which communication stability begins to decrease and response delay becomes less predictable. In addition, small inconsistencies in transmitted data and interaction patterns appear. Although these deviations are still insufficient to indicate an explicit failure, they lead to a gradual reduction in the integrated trust score calculated according to (1).

At the final stage, the accumulated deviations become persistent. In this case, the trust evaluation agent identifies that the trust score falls below the threshold defined by rule (2). After that, a local anomaly signal is transmitted to the coordination agent, which aggregates the received signal and generates an early warning about a possible trust anomaly associated with the observed node. Thus, the scenario demonstrates how the proposed model can identify suspicious node behavior before the occurrence of a clear system-level failure.

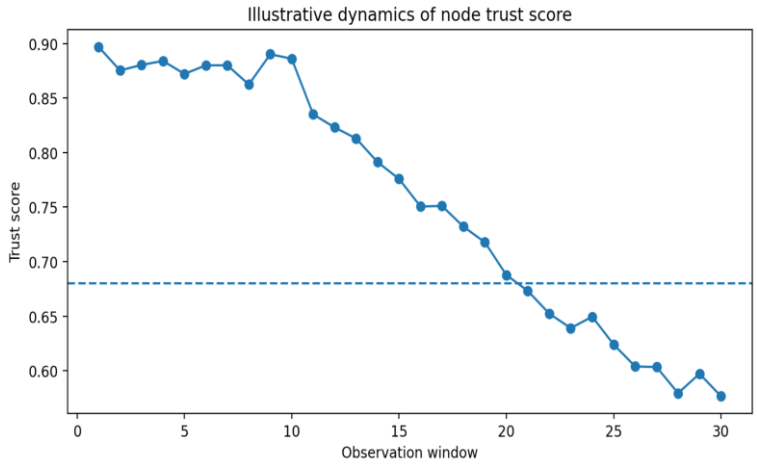

Fig 2. An illustrative example of the trust score dynamics for the monitored node.

In the normal state, the score remains relatively stable; during the degradation stage, it gradually decreases; and after crossing the threshold, the anomaly condition is detected. This behavior confirms that the proposed agent-based model can support early identification of trust anomalies in dynamic Industrial IoT conditions.

Conclusions

This paper proposed an agent-based model for the early detection of trust anomalies in Industrial IoT networks. The model is based on the interaction of local monitoring, trust evaluation, and coordination agents, which together support distributed observation of node behavior and early identification of suspicious deviations. A compact set of trust-related indicators and a threshold-based decision rule were used to formalize anomaly detection. The illustrative scenario showed that gradual degradation of node behavior leads to a reduction in the trust score and allows anomaly signaling before explicit failure becomes evident. The obtained results confirm that the proposed approach can be applied as a conceptual basis for distributed trust monitoring in dynamic Industrial IoT environments. Further research may focus on adaptive threshold selection, weighting of trust indicators, and validation of the model on simulated or real IIoT datasets.

References

1. Konsta A. M., Lluch Lafuente A., Dragoni N. Trust Management for Internet of Things: A Systematic Literature Review. arXiv. 2022. 25 p
2. Pustelnyk P. Real-Time Anomaly Detection in Distributed IoT Systems. 2025. P. 162–171
3. Sagar S., Mahmood A., Sheng Q. Understanding Trust Management in Social Internet of Things: A Survey. 2022.
4. Apte M., Kelkar S. Gateway-Based Trust Management System for Internet of Things. Revista Gestão Inovação e Tecnologias. 2021.
5. Ahmed S., Mahmood A. Trust-Aware Intrusion Detection in IoT Using Machine Learning. IEEE Transactions on Industrial Informatics. 2023. Vol. 19(4). P. 3201–3212.
6. Kumar P., Singh R. Distributed Intrusion Detection in IoT Using Multi-Agent Systems. Journal of Network and Computer Applications. 2021. Vol. 186. P. 103089.
7. Radanliev P. et al. Cyber Risk at the Edge: Current and Future Trends in IIoT Security. Future Internet. 2022. Vol. 14(3). P. 85.

Alkema V., Bilonenko V.

AN AGENT-BASED MODEL FOR THE EARLY DETECTION OF TRUST ANOMALIES IN INDUSTRIAL IOT NETWORKS

The paper proposes an agent-based model for the early detection of trust anomalies in Industrial Internet of Things networks operating under dynamic conditions. The relevance of the study is determined by the need for timely identification of abnormal node behavior that may indicate communication instability, compromised operation, false data injection, or data inconsistency before explicit failures occur. The proposed model is based on the interaction of local monitoring agents, trust evaluation agents, and a coordination agent, which together provide distributed observation of node behavior and cooperative interpretation of suspicious deviations. A compact set of trust-related indicators is used, including data consistency, communication stability, packet delivery regularity, response delay, and interaction reliability. To formalize anomaly detection, an integrated trust score and a threshold-based decision rule are introduced. An illustrative synthetic scenario is presented to demonstrate the operation of the proposed model under normal, degraded, and anomalous node states. The results show that gradual degradation of trust-related indicators leads to a decrease in the trust score and enables early anomaly signaling before explicit system-level failure becomes evident. The proposed approach can be used as a conceptual basis for distributed trust monitoring in dynamic Industrial IoT environments.

Keywords: *Industrial Internet of Things; trust management; trust anomalies; early anomaly detection; agent-based architecture; distributed monitoring; cyber-physical systems*

Алькема В., Білоненко В.

АГЕНТНА МОДЕЛЬ ДЛЯ РАННЬОГО ВИЯВЛЕННЯ АНОМАЛІЙ У РІВНІ ДОВІРИ В ПРОМИСЛОВИХ МЕРЕЖАХ ІНТЕРНЕТУ РЕЧЕЙ

У статті запропоновано агентну модель раннього виявлення аномалій довіри в мережах промислового Інтернету речей, що функціонують у динамічних умовах. Актуальність дослідження зумовлена потребою своєчасного виявлення аномальної поведінки вузлів, яка може свідчити про нестабільність комунікації, компрометацію вузла, ін'єкцію хибних даних або порушення узгодженості передавання інформації ще до виникнення явних відмов. Запропонована модель ґрунтується на взаємодії агентів локального моніторингу, агентів оцінювання довіри та координаційного агента, які забезпечують розподілене спостереження за поведінкою вузлів і спільну інтерпретацію підозрілих відхилень. Для оцінювання стану вузла використано компактний набір індикаторів довіри, зокрема узгодженість даних, стабільність комунікації, регулярність доставки пакетів, затримку відповіді та надійність взаємодії. Для формалізації виявлення аномалій введено інтегральний показник довіри та порогове правило прийняття рішення. Для демонстрації роботи моделі наведено ілюстративний синтетичний сценарій, який відображає нормальний, деградований та аномальний стани вузла. Показано, що поступове погіршення індикаторів довіри призводить до зниження інтегрального показника довіри та забезпечує раннє сигналізування про аномалію до настання явної системної відмови. Запропонований підхід може бути використаний як концептуальна основа для розподіленого моніторингу довіри в динамічних середовищах промислового Інтернету речей.

Ключові слова*: Промисловий Інтернет речей; управління довірою; аномалії довіри; раннє виявлення аномалій; архітектура на основі агентів; розподілений моніторинг; кіберфізичні системи.*

Стаття подана до редакції: 23/03/2026
Стаття прийнята до опублікування: 27/03/2026
Стаття опублікована: 27/04/2026