SOPHT: a PHase-based Trust management framework for Service-Oriented IoT/IIoT

Runbo Su, Arbia Riahi Sfar, Enrico Natalizio, Pascal Moyal, Ye-Qiong Song

SOPHT: a **PH**ase-based **T**rust management framework for **S**ervice-**O**riented IoT/IIoT

Runbo Su*, Arbia Riahi Sfar‡, Enrico Natalizio†*, Pascal Moyal§, and Ye-Qiong Song*
*LORIA, CNRS, Université de Lorraine, France
‡STD lab, Military Academy of Tunisia
†Autonomous Robotics Research Centre, TII, UAE
§IECL, INRIA, Université de Lorraine, France

Abstract

Industrial IoT (IIoT) is considered as the key technology for boosting Industry 4.0 revolution. However, the introduction of IoT devices and services raises new challenges in terms of cybersecurity. In this paper, a phase-based trust management framework for service-oriented IIoT (SOPHT) is proposed. This trust management (TM) model considers two trust levels at both plant and inter-plant. Plant TM enables the trustworthiness of IIoT plant nodes to be assessed dynamically and diversely in each phase, namely access control, service provider selection, service evaluation, and node classification. Inter-plant TM examines the trust between plants based on a three-phase mechanism. This trust management framework has been simulated under various attacks. The numerical results show its effectiveness and feasibility for safely evaluating the trust score of IIoT services at both plant and inter-plant levels, contributing thus to increasing the plant security and reliability.

Index Terms

Industrial Internet of Things (IIoT), Trust management (TM), Security, Attacks on services, Hybrid architecture.

I. Introduction

Since 'Industry 4.0' was first proposed in Germany [1], the interest and need in using IoT technologies in industry are rapidly growing [2], and the Industrial Internet of Things (IIoT) is becoming the core foundation of smart manufacturing. So far, several countries have announced their national industry 4.0 plan, such as 'Made in China 2025' [3], which was released in 2015. Despite these investments and developments, security issues encountered in IIoT remain insufficiently addressed when facing malicious attacks. To only name a few victims: Iran's nuclear facility in 2010 [4], Thailand's Eyeglass lens manufacturer in 2019 [5], and vaccine maker Pfizer/BioNTech in 2020 [6]. Indeed, all victims above have employed necessary and robust measures in terms of privacy and confidentiality, but they still suffered from financial loss, machine shutdown, or even severe accidents generated by malicious intrusions. Till now, more than 90% of industrial companies are vulnerable to cyber-attacks, according to new research from Positive Technologies [7]. The motivations of such attacks are diverse, including financial gain, espionage, and even criminal goals for creating disruptions and casualties. For this reason, a mechanism that monitors the behaviors of IIoT nodes is needed to secure the IIoT plants and to prevent untrustworthy or undesired activities from compromised nodes.

IIoT enables industrial assets, including both hardware and software sides, to be connected into the production chain and operated over a network [8]. In such way, physical production processing can be visualized by using numerical description, where diverse types of manufacturing services can be associated, classified, and assessed [9, 10]. While IoT and IIoT have the same requirements for general communications, smart manufacturing focuses more on offering an automated and efficient environment, where a massive number of nodes can collaboratively assist in service provision [11]. Therefore, IIoT has a specific demand for service evaluation, due to the fact that it encourages the entire network to involve connected devices in participating in repetitive and complex manufacturing services, i.e., preventing the negative effects caused by misbehaving of nodes or malicious attacks on services is an essential task for IIoT security. In this regard, trust management plays a crucial role as it analyses nodes' behaviors over time.

Existing trust models are mainly classified into centralized and distributed [12]. Centralized models conduct TM by a single entity, while nodes are self-organizing for TM in the distributed architecture. However, both are not optimal when facing the industrial environment with respect to the control system structure, node specified capabilities, and large scale in IIoT. Furthermore, most of the existing models in the literature use a static service evaluation scheme without differentiating service types and considering the service composition process. Only a few studies discuss the trustworthiness within the system before the service provision, namely service registration, and discovery. This also leads to vulnerability to attacks on services, since certain types of attacks behave in a random and intelligent manner. So a continuously operated TM, covering all the operation phases of IIoT services, is needed.

In this context, we propose a phase-based trust management framework for service-oriented industrial IoT (SOPHT). Our contribution is five-fold. First, we define a hybrid TM architecture containing plant TM and inter-plant TM, which is suitable to the IIoT environment. Second, we propose a plant TM scheme established on four consecutive phases fitting various contexts

and interacting with entity management and service management. Third, we design service grade to observe the quality on each service type to help with the trust estimation on service registration and discovery. Fourth, we design a node classification mechanism distinguishing good/malicious nodes, weak/bad service provider/rater, and malicious attackers. Finally, we develop a three-phase mechanism to measure the cooperativeness between plants.

The rest of this paper is organized as follows. Section II describes the background and reviews the related contributions on TM models. Section III discusses the framework of the proposed model. Section IV details the IIoT plant TM and the inter-plant TM. The simulation results and performance analysis are presented in Section V. Section VI draws the conclusion and outlines our future work.

II. Background and motivation

In this section, we give the motivation of this work by introducing the background and reviewing related work in detail. This also allows us to study the constraints and the techniques to design a TM model that can meet the requirements of a service-oriented IIoT and overcome its related issues.

A. Control systems and Service Oriented Architecture in IIoT

The control system is an important component of industrial automation since it enables managing and operating IIoT plants by use of the industrial controller. Authors in [13] classified control systems in three types: A single controller oversees IIoT plants in the centralized control system; The federated (also called decentralized) control system deploys individual controllers to host IIoT plants, and these controllers are networked; The hierarchical control system can be regarded as a combination of the former two types since the supervisory layer can coordinate plant controllers. IIoT devices are usually designed for a specified functionality, so that a fully distributed TM model cannot properly match industrial requirements due to its self-organizing mode. Moreover, all three types of control systems in IIoT are either locally or globally centralized. For this reason, a central entity is needed for TM in IIoT, so to have a global view for monitoring the nodes and services.

In a Service Oriented Architecture(SOA)-based industrial system [14], industrial devices can participate collaboratively to the manufacturing services. As shown in Fig.1, an SOA has three fundamental elements: service broker, service consumer, and service provider (SP). The SP publishes its services in the repository of the service broker, then the service consumer discovers and finally invokes the services. To summarize, three crucial activities in SOA are service registration, service discovery, and service provision [15].

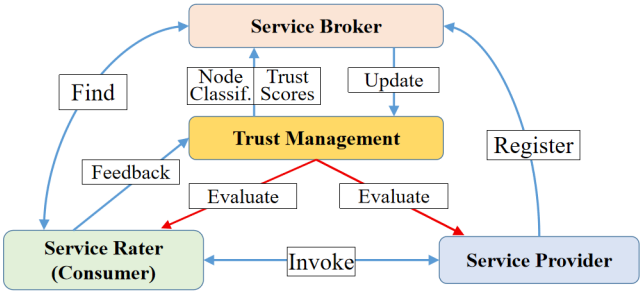


Fig. 1: SOA-based TM

Integrating the TM into the SOA, Fig. 1 shows a SOA-based TM model: Service consumer becomes service rater (SR) when sending its feedback to the TM entity after service provision, and then both service rater and service provider will be evaluated by the TM. Next, TM can assist service brokers with decision making through the results of the node classification and trust score values, e.g., checking available service types, removing malfunctioning nodes or malicious attackers. Finally, information related to services will be updated by the service broker. Indeed, the metrics are complex for service evaluation, e.g., a service provider, performing poorly the provision of service X, may be outstanding at service Y. Thus, securing a service-based IoT/IIoT requires the TM to interact with aforementioned service activities to assign to nodes and services the accurate trust values.

B. Attacks on services

In regard to the attacks on services, Table I classifies them by attack source and target: -Unfair Rating Attacks (URA) aim at creating disorder in the evaluation system by delivering dishonest ratings, and consist of three kinds:

- Ballot Stuffing Attack (BSA): The attacker highly recommends malicious nodes to increase their reputation.
- Bad Mouthing Attack (BMA): The attacker sends negative feedback to decrease the trust score of a good service provider.
- Self-promoting Attack (SPA): The attacker provides positive ratings for itself, intending to be selected for service provision.

TABLE I: Categories of attacks on services

Src.	Attack		Target	Ref.
SR	URA	BSA	Rating	[16]
		BMA		[17]
		SPA	Service, Rating	
	NCA			
SP	IBA	CBA		[18]
		OOA		
		SBA		[19]

-Newcomer Attack (NCA): The attacker re-enters the system with a new identity to refresh its trust score. The attack source can be a service rater or provider when NCA occurs. **-**Inconsistent Behavior Attacks (IBA) are from the malicious service provider and can also be of three distinct types:

- Conflicting Behavior Attack (CBA): The attacker performs differently with different nodes.
- On-off Attack (OOA): The attacker switches its behavior between good and bad over time to maintain its trust score above a certain threshold.
- Selective Behavior Attack (SBA): The attacker performs well and badly between services in an alternative manner.

Building countermeasures against attacks on services to prevent the adverse effects is an essential task in SOA-based TM, i.e., the TM model should show robustness and effectiveness in treating these attacks.

C. TM for service-oriented IIoT and related issues

Using the network quality of service (QoS) and some social features [20] to observe the trustworthiness of nodes have been largely investigated in the majority of existing TM models. Some studies have considered a mechanism that motivates excellent services and discouraging poor ones, e.g., service score in [21]. The service weight mechanism proposed in [22] enables differentiating service types, and the TM model in [19] measuring asymmetry between capabilities and service types before service provision is slightly beneficial for service discovery. However, none of them fits SOA-based IoT due to insufficient discussion for service publication and discovery. The authors in [23] designed a TM model for SOA-based IoT using distributed collaborative filtering scheme, and they proposed a trust-based service provider selection. However, the service composition concerning workflow remains neglected, and such distributed TM model in IIoT remains inapplicable since the TM architecture in IIoT should take a central entity into account. Authors in [24] aimed to improve the trustworthiness of a SCADA industrial network through a cyber-attack detection model based on a centralized architecture. However, the central entity must be over-capable in terms of computation and data storage regarding large scale in IIoT, and this also leads to the extension of network size being demanding. More importantly, centralized architecture is vulnerable to malicious intrusions since it possesses only one single point of failure. For overcoming these limitations in the centralized TM model, the hybrid architecture can be employed for TM in IIoT. Authors in [25] proposed a hierarchical TM model where community leaders manage the trust of community members, and an IIoT server governs all leaders. On the one hand, this model shows adaptability in the IIoT environment, and it also addressed various attacks on services such as BMA, BSA, and SPA. On the other hand, this model does not fit the SOA-based system due to the lack of discussion of service registration and composition, and the access control of nodes has not been addressed. Moreover, the attacks from the service provider side are not considered.

Table II gives a summarized comparison between the above-reviewed TM models.

TABLE II: Summary of related TM models

Ref.	Arch.	SO		IIoT	Attacks on services						
		Reg.	DSC		BSA	SPA	BMA	NCA	CBA	OOA	SBA
[21]	D	-	-	-	-	-	-	-	-	Y	-
[22]	D	x	-	-	-	-	-	-	-	Y	-
[19]	C	x	x	-	Y	-	Y	-	-	Y	Y
[23]	D	-	x	-	Y	Y	Y	-	-	-	-
[24]	C	-	-	Y	-	-	-	-	-	-	-
[25]	H	-	-	Y	Y	Y	Y	-	-	-	-
[26]	H	Y	x	-	Y	-	Y	Y	Y	Y	-
SOPHT	H	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

SO = Servic-oriented, C = Centralized, D = Distributed

H = Hybrid, Reg. = Registration, DSC = Discovery

Y = Supported, x = Partially Supported

In our previous work, we designed a four-phase TM model containing Access Control, Preselection, Service Evaluation, and Node Classification, based on a hybrid architecture [26]. This model is effective against several types of attacks on services, such as OOA, CBA, BMA, BSA, and NCA. However, concerning specific requirements in service-oriented IIoT, this work is subject to a few limitations. First, the access control should consider the industrial security requirements instead of general IoT ones. Second, more related metrics should be examined under an industrial context to prevent service registration and discovery from inaccuracy in IIoT. Third, the countermeasures against attacks on services have not been sufficiently discussed, namely SPA and SBA. Finally, the simulation scale can be enlarged in order to conform to the industrial scenario. To overcome these limitations, we design a novel trust framework for service-oriented IIoT.

III. Proposed framework

This section presents the hybrid TM architecture of SOPHT framework, which is suitable for IIoT environment.

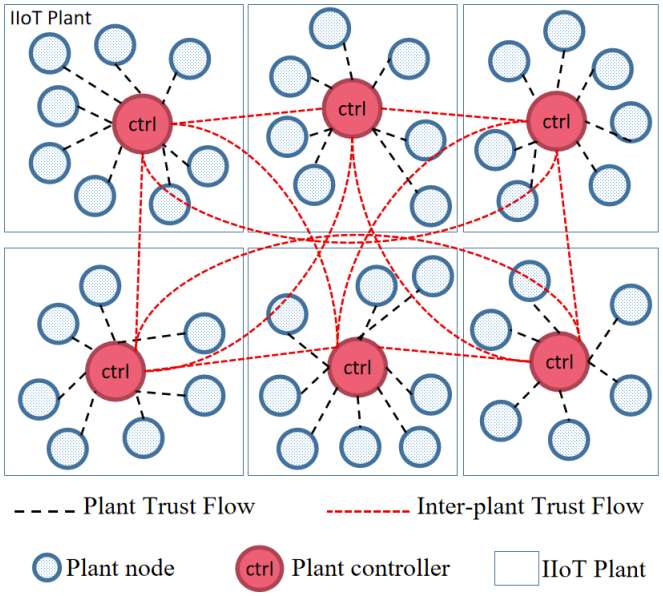


Fig. 2: Proposed SOPHT architecture

In light that fully centralized or fully distributed architectures are not sufficiently advantageous in terms of applicability and security within an industrial context, we design a hybrid architecture to support and improve the TM in IIoT. Fig. 2 demonstrates the proposed architecture of the SOPHT framework with two levels: plant and inter-plant TM. Industrial devices are assembled at the plant level, where nodes in the same plant can participate in cooperative missions to interact in a multi-service environment. Each plant represents an industrial community, and each plant controller is in charge of plant TM as a local responsible entity. Moreover, controllers are networked so that the communication and TM at the inter-plant level are conducted in a distributed manner. Notably, the access control (AC) policy of each plant controller is not identical since plants may have diverse missions, e.g., plants p and m may concentrate on raw material treatment and production chain, respectively. Hence, newcomer nodes will be examined much more strictly in those plants with specified demands.

IV. TM Model

To illustrate the trust computation of the SOPHT framework, we introduce the plant TM model, first, by detailing each phase. Then, we explain the distinction that the system is able to perform on the nodes that returns to the same plant after some time of inactivity and those that move to a new plant, to complement the AC phase concerning several plants. Lastly, we focus on the TM at the inter-plant level. All notations and acronyms used in this paper are gathered in Table III.

A. IIoT Plant TM

1) Overview of the four phases: We first detail four phases in plant TM by demonstrating the interactions between TM, service management (SM), and entity management (EM).

Fig. 3 illustrates the SOPHT phases consisting of four phases: access control (AC), service provider selection, service evaluation, and node classification. Initially, node identification allows function (fct), social (soc), and context (ctx) attributes (A) to be treated in the access control phase in order to generate a default score (DS) as the initial trust score of the newcomer node. Particularly, the AC phase will react with service registration activity in SM to determine the functional services (S^{fct})

TABLE III: Symbol description

SYM	Meaning	SYM	Meaning
SP	Service provider	PR	Parental relationship
SR	Service rater	CWR	Co-work relationship
A	Attribute	SOR	Social relationship
DS	Default score	CN	Connected nodes
SS	Selection score	Des	Description of the node
TS	Trust score	Pre	Prediction of node's return
QSP	Quality of SP	RS_i	Services rated by i
QSR	Quality of SR	PS_i	Services provided by i
SG	Service grade	f_{ij}	j's feedback to evaluate i
OSG	Overall SG	$\bar{f}_i$	Average of i's notes
S	Service	R_{-i}	Nodes that rated i
C	Capability	R_{i-}	Nodes that rated by i
fct	Function	R_{-i}^{sn}	Nodes that rated i's service sn
soc	Social	s_req	Requested service
ctx	Context	S_{req}	Requested services in workflow
E	Energy	plt	Current plant
P	Protection	S_{plt}	Available services in the plt
US	Usability	$\overline{S_{\mathrm{plt}}}$	Unavailable services in the plt
UR	Utilization rate	$S_{\widetilde{\mathrm{plt}}}$	Services of understaffed case
IS	Initial score	S^{fct}	Functional service
G	Centrality	$S^{\overline{\mathrm{fct}}}$	Nonfunctional service
N	Neighbor	C^{fct}	Functional capability
CF	Conformity	l	Punishment degree
ω, μ	Weights	CO	Cooperativeness
η, ε		CS	Cooperation score
φ, κ		l	Punishment degree

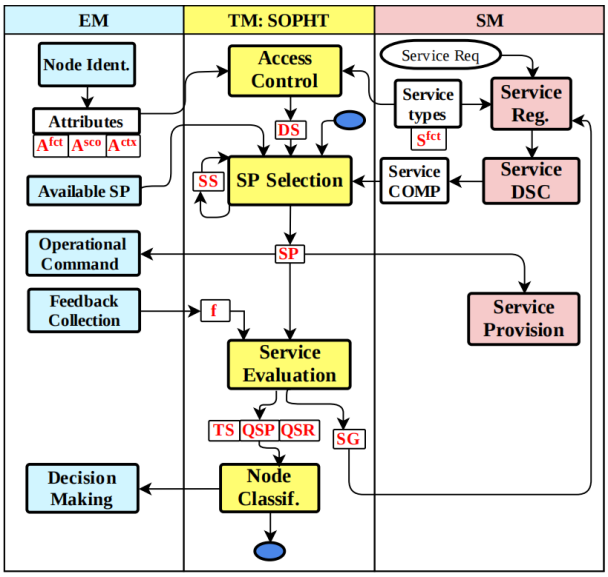


Fig. 3: Relationships between EM, TM, and SM

of the node by validating the node's capabilities [27]. Once a service request has been received and confirmed by the plant controller, service discovery activates the service composition (COMP) step, where the request mission can be depicted as a workflow composed by services registered. Next, the SP selection phase ranks available SP by calculating the selection score (SS) on the basis of the service composition and nodes' service grade (SG), and the controller transmits the operational command to the authorized SP with great selection score (SS) to start the service provision. After that, the feedback from service consumers will be collected to support the service evaluation phase that calculates trust score (TS), quality of service rater (QSR), provider (QSP), and SG. Eventually, based on the trust values issued from the last two phases (service evaluation and node classification), service registration updates service types according to current SG, and those badly-performed nodes must be isolated based on the result of node classification phase. The blue circles are to indicate the cycles of SOPHT phases.

The diagram in Fig. 3 gives an overview of how SOPHT works with EM and SM. We suggest a TM model that is applicable since the three blocks in SM are key activities in SOA, as previously discussed already, and the control system can carry EM out, while it conducts device identification, issues operational commands to plant nodes, and gathers their feedback after the service provision ends. From this diagram, it can also be seen that SOPHT model enables to monitor and evaluate behaviors of IIoT plant nodes dynamically, and can connect and interact with EM and SM to support the IIoT environment.

2) Access Control: Recording the node by its asserted attributes is more advantageous in terms of security [28], and ABAC (attribute-based access control) is considered a logical methodology for AC in IIoT [29]. For defining permissions in AC phase, we are concerned with the three types of attributes: function (fct), social (soc), and context (ctx). Fix a node i until the end of the section. The set of attributes of node i is denoted as

$$A_i = \langle A_i^{\mathrm{fct}} |\ A_i^{\mathrm{soc}} |\ A_i^{\mathrm{ctx}} \rangle. \tag{1}$$

Function attribute (A^{fct}) indicates the capabilities (C) of the node. By validating nodes' capabilities, the functional services (S^{fct}) will be classified and extracted, as demonstrated in Fig. 3, and those capabilities that are deployed to conduct S^{fct} are identified as functional ones C^{fct}. The assignment of the initial score to the newcomer depends on two aspects: usability (US) and utilization rate (UR). In the industrial context, the newcomer node falls into two broad categories, related to the service: either it can provide new functionalities that the current plant does not have (thereafter referred as 'newness'), or it meets the need of the current plant, due to the heavy workload (thereafter referred as 'understaffed'). Thus, the US measures if the current plant needs the newcomer node by analysing its S^{fct}, and the UR calculates the ratio between the functional capabilities and all the capabilities (functional and nonfunctional) of the node in order to determine if, in terms of missing capabilities, the node should be deployed.

Social attribute A^{soc}: Although social features are widely studied in Social Internet of Things (SIoT), the IIoT nodes also have such features, since they interact with each other, share data, and collaborate for service provision. In our model, we consider three main object relationships [20]: parental (PR), co-work (CWR), and social (SOR) relationships. Nodes belonging to the same manufacturer have higher PR, as their functional characteristics are somehow approximated. We measure the similarity of functional services of nodes because the CWR value increases when nodes have more opportunities to cooperate in service. The contact between nodes comes randomly, continuously, or periodically, and thus SOR is used to indicate the interactivity between nodes.

Context attribute (A^{ctx}) describes the relevant contextual information that can be used as security characteristics [30]. Here, we consider two environmental conditions: energy (E) and protection (P). E refers to the power source of the node such that it can somehow show device life-cycle information since nodes often suffer from constrained resources, and P demonstrates the importance of the establishment of physical protection.

Based on the three types of attributes of the newcomer node, the AC phase can assign it an initial trust value by (13) before the newcomer node participates in the SP selection.

a) DS of function attribute: DS_i^{fct} defined by

$$DS_i^{\mathrm{fct}} = US_i \cdot UR_i, \tag{2}$$

where

$$US_i = \begin{cases} 1, & \text{if } \ S_i^{\mathrm{fct}} \cap \overline{S_{\mathrm{plt}}} \neq \emptyset \text{ or } S_i^{\mathrm{fct}} \cap S_{\widetilde{\mathrm{plt}}} \neq \emptyset \\ 0, & \text{otherwise} \end{cases} \tag{3}$$

and

$$UR_i = \frac{|C_i^{\mathrm{fct}}|}{|C_i|}. \tag{4}$$

We now define S_{plt} that represents the available functional services in the plant plt:

$$S_{\mathrm{plt}} = \bigcup_{k \in CN} S_k^{\mathrm{fct}}, \tag{5}$$

where CN denotes the connected nodes in the current plant. In (3), $\overline{S_{\mathrm{plt}}}$ is the set of functional services unavailable in the current plant, and $S_{\widetilde{\mathrm{plt}}}$ represents the services of understaffed case. Thus, $S_{\widetilde{\mathrm{plt}}} \subseteq S_{\mathrm{plt}}$. In (4), $|C|$ denotes the cardinality of the set C.

b) DS of social attribute: DS_i^{soc} defined by

$$DS_i^{\mathrm{soc}} = \mu^{PR} PR_i + \mu^{CWR} CWR_i + \mu^{SOR} SOR_i, \tag{6}$$

where $\mu^{PR} + \mu^{CWR} + \mu^{SOR} = 1$,

$$PR_i = \frac{1}{|CN|} \sum_{k \in CN} v_{ik}^{PR}, \tag{7}$$

$$CWR_i = \frac{1}{|CN|} \sum_{k \in CN} \frac{|S_i^{fct} \cap S_k^{fct}|}{|S_i^{fct} \cup S_k^{fct}|}, \tag{8}$$

and

$$SOR_i = \frac{1}{|CN|} \sum_{k \in CN} v_{ik}^{SOR}. \tag{9}$$

In (7), (8) and (9), v^{PR} and v^{SOR} are binary values describing if they belong to same production batch and if the their interaction is adaptable in terms of their software specification, respectively.

c) DS of context attribute: DS_i^{ctx} defined by

$$DS_i^{\mathrm{ctx}} = \frac{1}{2} \cdot (E_i + P_i), \tag{10}$$

where

$$E_i = \begin{cases} 1, & \text{for mains-powered} \\ \dfrac{D_i \mathrm{res}}{D_i}, & \text{for other power source} \end{cases} \tag{11}$$

and

$$P_i = \begin{cases} 1, & \text{if physically protected} \\ 0, & \text{otherwise} \end{cases} \tag{12}$$

In (10), we weight the sum of E and P by $1/2$ because they are regarded equally critical as contextual information. For the calculation of E in (11), all power source types take the ratio of residual durability ($D\mathrm{res}$) and durability (D), except mains-powered ones take 1. In (12), P takes a binary value indicating if the node is protected physically, e.g., in a secure zone.

d) DS computation: With three sub-DS values calculated by (2-10), the DS of node i can be calculated as follows:

$$DS_i = \omega^{\mathrm{fct}} \cdot DS_i^{\mathrm{fct}} + \omega^{\mathrm{soc}} \cdot DS_i^{\mathrm{soc}} + \omega^{\mathrm{ctx}} \cdot DS_i^{\mathrm{ctx}}, \tag{13}$$

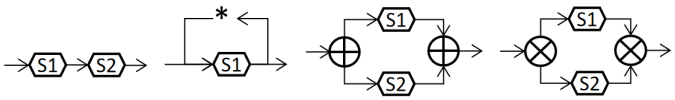
where $\omega^{\mathrm{fct}} + \omega^{\mathrm{soc}} + \omega^{\mathrm{ctx}} = 1$. Newcomer node is permitted to entry if its $DS{>}0.5$, and then the controller generates a description (Des) by adding trust score fields, functional and nonfunctional services (S^{fct} and $S^{\overline{\mathrm{fct}}}$), and service grade ($SG$) after the attributes A as follows:

$$Des_i = \langle A_i |\ TS_i |\ QSP_i |\ QSR_i |\ S_i^{\mathrm{fct}} |\ S_i^{\overline{\mathrm{fct}}} |\ SG_i \rangle. \tag{14}$$

The newcomer node is prohibited from requesting services unless the controller designates it to consume services. Furthermore, it will not be evaluated by the controller in the service evaluation phase since it has neither rated nor provided services. Thus, TS, QSR and SG are all null. DS is filled into QSP in order to have an initial level to compete for the service provider selection. $S^{\overline{\mathrm{fct}}}$ is initially empty but will be employed when any S^{fct} of the node are adjudicated ineligible. Lastly, this

description will be stored into the list of current nodes (CN).

3) Service provider (SP) selection: Upon receiving a service/mission request directly from the controller or from the node whose QSR>0.5, the service discovery activity will commence with the service composition process while some missions require a workflow that searches and interconnects services [31].



(a) Sequence (b) Loop (c) Flow (d) Switch

Fig. 4: Constructs for workflow

Fig.4 illustrates commonly-used service composition constructs, including sequence $\rightarrow$ (s1, then s2), loop * (s1 several times), flow $\oplus$ (s1 and s2), and switch $\otimes$ (s1 or s2).

If the workflow allows numerous nodes to take part in the service composition, the essential method is still looking for the best-ranked candidate nodes with outstanding SG, this remains the same scheme for single service requested. For a workflow dedicated to one node, to have better continuity for example, SG of single service type cannot accurately signify the trustworthiness of services requested in the workflow (denote as S_{req}). Thus, an overall opinion for the workflow should be estimated as well. The calculation of overall SG (OSG) is given in (15), and the r for loop * represents the number of repetition.

$$OSG_i = \begin{cases} \prod_{\mathrm{sn}\in \mathrm{S_{req}}} SG_i^{\mathrm{sn}}, & \text{for } \rightarrow \\ (SG_i^{\mathrm{sn}})^r, & \text{for } * \\ 1 - \prod_{\mathrm{sn}\in \mathrm{S_{req}}} (1 - SG_i^{\mathrm{sn}}), & \text{for } \oplus \\ max_{\mathrm{sn}\in \mathrm{S_{req}}} (SG_i^{\mathrm{sn}}), & \text{for } \otimes \end{cases} \tag{15}$$

Next, the controller can generate a ranking of selection scores (SS_i), calculated as follows:

$$SS_i = \begin{cases} QSP_i \cdot OSG_i, & \text{for a workflow} \\ QSP_i \cdot SG_i^{s\_\mathrm{req}}, & \text{for a single service} \\ QSP_i, & \text{if newcomer} \end{cases} \tag{16}$$

The examination of the candidate SP in (16) concerns two sides: QSP gives the opinion from a more general view, e.g., the stability (refer to section Section IV-A4c); and SG/OSG measures the specialty of the SP, which determines the feasibility of that SP can accomplish the dedicated service/mission. The node with poor QSP or SG/OSG will obtain a low value for SS. Due to the fact that the controller selects only the best-ranked candidates with significant SS, those of low rank barely have the opportunity to assist in service provision.

As discussed in Section IV-A2, there are two cases when the newcomer access control occurs: newness or understaffed. The SP selection is lightweight in the first case, since only the newcomer will provide the requested service. For the second case, the SP selection concerning newcomers must be started after all other candidates have been assigned some missions.

4) Service evaluation: In the service evaluation phase, the trustworthiness of nodes will be measured by four metrics, namely trust score (TS), quality of service rater (QSR), quality of service provider (QSP), and service grade (SG). TS gives an overall opinion on the basis of QSP and QSR, and SG corresponds directly to the quality of each service type. The feedback originated from service consumer (thereafter referred as 'service rater') j to rate the service quality of the service provider i is in the range of $[0, 1[$ (0 means no service conducted from service provider) and denoted as f_{ji}. To precise the workflow cases, the feedback should be gathered after every service provision of each service, i.e., the number of feedback from one SR and the number of services consumed by it must be equal, whatever the service composition is.

a) Trust score (TS): We set

$$TS_i = \frac{|RS_i|}{|RS_i + PS_i|} \cdot QSR_i + \frac{|PS_i|}{|RS_i + PS_i|} \cdot QSP_i, \tag{17}$$

where RS_i and PS_i denote the services rated and provided by the node i, respectively, and QSR_i and QSP_i are given by (18) and (20). It can be seen that a node has two roles: service rater (SR) and service provider (SP). This means the evaluation of a node depends on the behavior of both roles, e.g., a reputable SP may be dishonest when rating others' services; likewise, an excellent SR may be terrible at service provision. That is also the reason that we deploy the quantity parameter to weight (17). In such a way, the quality and quantity impact of QSR and QSP can be carried out accurately to assess the trustworthiness of the node as both SR and SP.

b) Quality of service rater (QSR):

$$QSR_i = \varphi \cdot CQSR_i + (1 - \varphi) \cdot LQSR_i \ , \tag{18}$$

where φ belongs to $[0.5, 1[$. $CQSR$ and $LQSR$ are current and last values of QSR. We put QSR=$CQSR$ for newcomers since they do not possess any rating records. The $CQSR$ in (18) is computed as follows:

$$CQSR_i = 1 - \frac{1}{|R_{i-}|} \sum_{j \in R_{i-}} |f_{ij} - \bar{f}_j|^{1/l} \ , \tag{19}$$

where R_{i-} represents the set of nodes that rated by i in the service evaluation phase, $\bar{f}_j$ is the average value of feedback evaluating node j, and the little l is the punishment degree such that the dishonesty will be amplified.

Indeed, the calculation of QSR is based on the comparison between the opinions of the rater node and the average value of other raters, which enables to distinguish the dishonest service raters by identifying the gap in this comparison. In IIoT, the feedback f_{ij} from i to evaluate j can emerge by a predefined measurement scheme that is objective, thus it will not have a large variance, as such in SIoT, due to the user preference or environmental perturbation. Therefore, an unfair rating from a dishonest rater that either ruins a well-behaved node's reputation (BMA) or boosts a misbehaved node's reputation (BSA), can be detected.

c) Quality of service provider (QSP):

$$QSP_i = \varepsilon \cdot CQSP_i + (1 - \varepsilon) \cdot LQSP_i \ , \tag{20}$$

where ε is set in the range $[0.5, 1[$, to weight the current value ($CQSP$) and the last value ($LQSP$). We put $LQSP$=DS for newcomers, and it is reasonable since we set DS to QSP for newcomer nodes in the AC phase. The $CQSP$ in (20) is calculated as follows:

$$CQSP_i = \frac{1}{|R_{-i}|} \sum_{j \in R_{-i}} \theta_{ji} \cdot \lambda_{ji} \cdot QSR_j \cdot f_{ji} \ , \tag{21}$$

where R_{-i} represents the set of nodes that rated services from i, θ and λ are stability parameters against OOA and CBA, respectively given by (22) and (23).

$$\theta_{ji} = \mathrm{sinc}(1 - f_{ji}) \cdot \mathrm{sinc}(\Delta f_{ji})^{\Delta t}, \tag{22}$$

$$\lambda_{ji} = 1 - |f_{ji} - \bar{f}_i|^{1/l}. \tag{23}$$

In (22), Δt and Δf_{ji} are time gap and difference of last feedback (lf_{ji}) and present feedback (cf_{ji}), i.e., $\Delta t = t_{cf_{ji}} - t_{lf_{ji}}$ and $\Delta f_{ji} = |cf_{ji} - lf_{ji}|$, we set both to 0 for newcomers. The (normalized) sinc function is defined as

$$\mathrm{sinc}(x) = \begin{cases} 1, & \text{for } x = 0 \\ \frac{\sin(\pi x)}{\pi x}, & \text{for } x \neq 0 \end{cases} \tag{24}$$

We choose the latter mapping in (22) because it is continuous at point 0, and maps $[0, 1]$ onto $[0, 1]$ with inflexions that can be used to penalize the large Δf_{ji} and poor f_{ji}. The unstable behaviors over time is penalized by use of θ_{ji}, since it is increasing in Δf_{ji}, with an exponent Δt that renders unacceptable any drastic changes in service quality. In (23), $\bar{f}_i$ is the average value of i's notes rated by other rater nodes and l is the punishment degree as same in (19). In other words, conflicting behavior will be captured due to λ that compares the service quality to each individual with the average level. By the very definitions of the θ and λ coefficients, the unique possibility for the node to earn reputation, is to keep steadily providing satisfying services.

d) Service grade (SG): To evaluate the service quality of type n (s^{n}), the service grade SG_i^{sn} is computed as follows:

$$SG_i^{\mathrm{sn}} = \kappa \cdot CSG_i^{\mathrm{sn}} + (1 - \kappa) \cdot LSG_i^{\mathrm{sn}}, \tag{25}$$

where

$$CSG_i^{\mathrm{sn}} = \frac{1}{|R_{-i}^{\mathrm{sn}}|} \sum_{j \in R_{-i}^{\mathrm{sn}}} QSR_j \cdot f_{ji}^{\mathrm{sn}}, \tag{26}$$

where R_{-i}^{sn} is the set of nodes that rated the s^{n} provided by i and f_{ji}^{sn} denotes the feedback from j for sn provided by i, i.e., we identify the service type that the feedback indicated. Notably, $SG^{\mathrm{sn}} = CSG^{\mathrm{sn}}$ for newcomer nodes. SG is used to observe specifically the service quality of each type that is marked as 'functional' since the AC phase, i.e., if any single type of S^{fct} gets a low value of SG, it will be regarded 'nonfunctional' service and cannot provide such service type anymore. Accordingly, this service type will be relocated from S^{fct} to $S^{\overline{\mathrm{fct}}}$.

The set of all service grades will be updated in each service evaluation phase and it is defined as follows:

$$SG_i = \{SG_i^{\mathrm{sn}} | \mathrm{sn} \in (S_i^{\mathrm{fct}} \cup S_i^{\overline{\mathrm{fct}}})\} \tag{27}$$

As a result of the calculation in (27), the SG^{sn} will decrease if a node persists in providing unsatisfying service on particular type n. After that $SG^{\mathrm{sn}}<0.5$, the plant controller must label this service type as malfunctioning and immediately remove it from S^{fct}. After the removal, the service is put into the $S^{\overline{\mathrm{fct}}}$, in order to prohibit the node from being selected as SP for the service type n, and alert other plants in case of need, e.g., when a node moves to another plant. Hence, the misbehavior aiming at service types from malicious SP, namely SBA, will be authorized to provide fewer and fewer service types due to the SG mechanism. Finally, two situations come to such node, either it performs well for the other service types to stay in the current plant, or it progressively loses its competitiveness for the SP selection, and eventually it will be eliminated from the plant.

5) Node classification: By classifying the values of TS, QSP and QSR under good (>0.5) and bad (≤ 0.5), the node classification scheme illustrated in Fig. 7 enables the controller to categorize nodes into 6 groups:

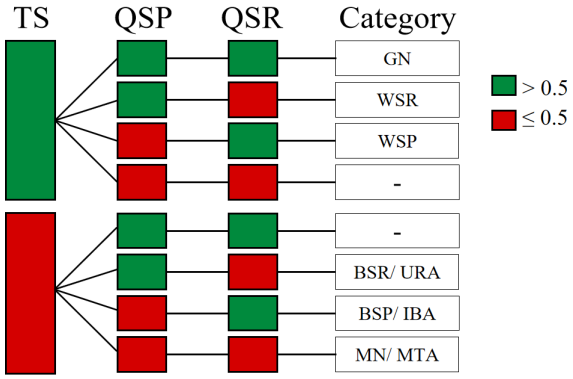


Fig. 5: Node classification scheme

- Good node (GN): This kind of node will surely stay in the current plant since its TS, QSP, and QSR are all at a good level.
- Weak service rater (WSR): WSR will be banned from requesting services as the QSR is ineligible for rating of the service.
- Weak service provider (WSP): Different from the treatment of WSR, a WSP node is not deprived of anything. However, it has been categorized into WSP because of its low QSP, thus, it has little chance to be picked since its QSP induces incompetence.
- Bad service rater (BSR)/unfair rating attacker (URA): It is difficult to determine precisely if this node is just incapable or malicious, but, in any of the two cases, the controller must eliminate the node in order to minimize the adverse effects of erroneous ratings from the controller's view.
- Bad service provider (BSP)/inconsistent behavior attacker (IBA): Analogously, SP belonging to this group may be simply unreliable in terms of service quality or may be an attacker who misbehaves. In any of the two cases, the controller must eliminate the node.
- Malicious node (MN)/mixed type attacker (MTA): It is the worst case among the node classification as all three metrics consisting TS, QSP, and QSR are bad. The controller must remove a node belonging to this group immediately.

In fact, the reason why WSP and WSR nodes are not isolated from the network is because their TS values remain good, i.e., they still have some valuable aspects that can benefit the current plant from a global perspective.

B. Returning to the same plant/moving to a new plant case

Fig.7(a) demonstrates how a newcomer is managed and registered. However, it is worth noting that, in IIoT, there are other possibilities besides the newcomer case. For instance, a device whose power source is rechargeable will be disconnected for recharging and then reconnected to the network. In order to keep the reputation of such node consistent throughout the recharging operation and prevent an undesirable node to whitewash its reputation (namely NCA), this type of node should be treated as a returner rather than as a newcomer.

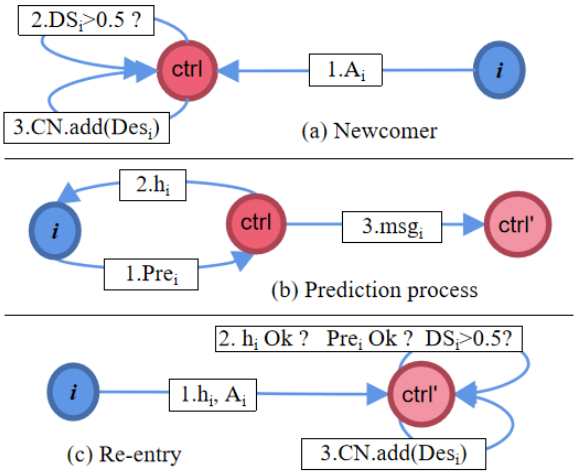


Fig. 6: Checking mechanism and prediction process

For this purpose, the node must inform the plant controller of the prediction for its return in the following form: $\mathrm{Pre_i}$=$\langle \mathrm{ctrl'} |\ \mathrm{loc'} |\ \mathrm{t'} \rangle$. The prediction contains target controller ($\mathrm{c'}$), location ($\mathrm{loc'}$), and time ($\mathrm{t'}$). After the prediction is accepted, the current controller will generate a message combining the prediction and the description of the node as follows: $\mathrm{msg_i}$=$\langle \mathrm{Pre_i} |\ \mathrm{Des_i} \rangle$, and this message will be transmitted to the target controller ($\mathrm{ctrl'}$) as announced in $\mathrm{Pre_i}$. Next, the current controller assigns a value to the node, that is converted by one-way hash function $\mathrm{h_i}$=Hash($\mathrm{msg_i}$). This prediction process is illustrated in Fig.7(b).

Fig. 7(c) describes the re-entry case, where the node should send the target controller ($\mathrm{ctrl'}$) the hash value ($\mathrm{h_i}$) received in the prediction process, then the target controller will collect attributes of this node and verifies the satisfaction of the three following conditions. First, the target controller investigates the hash value with the aid of the message from the original controller of the node, i.e., if $\mathrm{h_i}$ == Hash($\mathrm{msg_i}$). Second, the target controller checks if the information in prediction containing target controller ($\mathrm{c'}$), location ($\mathrm{loc'}$), and time ($\mathrm{t'}$), matches the entry of the node. Finally, the target controller analyses the attributes of the node and calculates the DS to decide if the node is permitted to enter the plant. As a policy for the returner, nodes from the same plant can continue to be assessed by the previous trust values; and nodes from other plants can only hold their previous QSR, if their QSR>0.5. In such manner, there is a sort of continuity in TM to benefit the returners. Furthermore, the target controller can utilize SG, S^{fct}, and $S^{\overline{\mathrm{fct}}}$ in Des to help the service registration activity to discern if a node fakes its capabilities. Therefore, using the triple checking rule illustrated in Fig. 7(c), the AC phase enables to distinguish the node that returned to the same plant, and the node that has moved to a new plant.

An NCA attacker attempts to re-enter the original plant or a new plant to obtain a refreshed trust score, but doing so very likely it makes its DS lower, as the AC phase is inherently dynamic, and the node is not aware of the service types. Furthermore, in the SP, the newcomers are always placed after the current active nodes in the plant, i.e., the newcomers have to earn the reputation after their entry. Hence, the NCA attacker's purpose of leaving the plant and then returning to refresh its trust scores is unachievable.

C. Inter-plant TM

1) Overview of phases: Unlike the plant TM, there is no service provision or rating at the inter-plant level but service migration (node moving to a new plant case). Therefore, the main objective of the inter-plant TM is to identify 'unfriendly' plants that may endanger the current plant security by sending malicious nodes. For this purpose, we design a simple three-phase mechanism for inter-plant TM. The evaluated plant shares its service types (S) and neighborhood situation (N) with the evaluator plant in the initial evaluation phase to issue an initial score (IS). In cooperation evaluation phase, the evaluator observes the cooperativeness of the evaluated one and calculates the cooperation score (CS) by analysing the behaviors of the nodes moving to a new plant from the evaluated plant. Finally, the evaluated plant will be classified in the plant classification phase based on the CS obtained.

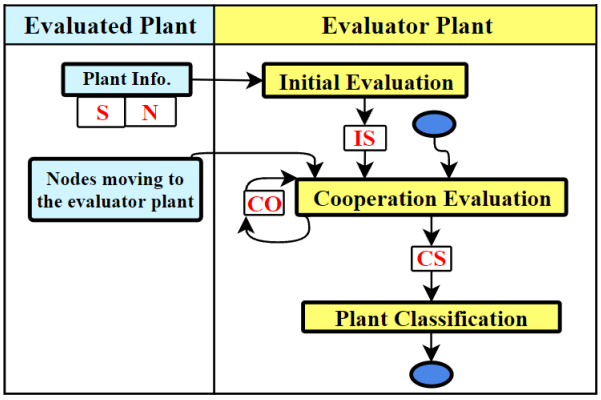


Fig. 7: Interaction between the evaluated and evaluator plants and three phases of inter-plant TM

2) Initial evaluation: For the initial evaluation, we set centrality (G) and conformity (CF) as trust metrics with equal importance:

$$IS_{mp} = \frac{1}{2} \cdot (G_{mp} + CF_{mp}), \tag{28}$$

Thus, the initial score (IS) describes the closeness of two plants in terms of service and location, and hence the evaluator plant can have a initial threshold of cooperation.

Centrality

$$G_{mp} = \frac{N_{mp}}{|N_m \cup N_p|}, \tag{29}$$

where N_p denotes the set of neighbors of p, and N_{mp} is a binary value describing if plants m and p are neighbors. The centrality G measures the relationship between plants from a co-location perspective, since industrial plants with high relevance or similarity are generally arranged close to each other. Thus, the term 'neighbor' means geographically close: A plant m within a certain distance can be considered as a neighbor of the plant p.

Conformity

$$CF_{mp} = \frac{|S_m \cap S_p|}{|S_m|}, \tag{30}$$

where S_m and S_p denote respectively all functional services needed in plants m and p. To differentiate with the S_{plt} utilized in Section IV-A2, S_{plt} denotes the available function services in the current services. The conformity CF examines the similarity of two plants in terms of community interest, and in such a way, they become complementary if this value is considerable. For instance, in case that plants p and m have high PCF, a sudden failure of a service type comes to plant p, and it can immediately ask plant m to help by sending nodes providing that service type.

3) Cooperation evaluation: After the initial evaluation phase, plants can interact with each other. This would make the nodes that moved to a new plant emerge, in order to deal with the 'newness' or 'understaffed' issues. When a plant requires another one to send nodes that provide functional services, these nodes may misbehave in the AC phase or service provision. By implementing the plant TM mechanism discussed before, the malicious nodes from other plants can be detected and removed, but the conclusion remains at the level of nodes, i.e., no evidence to confirm the role of the node-sender plant, especially if it has been compromised. For this reason, the cooperation evaluation should take into consideration the observation of nodes coming from other plants to determine the nature of the plant.

As stated already, the nodes that move to a new plant may behave badly in the AC phase or service provision, therefore, we measure the number of good nodes out of all those that moved to the new plant:

$$CO_{mp} = \frac{GN_{pm} + 1}{MNP_{pm} + 2}, \tag{31}$$

where GN_{pm} represents the good nodes (defined by the node classification scheme) from p to m, MNP (moved to new plant) are all the nodes that moved to the new plant. Cooperativeness describes the willingness of the evaluated plant sending nodes with functional services.

The cooperation score (CS) of p evaluated by m can be computed in an iterative way, as follows:

$$CS_{mp} = \begin{cases} IS_{mp}, & \text{before any interactions} \\ \eta^{CO} \cdot CO_{mp} + \eta^{IS} \cdot IS_{mp}^{\alpha}, & \text{otherwise,} \end{cases} \tag{32}$$

where $\alpha = 1/LCO_{mp}$, for LCO_{mp} the last CO_{mp} value, and $\eta^{IS} + \eta^{CO} = 1$. IS_{mp} given in the initial evaluation phase is somehow regarded as a threshold since two close plants should cooperate more, but a gap may emerge between the threshold and the reality that a plant with great IS can still send malicious nodes. Thus, the α is designed as a punishment parameter by amplifying the gap between the IS and CO.

4) Plant classification: With the CS value, Fig 8 classifies the evaluated plant into two groups: convenient plant (CP) and distant plant (DP).

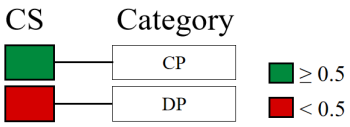


Fig. 8: Plant classification scheme

Consequently, the evaluator plant will reduce the communication frequency with the evaluated plants whose CS value is low since their interactions are considered valueless after the calculation. On the other hand, the evaluated plants with great CS value have higher priority for the evaluator plant when looking for support, since the evaluated plant is more profitable than others.

V. Simulation

This section analyses the simulation results and verifies the effectiveness of the SOPHT framework by using MATLAB platform.

A. Simulation parameters setup

TABLE IV: Simulation parameters values

Parameter	Value		Parameter	Value
ω^{soc}, ω^{ctx}	0.2		ω^{fct}	0.6
μ^{PR}, μ^{SOR}			μ^{CWR}	
η^{IS}			η^{CO}	0.8
ε, φ,κ	0.5		l	2

As illustrated in Table IV, we set ω^{fct} and μ^{CWR} 0.6 because they are regarded as more relevant than other parameters with respect to the need of services in the current plant. Similarly, for η^{CO}, we set 0.8 since it is considered as significant to demonstrate the cooperativeness between plants. Respecting the constraints of $\mu^{PR}+\mu^{CWR}+\mu^{SOR} = 1$, $\omega^{\text{fct}}+\omega^{\text{soc}}+\omega^{\text{ctx}} = 1$, and $\eta^{IS} + \eta^{CO} = 1$, we consider other parameters identically critical and thus assign them all 0.2. ε, φ, and κ are given 0.5 for the reason that the last and the current evaluations are equally important. Finally, the punishment degree l is set to 2. Other simulation configurations concerning plant and inter-plant TM are given in Sections V-B and V-C, respectively.

B. Plant TM

In the simulations of the plant TM, we focused on observing the trustworthiness within one single IIoT plant. Table V illustrates the simulation configuration of the plant TM, and the service types and capabilities are numbered to simplify the representations. In the current plant, there are 29 nodes belonging to 8 types as CN, and their trust values are all set to a random value in the range of [0.9 0.95] [1]. For the service composition, we randomly select 1 out of 5 possibilities (single, $\rightarrow$, *, $\oplus$, and $\otimes$), where $\rightarrow$, $\oplus$, and $\otimes$ contain 2 service types each (excluding $s4$ since understaffed). In addition, r=2 for * case. Finally, only 1/2 of candidate SP can participate in the final service provision ((candidate SP+1)/2 if odd), and service consumers are all nodes that are not candidates to involve more SR.

[1]Please, refer to Tables VI for the service type validation process through the capabilities of nodes.

TABLE V: Configuration of plant TM simulation

Conf.	Description
Controller	Single one
Service types	s1∼s3-general, s4-understaffed, s5-newness
Capabilities	Predefined c1∼c14, refer to Table VII
Node type	Predefined t1∼t12, refer to Table VII
Num of nodes	(t1∼t7)×4+8×1=29 CN; (t9∼t12)×1

INIT = Initialization, Num = Number

1) Access control: Two aspects of the AC phase performance will be analysed: the calculation of DS values and the demonstration of returning/moving to a new plant cases.

a) DS calculation: As defined in Tables V and VII, only the CN node of t8 is able to provide $s4$, and $s5$ is a new service that the current plant needs. On the one hand, we set t9 and t10 to demonstrate the AC phase for 'understaffed' and 'newness' cases. On the other hand, t11 has no service identified as functional, and t12 possesses too many capabilities, in fact its UR (utilisation rate) is too low to let it enter.

TABLE VI: Service Registration through capabilities of nodes

S	1	2		3			4		5		
C	1	2	3	4	5	6	1	7	2	5	8

TABLE VII: CN nodes and newcomers with their attributes utilized

Type	CN	C	S	ssp	PB	E	PT
t1	Y	-	1	a,b	i	-	-
t2	Y	-	1,2	b	i	-	-
t3	Y	-	1,2,3	a,b,c	i	-	-
t4	Y	-	1,3	a	i	-	-
t5	Y	-	2	a,c	j	-	-
t6	Y	-	2,3	b	j	-	-
t7	Y	-	1,3	a	j	-	-
t8	Y	-	1,4	a,b,c	i	-	-
t9	N	1,2,3,7	1,2,4	b	i	R	N
t10-1	N	2,4,5,8	5	a	j	MP	N
t10-2	N	2,4,5,8	5	a	j	R	N
t11	N	4,8	/	a,b,c	j	MP	Y
t12	N	2,5,8,9,10, 11,12,13,14	5	a,b,c	j	MP	Y

MP = Mains-powered, ssp = Software Specification
PB = Production Batch, R = Rechargeable

Table VIII illustrates the DS calculation of t9∼t12 nodes. Note that the CN list remains unchanged for each entry. t9 obtains 0 for DS^{ctx}, but it has a significant DS^{fct} value since it provides $s4$ and all of its capabilities can be deployed. In addition, its DS^{soc} is relatively higher than other types of nodes because it has more chances to cooperate and interact with other CN due to its 3 service types. Similarly, t10-1 and t10-2 have great values of DS^{fct}, due to the new service $s5$. Since their capability $c4$ is unusable, their UR<1. The reason why t10-1 entered but t10-2 did not, is that t10-1 is mains-powered. Although t11 and t12 are all given 1 for DS^{ctx}, and their ssp contains all types to communicate with other nodes, they cannot enter since t11 has no functional services and t12 is considered insufficient specified for the current plant due to low UR. Indeed, the DS calculation of t12 also shows the dynamicity and resilience of the AC phase: NCA attackers attempting to fake their capabilities to increase its DS^{fct} may decrease their UR and CWR because of less functional services identified. Considering DS values as illustrated in Table VIII, the policy of the AC phase is strict: Only t9 and t10-1, namely understaffed and newness cases, received considerable DS^{fct} values. Furthermore, t9 and t10-1 both have relatively low DS values, which is in line with their newcomer status, i.e., they should earn reputation to improve their trustworthiness.

b) Returning to the same plant/moving to a new plant case: We set here all nodes are good nodes (GN), and they are all honest and will give 0.95 $\pm$ 0.05 (noise) [2] to rate the satisfactory services. We chose the t9 node as the newcomer to simplify the visualization of the changes in trust values, i.e., the controller forces this node to provide $s4$ and to rate other nodes' services at the same time.

[2]Noise $\pm$0.05 counted for all ratings.

TABLE VIII: DS values for newcomers of types 9∼12

DIG	9	10-1	10-2	11	12
DS^{fct}	1	0.75	0.75	0	0.3750
DS^{soc}	0.4894	0.2	0.2	0.2552	0.2552
DS^{ctx}	0	0.5	0	1	1
DS	0.6979	0.59	0.49	0.2410	0.4760
Decision	Y	Y	N	N	N

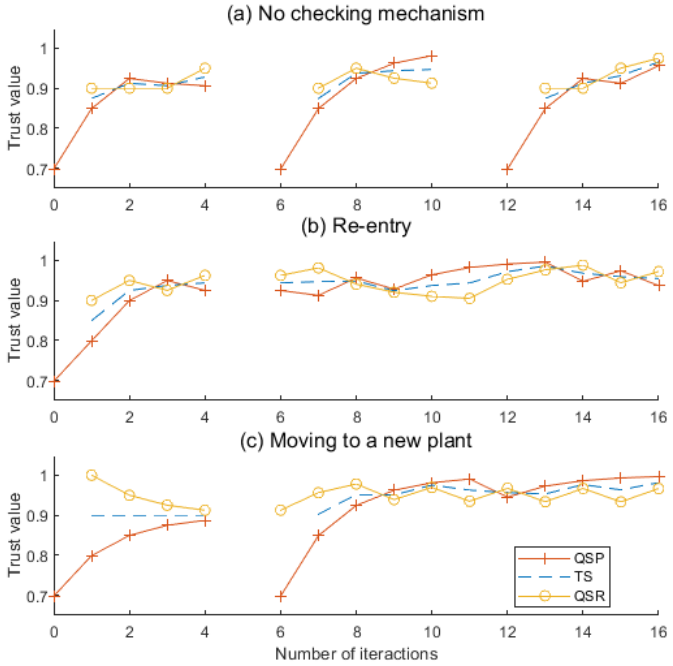


Fig. 9: Changes in trust values in three scenarios of the AC

In Fig. 9(a), without checking mechanism, t9 node suffers from gaining reputation after its re-entry even though its trust values remain great before it quits. Differently, Fig. 9(b) gives an example that the t9 node benefits from all previous trust values since it is treated as a returner rather than a newcomer. Lastly, in moving to a new plant case, t9 node can only continue using its QSR value.

2) SP selection: We demonstrate the effectiveness of the SP selection phase by two parts, the first one details how SP selection works, and the second part explains the importance of this phase in the plant TM.

a) Ranking SP by SS: Fig. 10 gives an example of the SP selection process, where we are looking for 5 SP out of 9 candidates (nodes of t2 and t3 + one t9) to conduct a workflow $\rightarrow$ composed by s1 and s2. We only visualize the DS of t9 since its SG are all null, and it is placed after the competition of CN.

As one can see, a node being outstanding at one service type may not be equally great at others, such as node 4 in Fig. 10(a). Furthermore, the ranking of SS also relies on the QSP of each node, e.g., node 7 with relatively poor OSG gets forth place in SS ranking due to its outstanding QSP. The performance analysis is discussed in the next part.

b) The performance of SP selection: We consider 3 scenarios: ranking the candidate SP by SS, only QSP, and random. We select 10 nodes (randomly, no t8) among CN to play WSP such that their service provision would be rated 0.25, and all other policies are unchanged, as stated in Section V-B. In addition, we employ OSG to compare three scenarios to illustrates the real quality level in terms of service composition.

As shown in Fig.11, the OSG values of ranking by SS case remain stable and outperform the random one and only QSP one. The random one is unsteady, and its OSG values are evidently bad. Ranking by QSP case is more stable than the random one, but it is still occasionally exceeded by random one, i.e., it does not extract the best SP. Moreover, OSG values in ranking by QSP case also have a decreasing trend since QSP is positively correlated with the feedback. Therefore, ranking by SS is optimal in SP selection, as it enables the selection of the best SP among candidates and prevents SBA by measuring the SG values.

3) Resilience: This section focuses on the resilience against attacks on services, namely NCA, OOA, CBA, SBA, BMA, BSA, and SPA. We observe the behaviors of the attacker by illustrating the changes in its trust value. In fact, the attacker

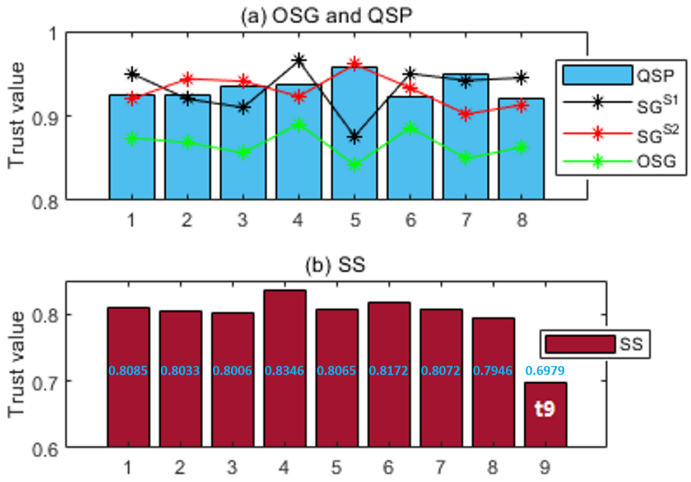


Fig. 10: A capture of selection score (SS) computation based on candidate nodes' overall service grade (OSG) and quality of service provider (QSP)

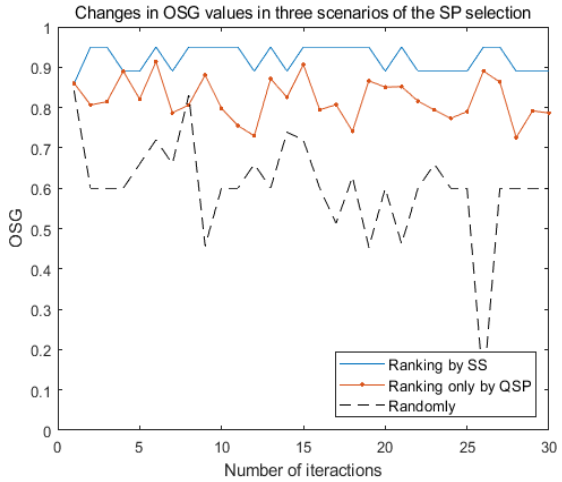


Fig. 11: Changes in overall service grade (OSG) values in three scenarios of the SP selection

will be treated with specific measures when some of their trust values are under 0.5 (TS, QSR, and SG). For this reason, we force the SP selection to choose the attacker to conduct/rate service in order to visualize their behavior and validate the effectiveness of the proposed model.

4) OOA: To demonstrate the behavior of the OOA attacker, we set a malicious node that provides services continuously by switching between good (0.95) and bad (0.45) over time. Fig. 12 shows that the OOA attacker behaves intelligently to keep its QSP above a certain threshold, e.g., 0.5. With the help of θ, the manager can detect earlier the OOA attacker by measuring the stability of behavior in terms of time, and punishing the services without good feedback. Furthermore, it costs longer time for the attacker to recover its reputation. As discussed in Section IV-A4c, service provider nodes can only gain reputation by keeping providing good services in a continuous way.

5) CBA: In the simulation performed to observe CBA, we consider the attacker misbehaves with 30% client nodes during its service provision. Table IX illustrates average feedback values from the attacked nodes and other nodes to evaluate the attacker.

TABLE IX: Feedback values for the attacker after the attack launched

Description	Value
Avg feedback from the attacked nodes	0.452
Avg feedback from others	0.9442

In Fig. 13, QSP of 'with λ' case decreases faster than the case without λ since λ enables the reduction of the QSP of nodes that behave differently with different nodes. The punishment degree of 'without' case is insufficient to segregate the attacker from general nodes, even though the simulation lasts long enough, i.e., it is too difficult to detect a CBA attacker

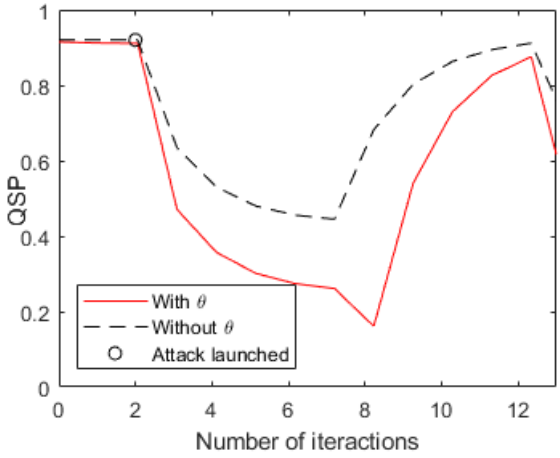


Fig. 12: Changes in quality of service provider (QSP) with θ and without θ in presence of on-off attack (OOA).

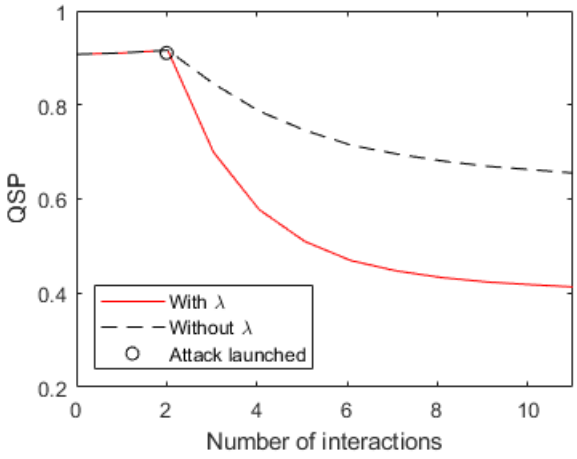


Fig. 13: Changes in quality of service provider (QSP) with λ and without λ in presence of conflicting behavior attack (CBA).

without λ.

6) SBA: In this scenario, we deploy one CN node of t3 as the SBA attacker, since it has three service types. We consider all three service types $s1{\sim}s3$ targets of SBA, i.e., in each service provision phase, the attacker picks one service type to misbehave (rated 0.45), and it does well for other types (rated 0.95). As we did before, we force the attacker to conduct service to observe its behaviors under the SG mechanism.

Fig. 14 illustrates the changes in SG values of three service types. As it can be seen, the attacker switches between services to alternatively behave well and badly, e.g., it recovers SG^{s1} and SG^{s2} when misbehaving in $s3$. Eventually, SG values all drop under 0.5. As defined in Section IV-A4d, the service types whose SG goes under 0.5 will be regarded as nonfunctional, and the SP cannot provide such service anymore. Furthermore, we measure the selection score SS by looking at the SG and QSP, the attacker's SG values are poor because of conducting bad services, and this also decreases its QSP value. Therefore, it has less chance to be selected as a SP.

7) BMA/BSA: These attacks lead a good service provider to be snubbed and a bad service provider to be promoted. To handle with them, comparing individual feedback with average level can determine the honesty of service raters. We set a compromised node act as a SR that dishonestly rates the 30% of SP (rate 0.45/0.95 for good/bad services). As shown in Fig. 15(a), the attacked node's QSP recovers its trustworthiness since the attacker node has been detected and isolated because of $TS < 0.5$. Analogously, badly-performing nodes' QSP drops after the isolation of the attacker node, in Fig. 15(b). Indeed, BMA and BSA act in an opposite way about each other, but they both aim at disrupting the rating mechanism, so that the good SP does not get positive feedback and the malfunctioning/malicious ones earn reputation.

8) SPA: SPA mainly consists of two kinds [32, 33]: The first case indicates that an end-user possessing multiple nodes in the network, can promote these nodes by self-assigning good feedback; To have greater competitiveness in SP selection, the node may promote its importance by boosting several trust values in second case. The first case often occurs in SIoT, since users can easily hold multiple endpoints, but it is constrained in IIoT, due to the plant controller as a centralized entity to conduct

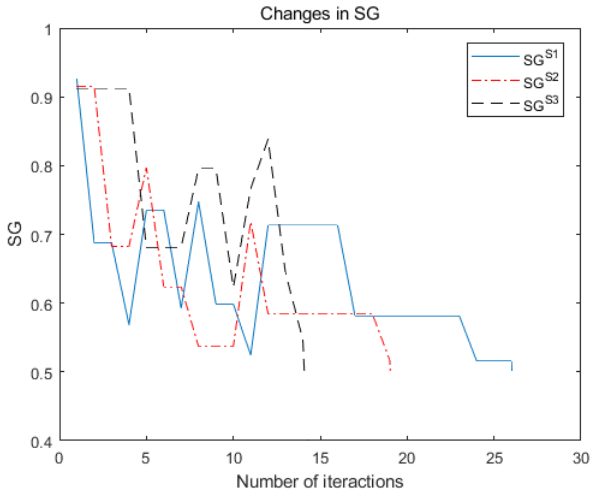


Fig. 14: Changes in service grade (SG) values by service types in presence of selective behavior attack (SBA).

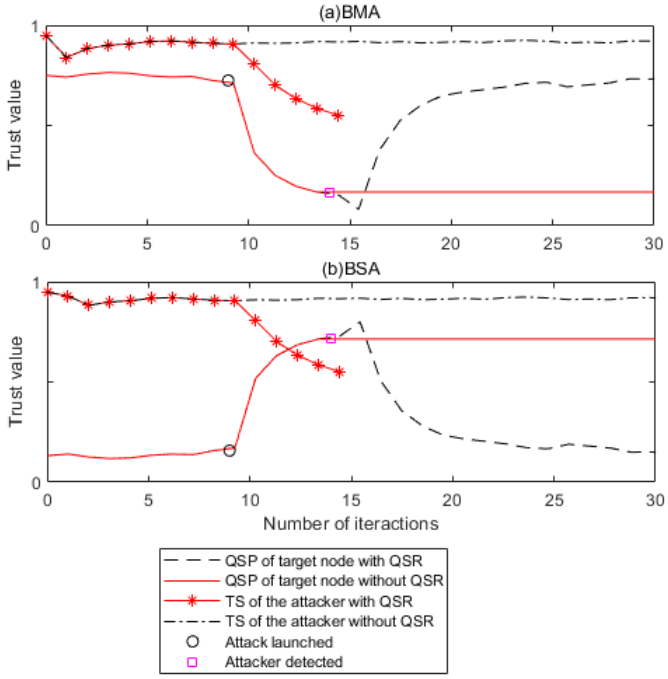


Fig. 15: Changes in trust values of both attacked and attacker nodes with quality of service rater (QSR) evaluation and without this evaluation in presence of (a) bad mouthing attack (BMA) and (b) ballot stuffing attack (BSA).

the local TM. Moreover, the service provider is disallowed to rate the service provided by itself in our model. To prevent the second one, it is necessary to exclude the metrics that are not relevant to service type and provider. For example, in our model, the way that the node can improve its importance in the SP selection is to be rated positively to increase its SG and QSP. To do so, it has to conduct outstanding services, and thus earning the reputation without giving satisfying services is impossible.

9) Comparison and discussion: In this part, we compare SOPHT with TMCoI-SIOT model [34] and CITM-IoT model [35] (thereafter referred as "CoI" and "CITM") to prove the robustness and ability of SOPHT under OOA, BMA and BSA. We choose these two models since they are reputable work and also recent proposed TM model addressing OOA and BMA/BSA attacks. Firstly, we foucs a comparative performance analysis of SOPHT against CoI and CITM models under OOA and BMA attacks, where the attack scenario remain unchanged as above. Next, we focus on single IIoT plant by varying percentage of malicious nodes (pm) to demonstrate the global performance evaluation by using F-scores, which are recall and precision.

The precision and the recall, defined as follows:

$$Precision = \frac{tp}{tp + fp}, \quad Recall = \frac{tp}{tp + fn}, \tag{33}$$

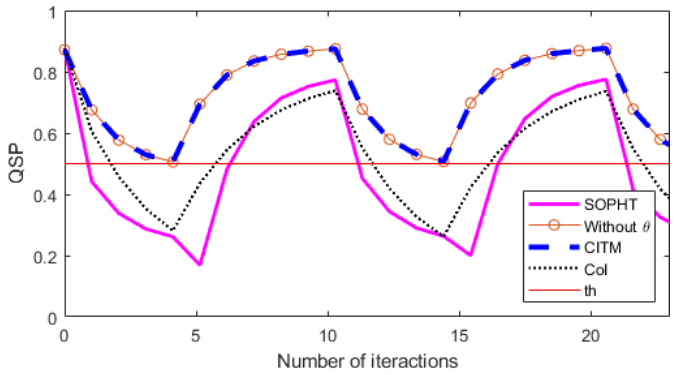


Fig. 16: Changes in quality of service provider (QSP) of attacked nodes in presence of on-off attack (OOA).

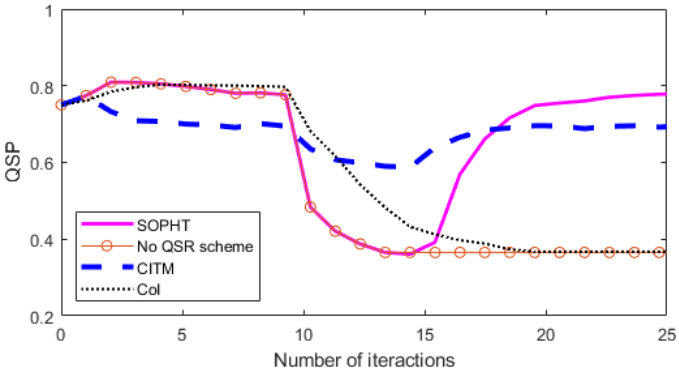


Fig. 17: Changes in quality of service provider (QSP) of attacked nodes in presence of bad mouthing attack (BMA).

where tp refers to attackers accurately detected, tp means normal nodes identified as attackers, and fn counts attackers not detected.

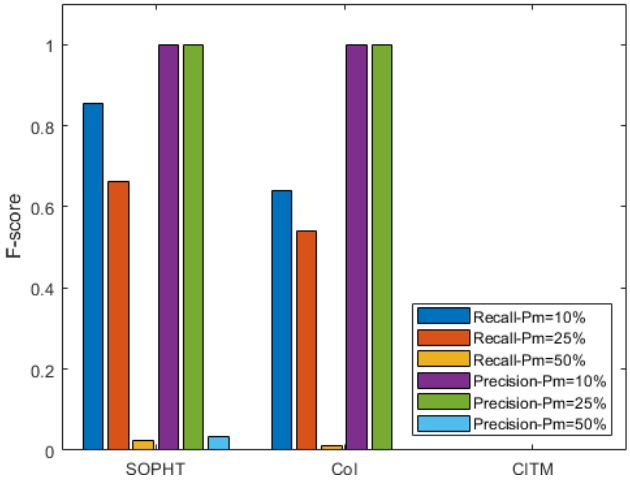


Fig. 18: Changes in quality of service provider (QSP) of attacked nodes in presence of bad mouthing attack (BMA).

The defense techniques against the attacks on services can be categorized into two groups: preventing the source of attack and punishing the misbehavior. The former type aims to make attacks avoidable, while the latter can only react after the attack has occurred. In the proposed TM model, NCA and SPA are addressed with predefined strict policies as described in Sections IV-B and V-B8. The countermeasures of other attacks, namely OOA, CBA, SBA, BMA, and BSA, are exclusively working after the service ratings are launched since defense strategies compare the individual opinion with others' or detect the gaps in terms of the time or service types. To summarise, the first type of attacks can be bounded by a systematic barrier, such as setting up a centralized TM to prohibit multiple identities, disallowing SP to rate the services by itself, and enforcing dynamic and strict AC policies for newcomers. The second type of attacks is more like facing a disciplinary mechanism that the attacker will be penalized once its misbehavior is detected.

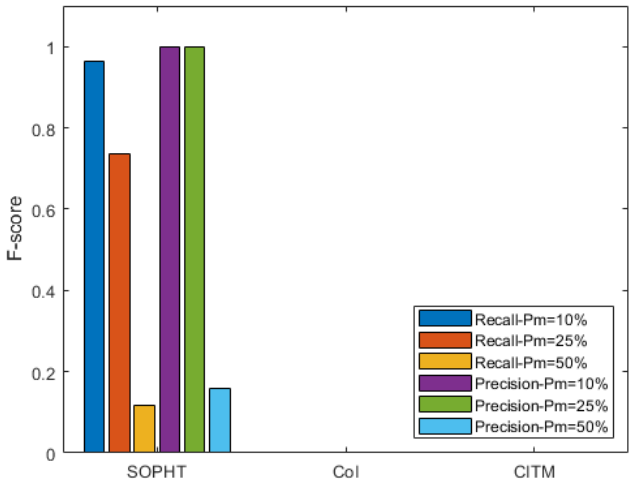


Fig. 19: Changes in quality of service provider (QSP) of attacked nodes in presence of bad mouthing attack (BMA).

C. Inter-plant TM

This section moves to the evaluation of the inter-plant TM. Table X illustrates the simulation configuration of the inter-plant TM, we set 5 plants with different service types and neighborhood situations. We consider that p1 and p4 are constrained so that they would ask other plants to give a hand by sending nodes providing functional services. Moreover, we set p2 that performs uncooperatively to p1.

TABLE X: Configuration of 5-plant simulation

Conf.	Description				
Plant	p1	p2	p3	p4	p5
Service types	1∼20	6∼25	15∼35	26∼35	30∼40
Neighbor	p2	p1,p3,p4	p2,p4,p5	p2,p3,p5	p3,p4
Constrained	Y	N	N	Y	N
Uncooperative	N	To p1	N	N	N

Fig. 20 gives the simulation results with related trust values, namely IS, CO, and CS. Sub-figures in each line represent the subjective opinions from the evaluator plant, e.g., the first line corresponds to the trust values calculated by the p1 to assess other plants. There are some no-interaction cases, such as p1-p4 and p1-p5, as shown in sub-figures 14, 15, 41, and 51, where the CO values remain unchanged, i.e., no nodes moving to a new plant between them. p1 differs from p4 and p5 in terms of services as defined in the simulation configuration, and thus they do not interact at all even although p1 is constrained. Particularly in sub-figures 53 and 35, p3 and p5 have common services but they keep silent to each other, this is because they are both unconstrained.

Since we set p2 to perform in an uncooperative manner with p1, as can be seen in sub-figure 12, the CO and CS values go down, and notably, these values increase at the same time in sub-figure 13. p2 sends nodes providing functional services to help p1 address p1's constrained status, as illustrated at the beginning of sub-figure 12. However, p1 suffers from the malfunctioning or malicious nodes from p2, and it switches the source of nodes when it detects that p2 is uncooperative, i.e., $CS_{12}<0.5$. p3 does not interact with p1 at the beginning due to the poor IS_{13} value, such that p1 does not count p3 as helpful. After that p2 is classified into the distant plant (DP) category, p1 asks p3 for help as they have common services. Similarly, p3 and p5 meet the need of p4, and thus their communication frequency remains significant.

VI. Conclusion

In this paper, we have presented a phase-based trust management framework for service-oriented IIoT (SOPHT), which considers two trust levels: plant and inter-plant. The plant TM designed four phases: access control, service provider selection, service evaluation, and node classification, to address the security issue in IIoT from the service perspective, and more importantly, the countermeasures against attacks on services, namely NCA, OOA, CBA, SBA, BMA, BSA, SPA. The inter-plant TM assesses the trustworthiness between plants by dynamically observing their relationship in terms of cooperativeness. Through intensive simulations, we have verified that the SOPHT model is adequate and accurate for dealing with trust issues in IIoT. For putting forward SOPHT into industrial plants, as future work, we plan to implement our SOPHT model functions within real-world SOA-based IIoT devices including service providers, service raters, and trust manager on the controllers.

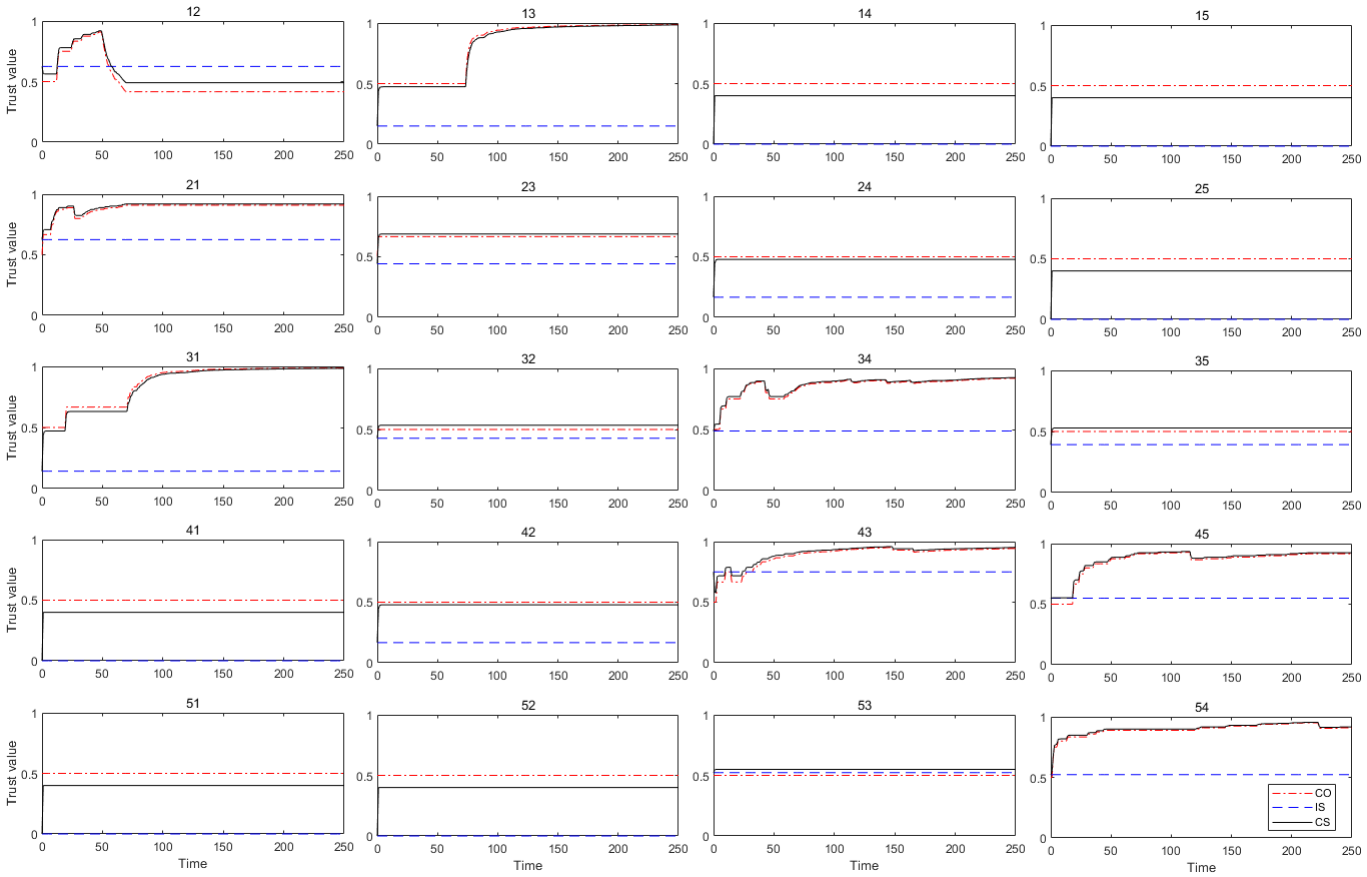


Fig. 20: Changes in centrality (G), cooperativeness (CO), conformity (CF) and inter-plant trust (PT) values in 5-plant scenario

REFERENCES

[1] Andreja Rojko. "Industry 4.0 concept: Background and overview." In: *International Journal of Interactive Mobile Technologies* 11.5 (2017).

[2] Yuan Li et al. "Towards a theoretical framework of strategic decision, supporting capability and information sharing under the context of Internet of Things". In: *Information Technology and Management* 13.4 (2012), pp. 205–216.

[3] Ling Li. "China's manufacturing locus in 2025: With a comparison of "Made-in-China 2025" and "Industry 4.0"". In: *Technological Forecasting and Social Change* 135 (2018), pp. 66–74.

[4] James P Farwell and Rafal Rohozinski. "Stuxnet and the future of cyber war". In: *Survival* 53.1 (2011), pp. 23–40.

[5] Jeff Stone. *Cyberattack at med-tech conglomerate Hoya slowed production at Thai factory by 60 percent*. 2019. URL: https://www.cyberscoop.com/hoya-cyberattack-cryptojacking-thailand/.

[6] Abi Millar. *Five pharma cybersecurity breaches to know and learn from*. 2021. URL: https://www.pharmaceutical-technology.com/features/pharma-cyber-attacks/.

[7] *Positive Technologies: 91% of Industrial Companies Open to Cyber-Attacks*. 2021. URL: https://www.ptsecurity.com/ww-en/about/news/positive-technologies-91-of-industrial-companies-open-to-cyber-attacks/.

[8] Yongxin Liao, Eduardo de Freitas Rocha Loures, and Fernando Deschamps. "Industrial Internet of Things: A systematic literature review and insights". In: *IEEE Internet of Things Journal* 5.6 (2018), pp. 4515–4525.

[9] Fei Tao et al. "SDMSim: a manufacturing service supply–demand matching simulator under cloud environment". In: *Robotics and computer-integrated manufacturing* 45 (2017), pp. 34–46.

[10] Jiangfeng Cheng et al. "Industrial IoT in 5G environment towards smart manufacturing". In: *Journal of Industrial Information Integration* 10 (2018), pp. 10–19.

[11] Sameer Mittal et al. "Smart manufacturing: Characteristics, technologies and enabling factors". In: *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture* 233.5 (2019), pp. 1342–1361.

[12] Nguyen B Truong, Tai-Won Um, and Gyu Myoung Lee. "A reputation and knowledge based trust service platform for trustworthy social internet of things". In: *Innovations in clouds, internet and networks (ICIN), Paris, France* (2016), pp. 104–111.

[13] Hansong Xu et al. "A survey on industrial Internet of Things: A cyber-physical systems perspective". In: *IEEE Access* 6 (2018), pp. 78238–78259.

[14] Norihisa Komoda. "Service oriented architecture (SOA) in industrial systems". In: *2006 4th IEEE international conference on industrial informatics*. IEEE. 2006, pp. 1–5.

[15] Naseem Ibrahim and Brandon Bench. "Service-oriented architecture for the internet of things". In: *2017 International Conference on Computational Science and Computational Intelligence (CSCI)*. IEEE. 2017, pp. 1004–1009.

[16] Ray Chen and Jia Guo. "Dynamic hierarchical trust management of mobile groups and its application to misbehaving node detection". In: *2014 IEEE 28th international conference on advanced information networking and applications*. IEEE. 2014, pp. 49–56.

[17] Yan Lindsay Sun et al. “A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks”. In: *Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications*. IEEE. 2006, pp. 1–13.

[18] Yanli Yu et al. “Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures”. In: *Journal of Network and computer Applications* 35.3 (2012), pp. 867–880.

[19] Yosra Ben Saied et al. “Trust management system design for the Internet of Things: A context-aware and multi-service approach”. In: *Computers & Security* 39 (2013), pp. 351–365.

[20] Luigi Atzori et al. “The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization”. In: *Computer networks* 56.16 (2012), pp. 3594–3608.

[21] A Meena Kowshalya and ML Valarmathi. “Trust management for reliable decision making among social objects in the Social Internet of Things”. In: *IET Networks* 6.4 (2017), pp. 75–80.

[22] Carolina VL Mendoza and João H Kleinschmidt. “Mitigating on-off attacks in the internet of things using a distributed trust management scheme”. In: *International Journal of Distributed Sensor Networks* 11.11 (2015), p. 859731.

[23] Fenye Bao and Ray Chen. “Trust management for the internet of things and its application to service composition”. In: *2012 IEEE international symposium on a world of wireless, mobile and multimedia networks (WoWMoM)*. IEEE. 2012, pp. 1–6.

[24] Mohammad Mehedi Hassan et al. “Increasing the trustworthiness in the industrial IoT networks through a reliable cyberattack detection model”. In: *IEEE Transactions on Industrial Informatics* 16.9 (2020), pp. 6154–6162.

[25] Chaimaa Boudagdigue et al. “Trust management in industrial Internet of Things”. In: *IEEE Transactions on Information Forensics and Security* 15 (2020), pp. 3667–3682.

[26] Runbo Su et al. “PDTM: Phase-based dynamic trust management for Internet of things”. In: *ICCCN 2021-30th International Conference on Computer Communications and Networks*. 2021.

[27] Golam Kayas et al. “SUPnP: Secure Access and Service Registration for UPnP-Enabled Internet of Things”. In: *IEEE Internet of Things Journal* (2021).

[28] Kwok-Yan Lam and Chi-Hung Chi. “Identity in the Internet-of-Things (IoT): New challenges and opportunities”. In: *International Conference on Information and Communications Security*. Springer. 2016, pp. 18–26.

[29] Stavros Salonikias et al. “Access control in the industrial internet of things”. In: *Security and privacy trends in the industrial internet of things*. Springer, 2019, pp. 95–114.

[30] Charith Perera et al. “Context aware computing for the internet of things: A survey”. In: *IEEE communications surveys & tutorials* 16.1 (2013), pp. 414–454.

[31] Asrin Vakili and Nima Jafari Navimipour. “Comprehensive and systematic review of the service composition mechanisms in the cloud environments”. In: *Journal of Network and Computer Applications* 81 (2017), pp. 24–36.

[32] Ray Chen, Fenye Bao, and Jia Guo. “Trust-based service management for social internet of things systems”. In: *IEEE transactions on dependable and secure computing* 13.6 (2015), pp. 684–696.

[33] Wafa Abdelghani. “A multi-dimensional trust-model for dynamic, scalable and resources-efficient trust-management in social internet of things”. Theses. Université Paul Sabatier - Toulouse III ; Université de Sfax (Tunisie), Dec. 2020. URL: https://tel.archives-ouvertes.fr/tel-03215718.

[34] Oumaima Ben Abderrahim, Mohamed Houcine Elhdhili, and Leila Saidane. “TMCoI-SIOT: A trust management system based on communities of interest for the social Internet of Things”. In: *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE. 2017, pp. 747–752.

[35] Mohammad Dahman Alshehri, Farookh Khadeer Hussain, and Omar Khadeer Hussain. “Clustering-driven intelligent trust management methodology for the internet of things (CITM-IoT)”. In: *Mobile networks and applications* 23.3 (2018), pp. 419–431.