An Ambient Intelligence Approach to Provide Secure and Trusted Pub/Sub Messaging Systems in IoT Environments

Geetanjali Rathee[a], Chaker Abdelaziz Kerrache[b,*], Carlos T. Calafate[c]

[a]*Department of Computer Science and Engineering, Netaji Subhas University of Technology, Dwarka Sector-3, New Delhi-110078, India*
[b]*Laboratoire d'Informatique et de Mathématiques, Université Amar Telidji de Laghouat, 03000 Laghouat, Algeria*
[c]*Computer Engineering Department (DISCA), Universitat Politècnica de València, 46022 Valencia, Spain*

Abstract

Ambient Intelligence (AmI) is defined as a high-quality vision technology where content and information can be sensed and adopted from anytime, anywhere, and by any user in the environment. Much of the research in this area has focused on several aspects of AmI, such as computational and storage complexity, accuracy, and transmission criteria. However, few works have focused on the various trust and security concerns associated to the message publish/subscribe (Pub/Sub) procedure when the on-the-fly technique is adopted. In fact, malicious devices may easily breach the legitimate devices with the aim of degrading the security and privacy in the network. The aim of this paper is to propose a secure and trusted on-the-fly Pub/Sub communication mechanism where the trust and transmission among various devices occurs by computing their trust using indirect factors. In addition, the accuracy and legitimacy of each communicating device is validated using a reinforcement learning scheme. Moreover, the proposed solution is validated and verified against various security measures over a traditional approach.

⋆Fully documented templates are available in the elsarticle package on CTAN.

*Corresponding author
Email addresses: geetanjali.rathee123@gmail.com (Geetanjali Rathee), ch.kerrache@lagh-univ.dz (Chaker Abdelaziz Kerrache), calafate@disca.upv.es (Carlos T. Calafate)

Keywords: Secure AmI; Malicious network security; trusted network; IoT; Trusted AmI; Pub/Sub Messaging Systems

1. Introduction

The recent advancements in supporting embedded systems, along with extensive technological efforts of both industry and academic, have made it possible to design modern in-house intelligent environments such as smart systems [1]. Smart environments support the physical infrastructure and intelligent frameworks by uniquely sensing and adopting independent decision-making without human intervention. The mechanism that controls the behavior of its surroundings by interacting with various actuators, sensors and intelligent devices to make on-the-fly decisions is known as Ambient intelligence (AmI) [2] (see Figure 1). The overall structure of the transmission process can be easily understood using Figure 1, which presents an overview of AmI Publish/Subscribe (Pub/Sub) messaging communication systems, and where the ambient network is divided into a number of subnetworks in order to speed up the transmission process. Each communicating device has its own trust value that is computed via an indirect scheme that can further analyze the legitimacy of each device. In addition, the reinforcement learning, along with indirect computation, may further categorize the system into two different categories such as legitimate and malicious. AmI is considered as one of the most promising technologies in the field of near-future IoT systems where the physical environment deals with humans in an unobstructive and intelligent manner [3, 4]. The rapid growth of IoT mechanisms has enabled various organizations to adopt techniques such as network edges, industry 4.0, smart environments, etc. [5, 6]. AmI is defined as a high-quality and futuristic vision of intelligent and responsive computing technologies where content and information can be sensed, and adopted from anytime, anywhere, and by any user in the environment. The technique is intended to minimize the intervention of humans by taking decisions autonomously and intelligently. A significant number of Pub/Sub messaging techniques have been

proposed by several academicians and scientists for further improving the decision making and accelerate responses in network data forwarding using the on-the-fly approach. However, with the increasing number of IoT devices, and the requirement to make significant decisions in real time, the system leads to a vast variety of generated information, computations and exchanges [7].

Furthermore, the generation of information by such a huge number of smart devices leads to compatibility, scalability, trust and security issues, where it becomes very crucial to determine the legitimate number of devices in the network [8, 9]. In fact, various mechanisms were proposed in the recent literature that address the aforementioned issues [10, 11, 12, 13, 14]; however, very few of them focus on trusted and secure frameworks for AmI.

The involvement of untrusted smart devices in the network, enabling intruders to steal the ideal device's identity and to breach security, generates various networking and security issues such as denial of service, congestion, network jamming, authentication delays, etc. [15, 16, 17]. The intruders may further steal the identity of authentic communicating devices, and act as legitimate devices for some amount of time. However, as the transmission process begins, these fake devices initially acting as legitimate, start behaving maliciously, and may perform a number of security breaches inside the network.

The malicious devices may take part in the communication process by generating fake or fraudulent information, spam records, or unverified systems, which may further hinder network performance. Organizations are not able to fully adopt AmI technology because of these concerns, as they completely rely on their network for sending, transmitting and forwarding confidential and sensitive information. Designing a trustworthy computation system is considered crucial in such a heterogeneous scenario. As a result, quantifying trust reliably for futuristic IoT methods, and in particular the concept of trust in AmI, is considered as a very difficult and a crucial concern. It further encouraged significant efforts by both academia and industry in this research area.

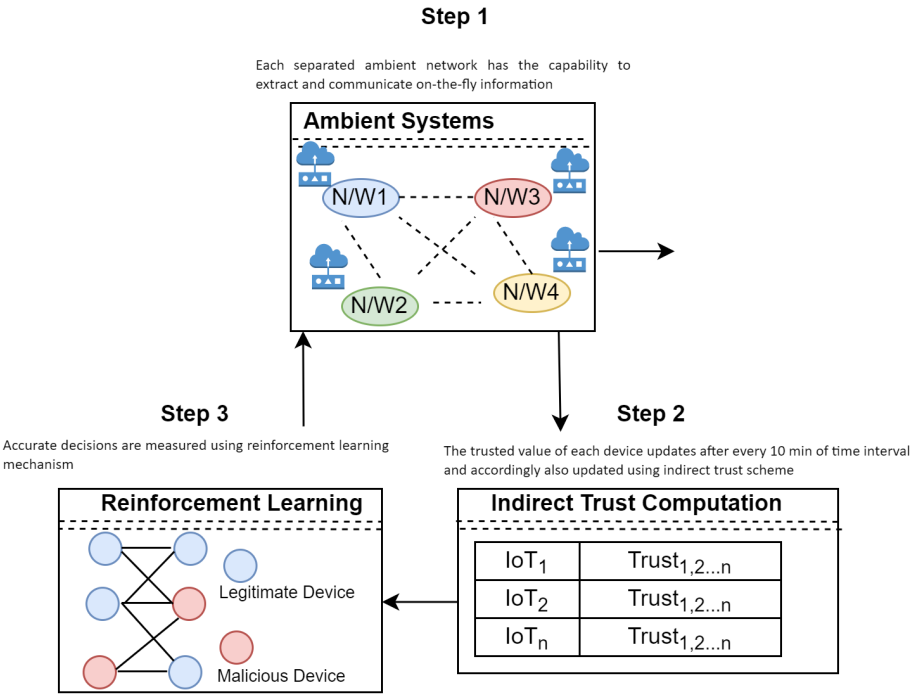

Figure 1: Overview of an Ambient Communication System.

1.1. Motivation

In the past few years, scientists and academic communities have started considering smart systems, future IoT mechanisms, cybersecurity and AmI for evaluating a secure and trusted communications environment. Some of the issues, such as computational storage and on-time responses, have been elaborated in [18, 11, 19]. However, most of them still hamper an accurate and authenticated context transmission among AmI elements in an IoT network. In addition, in the literature, we find that several authors have conducted research focusing on the trust schemes; they have mostly addressed key distribution and the encryption framework elaboration process, for identifying the legitimacy of devices. However, the accurate recognition of fraudulent systems introduces delay and computational overhead associated to analyzing the trust among de-

vices, leading to the same research question. The problem of selecting a reliable and accurate trust mechanism and computation process has not been solved effectively. Moreover, most of the traditional approaches have less capability to identify or distinguish between malicious and legitimate devices in the network. The basis of the aforementioned countermeasures remains mostly unexplored in the environment, and has become a challenging task in AmI systems. In addition, most of the researchers presented a number of mechanisms and schemes for ensuring a secure and efficient mechanisms by solely focusing on computational and storage overhead issues. Furthermore, very few of them have actually focused on providing a secure communication mechanism.

1.2. Contribution

By focusing on the concerns referred above regarding AmI, and on the basis of literature review, this paper presents an integration of reinforcement learning and indirect trust assessment. The trust values are generally hosted at the IoT devices while performing the communication in the network. The trust values are updated by recognizing the transmitting or receiving patterns of information. They are initially randomly allocated at the time of network establishment, and they can be further increased or decreased depending on future communications and on the transmissions of Pub/Sub messages in the environment. The proposed solution resolves the issues of conventional approaches whereby devices (both malicious and legitimate) are communicating on-the-fly, without any verification. Simulation results evidence that the proposed approach outperforms alternative solutions in terms of accurate decisions, sensing accuracy, and trusted devices' involvement during communication process. The main achievements of the paper are described as follows:

- An indirect trust mechanism [20] is proposed focusing on the issue of fraudulent devices attempting to disrupt the Pub/Sub messaging communication mechanism in the network. The trust values are computed using an indirect method to discriminate between legitimate and malicious devices in the network.

- A reinforcement learning mechanism [21] is further adopted to make accurate and significant decisions by sensing and interpreting the transmitted information in the network. The devices having ideal trust values may further participate in the learning and sensing process to accelerate on-the-fly decisions and transmissions. The indirect trust is used to identify the overall behaviour of the different system actors. The trust values are computed using an indirect method to classify legitimate and malicious devices in the network to allow or deny future transmissions. However, in order to sense the altered behaviour of any device, and to determine the accuracy of measuring the shift in device behaviour from legitimate to malicious, reinforcement learning is used continuously to sense the network and measure the accuracy in the system by tracing the behaviour of each communicating device in the network. Yet, in case of relying solely on the indirect trust, intruders may avoid being detected by slowly altering their behaviour so that their trust values will change at a very small rate, hence avoiding being detected in a timely manner in the network. By combining the devices' trust values and the reinforcement learning-based approach, the proposed mechanism is validated against a conventional mechanism for various security metrics including accuracy, reliability, malicious behaviour detection, and adaptability.

The remainder of this paper is structured as follows. Section 2 provides a review of recent literature on security measures for AmI and futuristic IoT applications. Section 3 describes the proposed solution in detail, including indirect and reinforcement learning mechanisms. Then, section 4 presents the experimentation and verification approach, comparing the performance of several security measures in AmI environments against traditional schemes. Finally, section 5 concludes the paper and discusses improvements upon the current work.

2. Related Work

Lashmi and Pillai [22] have proposed a decision support mechanism for identifying the intruders in intelligent ambient devices. They have proposed a home-based security ambient system by focusing on anomaly identification and face recognition techniques to determine the individuals' activities. In addition, the proposed solution sends alert messages to family members and authorities by enabling real-time capturing and monitoring of anomalies using IoT devices. The authors claimed a better proposed mechanism with a high performance outcome for intelligent ambient systems. Shabisha et al. [23] proposed a novel and enhanced security system for identifying emergency situations in healthcare environments. The proposed mechanism uses an authentication and key agreement mechanism for ensuring the untraceability and anonymity by relying on symmetric key operations. The authors developed a commercial off-the-shelf system that verified the validity against various existing mechanisms. The proposed solution claimed to be capable of identifying medical data transmissions, and to generate alerts and emergency warnings. Jia et al. [24] surveyed ambient communication mechanisms, and considered two parameters such as distance and sensitivity for backscatter transmission systems. The authors have established a mathematical framework based upon distances among backscatter nodes and transceivers to achieve path differentiation. In addition, they have designed an energy-based detector by analyzing the probability outcome of harvesting at bit error and tag rates. Table 1 illustrates the limitations and techniques proposed by various researchers in order to provide an efficient and secure communication mechanism for ambient systems.

Zhang et al. [25] have studied access control strategies, including device association and coefficient designs, from a network perspective. In addition, the authors have proposed both offline and online access control mechanisms by assuming the channel information. The authors have proposed a dual decomposition and convex functions for transforming the non-concave issues, designing a distributed controlling strategy. Furthermore, the authors have designed a

Table 1: Recent work on Secure and Trusted IoT Environments

Authors	**Technique**	**Definition**	**Limitation**
Lashmi et al. [22]	Decision Support Mechanism	Sends an alert messages to family members and authorities by enabling real-time capturing and monitoring of anomalies using IoT devices	Delay in real time monitoring
Shabaisha et al. [23]	Enhanced Security System	Ensuring the untraceability and anonymity by relying on symmetric key operations	Storage overhead
Jia et al. [24]	Ambient Communication Mechanism	mathematical framework based upon distances among backscatter nodes and transceiver	Communication and computation delay
Zhang et al. [25]	Dual decomposition and dual function	The authors have designed a combinatorial access control and multi-armed strategies	Computation latency
Lee et al. [26]	Trusted ontology framework	The proposed mechanism determined how the trust degree is estimated based on a trust ontology	Higher trust evaluation
Nguyen et al. [27]	Web-based application	The case study suggested the applicability of the trust-aware recommendation and ambient systems in the network	Communication latency

combinatorial access control and multi-armed strategies. The proposed solution is simulated for various security metrics in comparison of several benchmarked approaches. Lee et al. [26] have proposed a trusted ontology framework for individuals for personalized ontologies according to their perspectives, preferences and purposes. The proposed mechanism is evaluated by determining how

the trust degree is estimated based on a trust ontology. Saini et al. [28] have articulated and exemplified the requirement of reliability and trust over a period of time among different ambient systems environments. The author focused on two significant factors such as reliability while working in different networking environments, and trust factors that are required among devices while transmitting information. Nguyen et al. [27] have contributed a novel scheme and a definition of trust extended to several domains based on social patterns and events. In addition, the authors have proposed a web-based application for analyzing and gathering the information among various data resources. The case study also suggested the applicability of the trust-aware recommendation and ambient systems in the network. Mkpa et al. [29] have proposed a holistic decentralized mechanism based on blockchain technology to support assisted living environments. The proposed mechanism relied on smart contracts by defining the interaction rules that collaboratively contributed to computing and storage resources. It also promoted improved privacy and trustless interaction alliances. The proposed solution addressed the shortfall of storage measures exhibited in several intelligent systems.

Overall, despite researchers have projected a number of mechanisms and schemes, most of them focused solely on computational and storage overhead issues. Furthermore, very few of them have actually focused on providing a secure communication mechanism. This paper presents a secure and trusted communication system while reducing the computational and storage overhead in the environment.

3. Proposed Approach

This section introduces a security framework where an indirect trust mechanism is adopted to address the issue of fraudulent devices that attempt to disrupt the Pub/Sub messaging systems. The trust values are computed using an indirect method to discriminate between legitimate and malicious network devices. In addition, a reinforcement learning mechanism is adopted to make

accurate and significant decisions by sensing and interpreting the transmitted information in the network. The reinforcement learning is based on five different principles starting from taking the input from the environment to train the network or provide inference. The system will initially take some input which determines its efficiency. The input changes over the time, that simply determines how well the system behaves according to the given input. The system will infer using decision Markov model where the given input further decides the acceptance or rejection of the state by analysing its behaviour. The system will infer according to the inputs behaviour that decides on the acceptance or the rejection of the input state using decision Markov model.

Figure 2 illustrates the system design of the proposed security mechanism which consists of two major components: indirect trust and reinforcement learning. Below we proceed to detail both components.

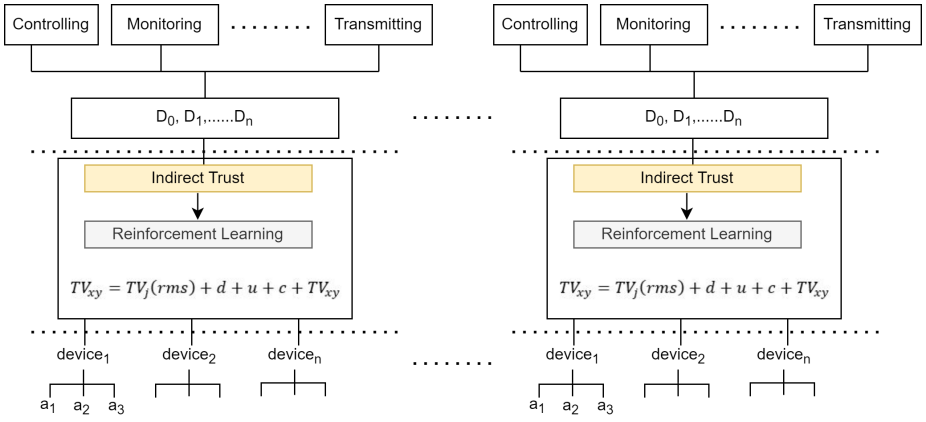

Figure 2: Proposed Security Framework.

3.1. Indirect Trust

In our solution, indirect trust is used to measure the legitimate behavior of any communicating device. In order to compute the trust of any device during the communication mechanism, the device that computes the trust of other device is called evaluation device and the device whose trust is being measured

is called evaluated device. The evaluated device x computes the trust value of device y by measuring from various associated devices. The indirect trust value computed by device x evaluates the trust of device $I_1, I_2, \ldots . I_n$ in order to finalize the trust value of device y. Therefore, the involvement of various devices in the network increases the possibility of an accurate trust measure by each evaluated device d. The fake trust value (lower trust value) produced by malicious devices can be involved while computing the overall trust of a device. Hence, it is needed to filter out the number of fake trust values produced by the intruders by analyzing various impact factors that affect their trust. The indirect trust value is used to determine the comprehensive analysis of indirect trust required to filter the fake results. The text below details the filtering out process of devices having a lower trust values using the proposed indirect scheme.

Step 1: A significant threshold is needed for analyzing the highly trusted, trusted, medium, lesser trusted and fake devices in the network by considering various factors. 0.47 is the threshold value set by our proposed system to filter out the devices into certain categories. If a network or a device whose trust value is less than 47% will be considered as highly infected device. The infected device will start completely starts behavior according to intruders' behavior. The highly infected devices, whose trust value is much lower than the threshold, can be automatically or directly analyzed and filtered out by the systems by checking their trust values. Furthermore, a direct formula can be used to directly block the highly infectious devices, i.e.:

$$TV_j(rms) = \frac{\sqrt{\sum_{z=1}^{n} TV_j^2}}{n} \tag{1}$$

where $(TV)_j(rms)$ defines the root mean square trust value of device j among n devices in the network.

Step 2: Recommender trust: $(TV)_{xny}$ is the direct trust of subject I to recommender y, and $(TV)_{ynx}$ is the recommendation trust of recommender k to device y, and k needs to recommend this trust to device i.

$$d = |TV_{xny} - TV_{ynx}| \tag{2}$$

Step 3: Degree of understanding and recommended conflict: It is computed based on the number of previous successful interactions of a device x over a period of time, and k deviations between device x and device m to recommend the trust value of device y.

$$U = \frac{S}{N} e^{-\lambda(t-\delta t)} \tag{3}$$

$$C = \frac{\sum_{n!=m} |t_{kn} - t_{km}|}{n} \tag{4}$$

The hierarchical trust device is used to recommend the trust of m devices after pruning and filtering the m devices' recommendations as:

$$TV_{xy} = \frac{1}{m} \sum_{p=1} mTV_{xkp} \times TV_{kpy} \tag{5}$$

The overall indirect trust value of device x over an intermediate number of devices is computed as:

$$TV_{xy} = TV_j(rms) + d + u + c + TV_{xy} \tag{6}$$

In order to handle the large dimensional and dynamic features of the AmI environment, it is further needed to approximate the action-value function by defining Q-learning selections. In order to analyze the reinforcement algorithm, it is needed to measure the state, action and reward function space of the network. We have motivated to use the reinforcement learning scheme from Liu et al. [21] in order to understand the trust, and to continuously measure the trusted environment during on-the-fly transmissions of an AmI system. Below we detail the complete description of state, action and reward function solution as follows:

3.2. Reinforcement Learning

State space: In order to take a decision about the legitimacy of the device regarding a transaction of size η, the distribution of indirect trust delta, the coordinates associated to the devices' location y, the computing capacity of each device $dc = dc$, and the information transmission rate for links between each pair of devices $TR = (TR)_{x,y}$ at an epoch t $t = 1, 2, \ldots n$ must be taken into account; hence, the state space can be denoted as:

$$SS^t = \eta, \delta, y, d_c, TR^{(t)} \tag{7}$$

Action space: In order to improve the overall throughput of the network, a number of trusted parameters should be adjusted to adapt to the dynamic and changing behavior of the network. This includes the trust producer's alpha, the trust selection zeta, the information size I_d, and the data interval D_i. Formally, the action space can be expressed at a decision epoch t where $t = 1, 2, \ldots n$ by:

$$AS^{(t)} = \alpha, z, I_D, {D_I}^{(t)} \tag{8}$$

where the trust producer indicator is $\alpha = \alpha_n, \alpha_n \epsilon \{0, 1\}$

Reward function: It is used to maximize or speedup the devices legitimacy verification while guaranteeing the significant throughput; flexibility is required at each epoch to solve the following issues:

$$\begin{aligned} \chi = max_a Q(s, a) \\ P1 : G() \leq \phi_s, G(\lambda) \leq \phi_t \\ P1 : TR_r^{(fun)} \leq W \times TR_r, \eta = 0, 1, 2... \\ P3 : f \leq F^{\phi}, \phi = 0, 1, 2.. \end{aligned} \tag{9}$$

Whereas, the indirect trust value, the dynamic behaviour of each device and the scalable nature of the proposed system can be measured using two typical factors (i.e., indirect distribution scheme and coordination location method). In

order to measure the inequality, a Gini coefficient of the trust producers can be computed as:

$$G(\eta) = \frac{\sum ub_x \epsilon\delta_D \sum ub_y \epsilon\delta_D |\eta_{bx} - \eta_{by}|}{2\sum ub_x \epsilon\delta_D \sum ub_y \epsilon\delta_D \eta_{bx}}$$
$$G(\eta) = \frac{\sum ub_x \epsilon\delta_D \sum ub_y \epsilon\delta_D |\eta_{bx} - \eta_{by}|}{2k\sum ub_x \epsilon\delta_D \eta_{bx}} \tag{10}$$

It is defined as the half of RMS difference that is mathematically equivalent to the Lorenz curve definition. The absolute difference is computed by the average absolute difference of all item pairs, and the RMS difference is the mean absolute difference divided by an average. Since the Gini coefficient is a density distribution $D\lambda(x)$, it can be further recomputed as the following integration function:

$$G_{IF}(D_\lambda) = \frac{\int\int D_\lambda(x) - D_\lambda y|dydx}{2k} \tag{11}$$

Algorithms 1, 2 and 3 elaborate on the the process of secure communications in ambient systems using indirect trust and reinforcement learning scheme. The indirect trust measures the trust of each device in order to detect their behavior as either legitimate and malicious, while the reinforcement learning method is used to further fasten up and achieve a continuous surveillance of the environment while making an accurate decision over the network.

4. Performance Analysis

In order to validate and demonstrate the effectiveness of the proposed solution in terms of accuracy, reliability and trust computation when handling on-the-fly interactions between devices, we have performed a set of extensive numerical simulation results to analyze the security on the basis of a synthesized real-world dataset. The proposed framework simulation is entirely based upon NetLogo [30], which is particularly suitable for exploring and modelling complex environmental systems. The proposed approach is validated and evaluated from various perspectives such as: 1) accuracy, that is used to determine

Algorithm 1 Trusted and accurate decision during transmission

Input: A network 'N' having 'd' devices separated into two different categories i.e., legitimate and malicious
Output: System is able to identify the behavior of devices and take an accurate decision while making the transmission
Requirement: System is ideal (all the devices are legitimate) in nature during the establishment and keeps changing with 5%-35% alteration of legitimate devices into malicious
For 'd' = 1 to 'n' **do**
Compute the behavior of each communicating device using indirect method
Call **Indirect Trust ()**
if the device 'd' is legitimate **then**
    Reinforcement process is used to make an accurate decision in order to speed up the process
Call **Reinforcement Learning process ()**
else
    device 'd' is malicious
end if

Algorithm 2 Indirect Trust calculation

Input: A network 'n' consist of having 'd' devices
Output: The IoT devices are either legitimate or malicious
Step 1: **For** 'd' = 1 to 'n' **do**
Step 2: Compute threshold using eq. (1)
Step 3: Calculate indirect trust using eq. (6)
if (device 'd'==legitimate) **then**
    Device is considered as legitimate
    Continue further process by the device 'd+1' in the network
else
    Device 'd' is malicious
    Block device 'd' for further communication from the network
end if

Algorithm 3 Reinforcement Learning Process

1: **Input:** A network 'n' consisting of 'd' devices
2: *Step 1:* **For** 'd' = 1 to 'n' **then**
3: *Step 2:* Compute State space of legitimate devices using eq. (9)
4: *Step 3:* Compute Action space to measure the overall throughput using eq. (10)
5: *Step 4:* Compute Reward function to maximize and speed up the accurate decision process using eq. (11)

the accuracy of trustworthiness computation; 2) reliability, which is used to measure the systems reliability in terms of malicious devices availability; 3) the percentage of malicious behavior, which is used to identify the accuracy of measuring the legitimate behavior of each communicating device; and 4) adaptability, which is used to measure the response capacity of the proposed solution when dealing with complicated behavior.

4.1. Dataset description

In order to achieve the research aim, we have considered the given the volume of the available dataset, obtained by crawling individuals' microblogs [31], the evaluation trust of all the devices is impractical. Therefore, we specially concentrated on the suitable number of users/devices who provided incorrect or recent information. In addition, to represent a fine-grain evaluation, the dataset is divided into three basis such as advertising, social, health science, containing 4312, 1320, 1580 devices, respectively.

4.2. Simulation settings

For the numerical simulation, we consider both legitimate and adversary devices publishing either ideal or trustable information, or altered or fake quality information, in a specific interval of time as $I(t)$. Let $P(l)$ represent the proportion of legitimate devices, and $P(m)$ represent the proportion of malicious devices. The time step is defined as the running time of the simulator.

In order to validate the proposed framework, the proposed security framework is simulated against [24] in which the authors have established a mathematical framework based upon distances among backscatter nodes and transceivers to achieve path differentiation. In addition, they have designed an energy-based detector for the readers, and analyzed the probability outcome of harvesting at bit error, along with tag (trust) rates. The proposed phenomenon is simulated against various security concerns with traditional [24] security approaches, as discussed below. In addition, depending on the above dataset and the chosen performance metrics, the simulation parameters are defined in Table 2.

Table 2: Simulation environment of the proposed framework.

Parameters	**Values**
Simulation Time	120s
Devices Type	Static
Grid Area	700m × 700m
Number of Devices	5-50
Wireless Radio Range	25 m
Comparisons Protocols	Ambient backscattering, Reinforcement Learning
Devices Type	Legitimate and Malicious
Dataset Division	Advertising, Social, Health science
Physical layer	PHY 802.11

4.2.1. Accuracy

All the computed trust mechanisms should have significant accuracy in the evaluation environment. In this research, we have used the mean deviation in order to analyze the accuracy of the system. It is defined as:

$$\Gamma(t) = \frac{\sum |T_t - P_t|}{\sum t} \tag{12}$$

where $T(t)$ is the expected value computed at time t, and $P(t)$ is the predicted value of trust at time t. Figure 3 represents the mean deviations of accuracy when classifying devices into either legitimate or malicious categories.

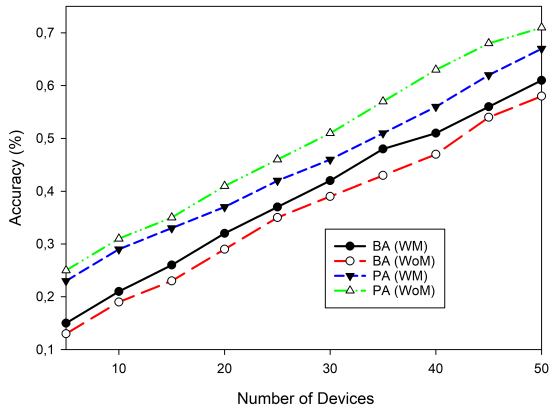

Figure 3: Accuracy values vs. the number of devices, comparing our approach (BA) against PA. The accuracy rate keeps increasing linearly.

The existing Baseline Approach (BA) and Proposed Approach (PA) are simulated for both scenarios where 1) malicious number of devices are included in the network and 2) ideal network where all the devices are legitimate. Besides, WM represents the first scenario where a number of malicious devices are included to the network, and WoM represents the second scenario where all network devices are legitimate.

4.2.2. Reliability

The reliability of the system measures the resiliency in the network; this means it measures how many faults a network can tolerate and still respond correctly to the user's requests. Reliability is defined as the number of legitimate devices able to transmit in the network among the total number of malicious and legitimate devices in the network. It can be expressed as:

$$R(t) = \frac{\sum |L_t - M_t|}{\sum A_t} \tag{13}$$

where $l(t)$ is defined as total number of legitimate devices that transmit information over a period of time t, $m(t)$ determines the total number of malicious devices, and $a(t)$ illustrates the total number of legitimate and malicious devices

that transmit the information in a specific interval of time t.

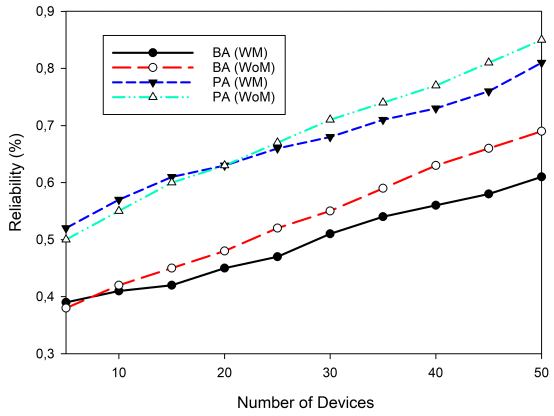

Figure 4: Reliability values vs. the number of devices.

Figure 4 shows a reliability comparison of the proposed mechanism over the traditional method. The indirect trust evaluation and reinforcement learning measures and examines the malicious behavior of the devices. The proposed mechanism outperforms the traditional scheme due to a continuous computation and surveillance of malicious devices, blocking them immediately to prevent further communications in the network.

4.2.3. Percentage of Malicious Behavior during a period of Time

The percentage of malicious behaviour is defined where legitimate devices are being altered and starts behaving maliciously during a period of time in the network. We now proceed by determining the involvement of malicious number of devices over a period of time in the network, and how the system behaves when increasing the number of malevolent devices. In our proposed mechanism, the validity is verified by increasing the malicious number of devices from 15-35% in the network, and then analyzing the performance achieve and the identification accuracy of malicious devices compared to the traditional approach. Figure 5 represents the comparison of ideal identification of malicious number of devices, blocking them in the network after validation. The proposed mechanism is able

to efficiently detect/identify the number of malicious devices upon increasing in the system in comparison to a traditional approach due to the reinforcement learning mechanism.

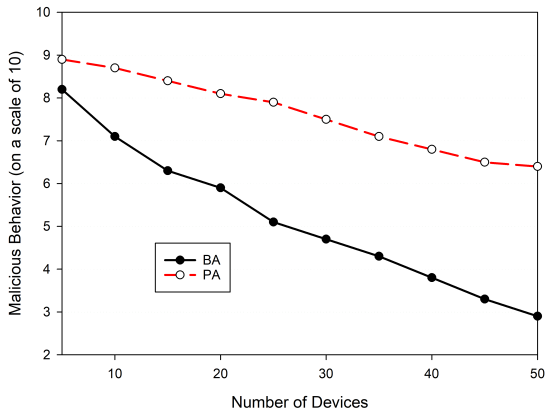

Figure 5: Malicious Behavior values vs. the number of devices.

4.2.4. Adaptability

The system's adaptability is measured in terms of their dynamic behavior. The behavior of the system determines the device's nature such as ideal and malevolent by forwarding the requested information and amount of time required to transmit the requested information to their neighbouring device's. The request or information processed by the legitimate device in the network generally evaluate the overall trust behaviour of the system. It can be further identified as:

$$PB(t) = \frac{\sum_{t=1} tL(t)}{\sum_{t=1} tS(t)} \times 100\% \tag{14}$$

where $PB(t)$ determines the posting behavior of legitimate devices measures in terms of information forwarded by ideal devices or well-behaved devices, and $S(t)$ refers to the total information sent by all the devices over a specified interval of time.

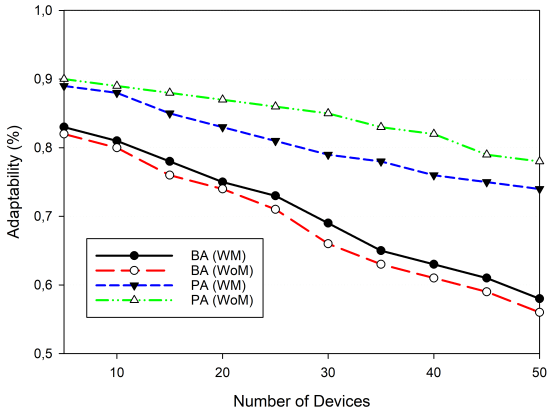

Figure 6: Adaptability values vs. the number of devices.

Figure 6 depicts the adaptability of our proposed solution over an existing scheme by measuring the total amount of information sent by both malevolent and legitimate devices. The proposed mechanism is able to efficiently distinguish between the information sent by both malicious and legitimate devices because of their trust computation mechanism.

4.2.5. False Positive and False Negative

The validation of the proposed solution is also measured for both false positive and false negative metrics. False positives can be defined as the case where a number of devices are identified as legitimate while, actually, the intruders to become malicious alter them. However, a false negative refers to the situation where a number of devices are identified as malicious, despite they are actually legitimate.

Both metrics are measured over the baseline and the proposed approach to further identify the accuracy of the system. Figure 7 depicts the false positive scenario where the proposed approach performs better when compared to the baseline approach; in this context, indirect trust computation reflects the legitimacy of the communicating device. The trusted devices have a higher trust rate, while malicious devices present lower trust values that can be easily traced

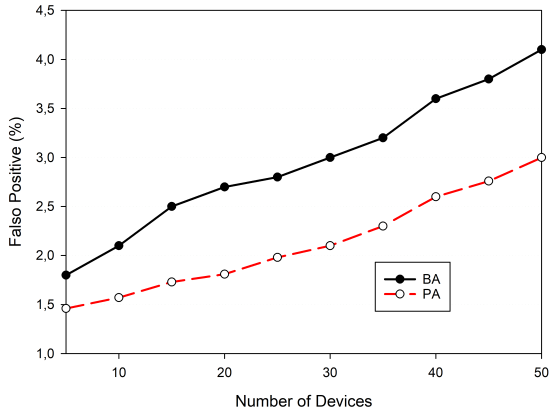

Figure 7: False Positive values vs. the number of devices.

with our proposed approach.

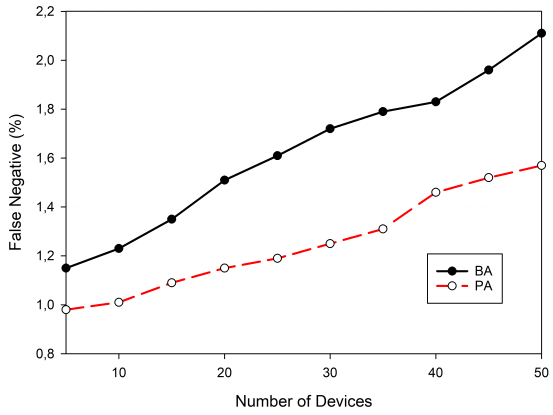

Figure 8: False Negative values vs. the number of devices.

In addition, Figure 8 represents the false negative scenario, where the legitimacy of each communicating device can be easily identified through the reinforcement learning and trusted values. The identification of false negative values is better in the proposed approach as compare to baseline scheme.

5. Conclusions

The involvement of malevolent smart devices in the network, enabling intruders to steal the ideal device's identity and to breach security by generating various security and networking issues. In addition, Organizations are not able to fully adopt new technologies because of these security concern. This paper presents a secure and trusted on-the-fly publish/subscribe messaging system for IoT environments by computing the trust values of each device using indirect factors and a reinforcement learning scheme. The indirect trusted scheme distinguishes between legitimate and malicious devices through their trust values, while reinforcement learning further ensures the accuracy and legitimate transmissions among secured devices in the network. Simulation results for the proposed solution validated its superiority with respect to state-of-art methods [24] for various security metrics. Furthermore, the AmI systems considered for futuristic IoT scenarios provided a reliable and fast transmission mechanism when legitimate devices are segregated from the rest. Moreover, as future work, the various security concerns, such as authentication latency and miners validation delay, both emphasizing upon on-the-fly systems, can be considered and resolved for real-time applications such as intelligent transportation systems and healthcare monitoring.

Acknowledgment

This work is derived from R&D project PID2021-122580NB-I00, funded by MCIN/AEI/10.13039/501100011033 and "ERDF A way of making Europe".

References

[1] J. J. Bryson, Patiency is not a virtue: the design of intelligent systems and systems of ethics, Ethics and Information Technology 20 (1) (2018) 15–26.

[2] F. J. Gutierrez, D. Muñoz, S. F. Ochoa, J. M. Tapia, Assembling mass-market technology for the sake of wellbeing: a case study on the adoption

of ambient intelligent systems by older adults living at home, Journal of Ambient Intelligence and Humanized Computing 10 (6) (2019) 2213–2233.

[3] Z. Falomir, Qualitative descriptors applied to ambient intelligent systems, Journal of Ambient Intelligence and Smart Environments 9 (1) (2017) 21–39.

[4] M. Bahache, A. E. K. Tahari, J. Herrera-Tapia, N. Lagraa, C. T. Calafate, C. A. Kerrache, Towards an accurate faults detection approach in internet of medical things using advanced machine learning techniques, Sensors 22 (15) (2022) 5893.

[5] G. Rathee, S. Garg, G. Kaddoum, B. J. Choi, Decision-making model for securing iot devices in smart industries, IEEE Transactions on Industrial Informatics 17 (6) (2020) 4270–4278.

[6] G. Rathee, M. Balasaraswathi, K. P. Chandran, S. D. Gupta, C. Boopathi, A secure iot sensors communication in industry 4.0 using blockchain technology, Journal of Ambient Intelligence and Humanized Computing 12 (1) (2021) 533–545.

[7] G. Rathee, R. Sandhu, H. Saini, M. Sivaram, V. Dhasarathan, A trust computed framework for iot devices and fog computing environment, Wireless Networks 26 (4) (2020) 2339–2351.

[8] U. Khalil, A. Ahmad, A.-H. Abdel-Aty, M. Elhoseny, M. W. A. El-Soud, F. Zeshan, Identification of trusted iot devices for secure delegation, Computers & Electrical Engineering 90 (2021) 106988.

[9] M. Faisal, I. Ali, M. S. Khan, S. M. Kim, J. Kim, Establishment of trust in internet of things by integrating trusted platform module: To counter cybersecurity challenges, Complexity 2020.

[10] P. Shi, H. Wang, S. Yang, C. Chen, W. Yang, Blockchain-based trusted data sharing among trusted stakeholders in iot, Software: practice and experience 51 (10) (2021) 2051–2064.

[11] W. Wang, H. Xu, M. Alazab, T. R. Gadekallu, Z. Han, C. Su, Blockchain-based reliable and efficient certificateless signature for iiot devices, IEEE transactions on industrial informatics.

[12] E. M. Abounassar, P. El-Kafrawy, A. El-Latif, A. Ahmed, Security and interoperability issues with internet of things (iot) in healthcare industry: A survey, in: Security and Privacy Preserving for IoT and 5G Networks, Springer, 2022, pp. 159–189.

[13] S. S. Kute, A. K. Tyagi, S. Aswathy, Security, privacy and trust issues in internet of things and machine learning based e-healthcare, in: Intelligent Interactive Multimedia Systems for e-Healthcare Applications, Springer, 2022, pp. 291–317.

[14] G. Rathee, C. A. Kerrache, M. Lahby, Trustblksys: A trusted and blockchained cybersecure system for iiot, IEEE Transactions on Industrial Informatics (2022) 1–8doi:10.1109/TII.2022.3182984.

[15] S. Smys, A survey on internet of things (iot) based smart systems, Journal of ISMAC 2 (04) (2020) 181–189.

[16] D. B. Rawat, V. Chaudhary, R. Doku, Blockchain technology: Emerging applications and use cases for secure and trustworthy smart systems, Journal of Cybersecurity and Privacy 1 (1) (2020) 4–18.

[17] S. P. RM, P. K. R. Maddikunta, M. Parimala, S. Koppu, T. R. Gadekallu, C. L. Chowdhary, M. Alazab, An effective feature engineering for dnn using hybrid pca-gwo for intrusion detection in iomt architecture, Computer Communications 160 (2020) 139–149.

[18] M. Numan, F. Subhan, W. Z. Khan, S. Hakak, S. Haider, G. T. Reddy, A. Jolfaei, M. Alazab, A systematic review on clone node detection in static wireless sensor networks, IEEE Access 8 (2020) 65450–65461.

[19] B. Can, A. G. Yavuz, E. M. Karsligil, M. A. Guvensan, A closer look into the characteristics of fraudulent card transactions, IEEE Access 8 (2020) 166095–166109.

[20] B. Su, C. Du, J. Huan, Trusted opportunistic routing based on node trust model, IEEE Access 8 (2020) 163077–163090.

[21] M. Liu, F. R. Yu, Y. Teng, V. C. Leung, M. Song, Performance optimization for blockchain-enabled industrial internet of things (iiot) systems: A deep reinforcement learning approach, IEEE Transactions on Industrial Informatics 15 (6) (2019) 3559–3570.

[22] K. Lashmi, A. S. Pillai, Ambient intelligence and iot based decision support system for intruder detection, in: 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), IEEE, 2019, pp. 1–4.

[23] P. Shabisha, C. Sandeepa, C. Moremada, N. Dissanayaka, T. Gamage, A. Braeken, K. Steenhaut, M. Liyanage, Security enhanced emergency situation detection system for ambient assisted living, IEEE Open Journal of the Computer Society 2 (2021) 241–259.

[24] M. Jia, C. Yao, W. Liu, R. Ye, T. Juhana, B. Ai, Sensitivity and distance based performance analysis for batteryless tags with transmit beamforming and ambient backscattering, China Communications 19 (2) (2022) 109–117.

[25] L. Zhang, G. Feng, S. Qin, Y. Sun, B. Cao, Access control for ambient backscatter enhanced wireless internet of things, IEEE Transactions on Wireless Communications.

[26] O.-J. Lee, H. L. Nguyen, J. E. Jung, T.-W. Um, H.-W. Lee, Towards ontological approach on trust-aware ambient services, IEEE Access 5 (2017) 1589–1599.

[27] H. L. Nguyen, O.-J. Lee, J. E. Jung, J. Park, T.-W. Um, H.-W. Lee, Event-driven trust refreshment on ambient services, IEEE Access 5 (2017) 4664–4670.

[28] N. K. Saini, Trust factor and reliability-over-a-period-of-time as key differentiators in iot enabled services, in: 2016 International Conference on Internet of Things and Applications (IOTA), IEEE, 2016, pp. 411–414.

[29] A. Mkpa, J. Chin, A. Winckles, Holistic blockchain approach to foster trust, privacy and security in iot based ambient assisted living environment, in: 2019 15th International Conference on Intelligent Environments (IE), IEEE, 2019, pp. 52–55.

[30] J. C. Thiele, W. Kurth, V. Grimm, Agent-based modelling: Tools for linking netlogo and r, Journal of Artificial Societies and Social Simulation 15 (3) (2012) 8.

[31] J. Littman, D. Kerchner, Y. He, Y. Tan, C. Zeljak, Collecting social media data from the sina weibo api, Journal of East Asian Libraries 2017 (165) (2017) 12.