Proceedings of the ASME 2018 International Design Engineering Technical Conferences & Computers and Information in Engineering Conference
IDETC/CIE 2018
August 26-29, 2018, Quebec City, Quebec, Canada

DETC2018-86198

TRUST BASED CYBER-PHYSICAL SYSTEMS NETWORK DESIGN

Yan Wang
Woodruff School of Mechanical Engineering
Georgia Institute of Technology, Atlanta, GA 30332
yan.wang@me.gatech.edu

ABSTRACT

Cyber-physical systems (CPS) extensively share information with each other, work collaboratively over Internet of Things, and seamlessly integrated with human society. Designing CPS requires the new consideration of design for connectivity where security, privacy, and trust are of the main concerns. Particularly trust can affect system behavior in a networked environment. In this paper, trustworthiness is quantitatively measured by the perceptions of ability, benevolence, and integrity. Ability indicates the capabilities of sensing, reasoning, and influence in a society. Benevolence measures the genuineness of intention and reciprocity in information exchange. Integrity captures the system predictability and dependability. With these criteria, trust-based CPS network design and optimization are demonstrated.

1 Introduction

Systems with integrated capabilities of sensing, computing, communication, and execution were recently termed as cyber-physical systems (CPS). They are the realization of mechanisms where physical components are directly controlled and monitored by computational algorithms and tightly integrated with Internet and users. Most of future industry and consumer products such as manufacturing equipment, office and home appliances, personal health care devices, automobiles, and many others are likely to be the examples of CPS. The unprecedented values and functions of CPS rely on the networks formed by themselves, which is also referred to as the Internet of Things.

In addition to common design challenges for systems of systems such as interoperability, scalability, lifecycle management, resiliency, usability, adaptability, safety, security, and sustainability, there are a few unique characteristics about CPS products. First, with the advancement of novel materials for sensing, actuation, computation, and communication, future CPS may have diverse physical forms and properties, including those with self-adaptive, biomorphological, and soft structures. CPS can be created at different size scales and can exist at micro- and nano-scales. CPS may also have certain levels of reasoning capability and intelligence as well as self-production and self-organization characteristics [1, 2]. Second, the complexity of CPS products has significantly increased from traditional ones. Designing each product requires the consideration of materials, hardware, software, algorithms, as well as network connectivity [3]. High complexity requires new systems design principles. For instance, it is impossible to keep networked low-cost CPS with millions of nodes secure and failure-proof. Instead resilience should be the design objective [4, 5]. Third, CPS extensively interact with human users and will be deeply embedded in human society. Social consciousness and cognitive capability will also be important factors in systems design. For instance, issues of privacy and trust in the context of information sharing and collaboration should be considered.

The controllability of shared information quickly diminishes as it propagates through CPS networks. Therefore trust is essential for CPS nodes to collaborate. Here, how to quantify trustworthiness and apply it in the design of CPS is studied. In recent research of trust quantification for networked systems, two approaches are taken. In the top-down approach, trustworthiness is treated as an overall perception or belief about an individual's

reputation or ability. It is quantified with probabilistic or non-probabilistic measures. In the bottom-up approach, trustworthiness consists of multiple factors such as availability, dependability, and quality of services, each of which can be calculated from the statistics of physical systems, e.g. data transmission rates, executed routing protocols, and positive recommendations. In CPS networks, the quantification of trustworthiness needs to be at the systems level with multiple functions and networked communities, instead of only at individual components.

With the intensive interaction between humans and CPS, user-oriented trust management is essential. Trust is a state of mind, subjective, and multi-faceted. The study of trust should be in the context of social behavior. The dynamics of human perception and subjectivity needs to be emphasized in trustworthiness quantification for CPS.

In this paper, a perception-oriented approach is taken to quantify trustworthiness. Trustworthiness is measured by perceptions of three major metrics instead of an abstract one. The three metrics, which include perceptions of *ability*, *benevolence*, and *integrity*, are carefully chosen based on the concepts studied in social sciences and to avoid redundancy. To model large-scale CPS networks, a probabilistic graph model is applied to capture the functions of sensing, prediction, and communication. This mesoscale model provides a generic abstraction of CPS networks with scalability consideration. The three trustworthiness metrics are calculated based on the probabilistic graph model. These three perception-level metrics are calculated with Bayesian methods. Compared to other trustworthiness quantification approaches, the uniqueness of the proposed approach includes the considerations of different CPS functions including sensing, prediction, and communication. The perception based quantification method directly models subjectivity of beliefs and the influence of social behavior, with quantitative measures of ability, benevolence, and integrity, which have not been considered in other quantitative approaches.

In the remainder of the paper, a review of relevant work on trust quantification in the domains of computer and social sciences is first provided. Then the new probabilistic graph model is introduced in Section 2.2. The metrics of ability, benevolence, and integrity are provided in Sections 3.1, 3.2, and 3.3 respectively. The estimation of metrics from network traffic statistics is demonstrated in Section 4. In Section 5, the network design and optimization approach based on the metrics of ability and benevolence is described.

2 Background

2.1 Trust quantification

The study of trust in computer science had been traditionally focused on security policy for exchanging credentials, controlling access, and referring reputation [6, 7]. Recently, it was studied in the context of social networks and semantic web [8, 9]. In the vast majority of those studies, trust was only defined qualitatively instead of providing quantitative specifications and calculations.

In social networks and multi-agent environments, most researchers model trust as reputation and rely on users' explicit ratings and recommendations to estimate the levels of trust. For instance, trust was calculated from the scaled reputation ratings [10], the number of finished transactions [11], and users' explicit ratings [12].

In computer networks, trust was measured by quality of services, the numbers of forwarded data packets, executed routing protocols, etc. For sensor networks, trust has been measured with local and global success rates of transactions [13], consistency of individual nodes from their historical data [14], consistency between nodes in local regions [15], as well as neighbors' data forwarding behaviors [16].

The subjective and uncertain aspects of trustworthiness has been modeled with belief of information reliability [17], Dempster-Shafer evidence [18], expectation of fulfilled commitments [19], Bayesian networks [20], probability of resource availability [21], and information entropy in data exchange [22]. Fuzzy logic was also applied to capture the linguistic imprecision of trust description, either as one concept [23, 24], or a combination of multiple factors such as ability, availability, motivation, usefulness, honesty, and others [25, 26].

Different qualitative definitions of trust exist in the domains of psychology, marketing, human behavior, and organization. Mayer et al. [27] carefully studied dozens of characteristics of trust in literature, identified commonality, and defined trustworthiness as a set of three categories of perception: *ability*, *benevolence*, and *integrity*. Ability is about perception of skills, expertise, and competency associated with trustee. Benevolence is the extent to which the trustor believes that the trustee acts for the welfare of the trustor, rather than just maximizing its own profit. Benevolence is a summary of related characteristics such as loyalty, openness, receptivity, and availability. Integrity is the trustor's perception that the trustee will be honest and adhere to an acceptable set of principles. Integrity is associated with consistency, discreetness, fairness, promise fulfillment, reliability, and value congruence.

The ability-benevolence-integrity model has been widely adopted in different fields. The three factors have been applied in designing psychological and behavioral studies of trust [28, 29]. The model was applied to measure the trustworthiness of online shopping merchants [30], and electronic banking service providers [31]. The model has also been adopted in designing information systems with better privacy policies [32], better understanding of users intention [33], user participation [34], security [35], and technology integration [36]. The concerns of security, privacy, and trust in CPS networks are similar to those in traditional information systems. The trust model of ability, benevolence, and integrity thus can be applied in CPS. Nevertheless,

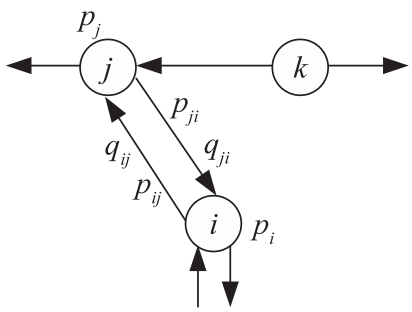


Figure 1: The probabilistic graph model

in all of the above studies ability, benevolence, and integrity were defined qualitatively without providing quantitative measures.

In this work, quantitative metrics of ability, benevolence, and integrity are defined. The perceptions of these three metrics are captured based on a generic probabilistic graph model of CPS networks. The graph model provides a mesoscale abstraction to represent the major functions of information gathering and exchange between nodes in CPS networks. Particularly, the probability of accurate sensing and prediction by each node, as well as the probabilities of positive and negative correlations as mutual influence between nodes are explicitly modeled, which allows for quantitative measurement of ability and benevolence directly. Notice that ability, benevolence, and integrity aspects of trust co-exist in trustworthiness quantification. These three independent dimensions need to be considered separately and not simply combined into one metric.

2.2 Probabilistic graph model

As illustrated in Fig. 1, a probabilistic graph [4, 5] $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{R}, \mathcal{P}, Q)$ is a collection of nodes $\mathcal{V} = \{v_k\}$ and directed edges $\mathcal{E} = \{(v_i, v_j)\}$. Each node v_k is associated with a *prediction probability* $p_k \in \mathcal{R}$, and each edge (v_i, v_j) is associated with a *P-reliance probability* $p_{ij} \in \mathcal{P}$ and a *Q-reliance probability* $q_{ij} \in Q$.

The prediction probability p_k is the probability that node k predicts the true state of world θ and is defined as

$$P(x_k = \theta) = p_k, \tag{1}$$

where x_k is the state variable of node k. The information dependency between node j and node i is modeled by P-reliance probability

$$P(x_j = \theta | x_i = \theta) = p_{ij}, \tag{2}$$

and Q-reliance probability

$$P(x_j = \theta | x_i \neq \theta) = q_{ij}. \tag{3}$$

P-reliance probability indicates the positive effect of information exchange between nodes, whereas Q-reliance probability captures the negative influence. Particularly $P(x_k = \theta | x_k = \theta)$ and $P(x_k = \theta | x_k \neq \theta)$ indicate how much a node's prediction relies on its own observation. To simplify the notation, we use $P(x_k)$ to denote $P(x_k = \theta)$, $P(x_k^c)$ to denote $P(x_k \neq \theta)$, $P(x_j|x_i)$ to denote $P(x_j = \theta | x_i = \theta)$, and $P(x_j|x_i^c)$ to denote $P(x_j = \theta | x_i \neq \theta)$. Note that the probabilistic graph model here is different from Bayesian belief network.

CPS nodes collect information by themselves or from their neighboring collaborators. With the new information, the prediction probabilities are updated. Different information assimilation rules can be adopted by nodes to update their prediction probabilities, such as best-case, worst-case, and Bayesian rules.

An example *best-case* or *optimistic* fusion rule is

$$P'(x_k) = 1 - \Pi_{i=1}^{M}(1 - P(x_k|x_i)), \tag{4}$$

where node k has a positive prediction with updated probability P' if any of the M nodes as its information sources provides a positive cue. Some variations of this rule can also be used, such as

$$P'(x_k) = 1 - \Pi_{i=1}^{M_1}(1 - P(x_k|x_i))\Pi_{j=1}^{M_2}(1 - P(x_k|x_j^c)), \tag{5}$$

where both positive cues from M_1 nodes and negative cues from M_2 nodes ($M_1 + M_2 = M$) are considered. Another version could be

$$P'(x_k) = 1 - \Pi_{i=1, i\neq k}^{M}(1 - P(x_k|x_i)), \tag{6}$$

where the node's own prior observation is not included in the update.

The *worst-case* or *pessimistic* fusion rule is

$$P'(x_k) = \Pi_{i=1}^{M} P(x_k|x_i), \tag{7}$$

where the prediction of a node is positive only if all cues it receives from other nodes are positive.

The *Bayesian* fusion rule is

$$P'(x_k) \propto P(x_k)\left[(P(x_k))^r (1 - P(x_k))^{M-r}\right], \tag{8}$$

where the prediction of node k is updated from prior prediction probability $P(x_k)$ given that r out of a total of M cues provided by others are positive.

For simplicity, only binary value of state variables is considered here. Obviously, further generalization to multi-valued discrete state variables is straightforward. Suppose there are a finite set of discrete values $\{\theta_1, \ldots, \theta_N\}$ that the state variable x_k can take. The multi-valued prediction probability $P(x_k = \theta_n)$ ($n \in \{1, \ldots, N\}$) can be obtained similar to binary values. Similarly, reliance probabilities $P(x_j = \theta_n | x_i = \theta_m)$ ($m, n \in \{1, \ldots, N\}$) can be obtained enumeratively.

The above information fusion rules can be similarly extended to multi-valued state variables. For instance, the optimistic fusion rule in Eq.(5) becomes

$$\begin{aligned} P'(x_k) = 1 - &\Pi_{i=1}^{M_1}(1 - P(x_k|x_i = \theta_1)) \cdots \\ &\Pi_{j=1}^{M_N}(1 - P(x_k|x_j = \theta_N)), \end{aligned} \tag{9}$$

The prediction and reliance probabilities can be estimated from the collected historical data. For instance, the prediction probability of a CPS node can be based on data collected by its sensing and reasoning units. It can be estimated as the frequency of correct prediction. The reliance probabilities can be estimated similarly from the frequencies of positive and negative predictions by the neighboring nodes given the node's own prediction. If no data are available, subjective estimations from domain experts can be elicited, with standard probability elicitation procedure.

3 Trustworthiness Metrics

The new quantitative trustworthiness metrics are perceptions of ability, benevolence, and integrity. They are summarized in this section. Detailed description and evaluation of the metrics are available in Ref. [37].

3.1 Ability

The ability of CPS consists of *capability* and *influence*. In the context of probabilistic graph model, the capability of a node is generally quantified as the perceived probability that it can provide accurate prediction about the true state of the world based on its available information. Within a networked society, the influence of a node to others, which can be interpreted as leadership, is also regarded as part of its ability. The leadership that a CPS node has is characterized as the extent of its positive or negative influence to its neighbors.

3.1.1 Capability of prediction The perception of ability is subjective and varies among different people. Suppose that the perceived capability for node j is the perceived prediction probability $A_j(\theta) = \mathbb{P}(P(x_j = \theta))$ with respect to the true state of world θ, which follows a Gaussian distribution with mean p_j and precision τ_0. Here $\mathbb{P}(\cdot)$ denotes perception. In other words, the perceived capability of node j is randomly distributed, with expectation

$$\mathbb{E}(A_j(\theta)) = p_j, \tag{10}$$

and variance

$$\mathbb{V}(A_j(\theta)) = \tau_j^{-1}. \tag{11}$$

In a society with extensive information exchange, the perception of capability can be updated with newly obtained information. For instance, if reliance probabilities with respect to node j are made available to the public, then the perceived capability of the node can be updated.

Suppose that the perceived reliance probabilities $L_{ij} = \mathbb{P}(P(x_j|x_i))$ and $L_{ij}^c = \mathbb{P}(P(x_j|x_i^c))$ for all $i, j \in \mathcal{V}$ are Gaussian random variables, with expectations

$$\mathbb{E}(L_{ij}|A_j) = p_{ij}(\forall i, j \in \mathcal{V}) \tag{12}$$

and

$$\mathbb{E}(L_{ij}^c|A_j) = q_{ij}(\forall i, j \in \mathcal{V}) \tag{13}$$

under the condition of the perceived capability A_j.

The variances of the perceptions may depend on the nature of information sources. For the perceptions related to the information shared with node j from others, the variances are

$$\mathbb{V}(L_{ij}|A_j) = \tau_{ij,p}^{-1}(\forall i \in \mathcal{S}_j), \tag{14}$$

and

$$\mathbb{V}(L_{ij}^c|A_j) = \tau_{ij,q}^{-1}(\forall i \in \mathcal{S}_j), \tag{15}$$

where $\mathcal{S}_j = \{v_i|(v_i, v_j) \in \mathcal{E}\}$ is the collection of *source nodes* with respect to node j and each of the source nodes sends information to node j. Without the loss of generality, we can assume that the variances of the perceived reliance probabilities are the same, i.e. $\tau_{ij,p} = \tau_{s,p}$ and $\tau_{ij,q} = \tau_{s,q}$ $(\forall i \in \mathcal{S}_j)$. The complete set of perceived P- and Q-reliance probabilities for the source nodes with respect to node j is denoted as $\mathcal{L}^{(+j)} = \{L_{ij}|i \in \mathcal{S}_j\} \cup \{L_{ij}^c|i \in \mathcal{S}_j\}$.

With the reliance probability information, the perception of capability is updated based on the Bayesian belief update scheme or Bayes' rule. Because the perceptions follow Gaussian distributions, the expectation of posterior perception for capability of node j is

$$\mathbb{E}(A_j(\theta|\mathcal{L}^{(+j)})) = \frac{\tau_j p_j + \tau_{s,p}\sum_{i\in\mathcal{S}_j} p_{ij} + \tau_{s,q}\sum_{i\in\mathcal{S}_j} q_{ij}}{\tau_j + \tau_{s,p}s_j + \tau_{s,q}s_j}, \tag{16}$$

where $s_j = |\mathcal{S}_j|$ is the number of source nodes with respect to node j.

The consideration of Q-reliance probabilities in capability in Eq.(16) is necessary. When a node gives correct prediction even when its information sources provide negative or wrong predictions, the node exhibits good capability. Also note that if the assumption of equal variances is not made, the posterior perception of capability in Eq.(16) still can be calculated with $\tau_{s,p}\sum_{i\in\mathcal{S}_j} p_{ij}$ replaced by $\sum_{i\in\mathcal{S}_j}\tau_{ij,p}p_{ij}$, $\tau_{s,q}\sum_{i\in\mathcal{S}_j} q_{ij}$ by $\sum_{i\in\mathcal{S}_j}\tau_{ij,q}q_{ij}$, $\tau_{s,p}s_j$ by $\sum_{i\in\mathcal{S}_j}\tau_{ij,p}$, and $\tau_{s,q}s_j$ by $\sum_{i\in\mathcal{S}_j}\tau_{ij,q}$ respectively.

The variance of the updated perceptions for the capability of node j is

$$\mathbb{V}(A_j(\theta|\mathcal{L}^{(+j)})) = (\tau_j + \tau_{s,p}s_j + \tau_{s,q}s_j)^{-1}. \tag{17}$$

3.1.2 Influence The influence or leadership of node j is associated with the effectiveness of information sharing from node j to others. When the information sharing from node j to *destination nodes* in $\mathcal{D}_j = \{v_k|(v_j, v_k) \in \mathcal{E}\}$ is considered, where each of the destination nodes receives information from node j, the perception of the capability of node j can be further updated. When the precision of the perceptions related to the information shared *from* node j to others are characterized by

$$\mathbb{V}(L_{jk}|A_j) = \tau_{jk,p}^{-1}(\forall k \in \mathcal{D}_j) \tag{18}$$

and

$$\mathbb{V}(L^c_{jk}|A_j) = \tau^{-1}_{jk,q}(\forall k \in \mathcal{D}_j), \tag{19}$$

the complete set of perceived P- and Q-reliance probabilities for the destination nodes with respect to node j is denoted as $\mathcal{L}^{(-j)} = \{L_{jk}|k \in \mathcal{D}_j\} \cup \{L^c_{jk}|k \in \mathcal{D}_j\}$. Similarly, to simplify the notation, it is assumed that the variances of the perceived reliance probabilities are the same, i.e. $\tau_{jk,p} = \tau_{d,p}$ and $\tau_{jk,q} = \tau_{d,q}$ $(\forall k \in \mathcal{D}_j)$. The expectation of the updated perception of ability based on the influence to others is

$$\mathbb{E}(A_j(\theta|\mathcal{L}^{(-j)})) = \frac{\tau_j p_j + \tau_{d,p}\sum_{k\in\mathcal{D}_j} p_{jk} + \tau_{d,q}\sum_{k\in\mathcal{D}_j}(1-q_{jk})}{\tau_j + \tau_{d,p}d_j + \tau_{d,q}d_j}, \tag{20}$$

where $d_j = |\mathcal{D}_j|$ is the number of destination nodes with respect to node j. Notice that $(1-q_{jk})$ is used here to quantify the influence of node j to others, which captures how likely others end up with negative predictions given that node j provides a negative cue.

The variance of the updated perceptions for node j's ability after obtained information from destination nodes is

$$\mathbb{V}(A_j(\mathcal{L}^{(-j)})) = (\tau_j + \tau_{d,p}d_j + \tau_{d,q}d_j)^{-1}. \tag{21}$$

3.1.3 Overall ability The expectation of the further updated perception of ability that includes both capability of prediction and influence to others is

$$\mathbb{E}(A_j(\theta|\mathcal{L}^{(+j)}, \mathcal{L}^{(-j)})) = \frac{\begin{bmatrix}\tau_j p_j + \tau_{s,p}\sum_{i\in\mathcal{S}_j} p_{ij} + \tau_{s,q}\sum_{i\in\mathcal{S}_j} q_{ij} \\ \quad + \tau_{d,p}\sum_{k\in\mathcal{D}_j} p_{jk} + \tau_{d,q}\sum_{k\in\mathcal{D}_j}(1-q_{jk})\end{bmatrix}}{\tau_j + \tau_{s,p}s_j + \tau_{s,q}s_j + \tau_{d,p}d_j + \tau_{d,q}d_j}. \tag{22}$$

The variance of the updated perceptions for node j's ability after both information from source and destination nodes is

$$\mathbb{V}(A_j(\theta|\mathcal{L}^{(+j)}, \mathcal{L}^{(-j)})) = (\tau_j + \tau_{s,p}s_j + \tau_{s,q}s_j + \tau_{d,p}d_j + \tau_{d,q}d_j)^{-1}. \tag{23}$$

3.1.4 Higher-order perception In a society, one's perception can be influenced by others' perceptions. In the context of trust, one's perceived trustworthiness can be a function of others' perceived trust levels because of mutual influence in judgment and decision making. Therefore, the previous ability perception model can be further extended to a higher-order one with the consideration of mutual influence. The expected ability in Eq.(22) and variance in Eq.(23) are considered as the *first-order* model, where the perception of a node's ability is only affected by its interaction with the immediate neighbors. For the second-order model, the ability of a node is also affected by the perceived abilities of its intermediate neighbors, particularly the destination nodes which it directly shares information with. That is, the ability of a node is also related to the abilities of the nodes that it has direct influence on.

If the notations of $\mathbb{E}(A_j(\theta|\mathcal{L}^{(+j)}, \mathcal{L}^{(-j)}))$ and $\mathbb{V}(A_j(\theta|\mathcal{L}^{(+j)}, \mathcal{L}^{(-j)}))$ are simplified to

$$\mathbb{E}(A_j(\theta|+,-)) = E_j \tag{24}$$

and

$$\mathbb{V}(A_j(\theta|+,-)) = V_j \tag{25}$$

respectively, then in the *second-order* model, the expected ability is

$$\mathbb{E}^{(2)}(A_j(\theta|+,-)) = \frac{\begin{bmatrix}V_j^{-1}\cdot E_j + \tau_{d,p}\sum_{k\in\mathcal{D}_j} p_{jk}(V_k^{-1}\cdot E_k) \\ \quad + \tau_{d,q}\sum_{k\in\mathcal{D}_j}(1-q_{jk})(V_k^{-1}\cdot E_k)\end{bmatrix}}{V_j^{-1} + \tau_{d,p}\sum_{k\in\mathcal{D}_j} p_{jk}V_k^{-1} + \tau_{d,q}\sum_{k\in\mathcal{D}_j}(1-q_{jk})V_k^{-1}}, \tag{26}$$

which is the same as the first-order expectation, and the variance is

$$\mathbb{V}^{(2)}(A_j(\theta|+,-)) = \left[V_j^{-1} + \tau_{d,p}\sum_{k\in\mathcal{D}_j} p_{jk}V_k^{-1} + \tau_{d,q}\sum_{k\in\mathcal{D}_j}(1-q_{jk})V_k^{-1}\right]^{-1}. \tag{27}$$

Similarly, the third-order model can be constructed by incorporating the perceived abilities of the neighbors' neighbors, which the reference node indirectly shares information with. Therefore, the higher-order perception model incorporates the lower-order perceptions, as an extension of weighted averages where weights are the associated precisions. Recursively the n^{th} order model is defined based on the $(n-1)^{th}$ order ones.

3.1.5 An illustrative example A graph with 11 nodes shown in Fig. 2 is used to illustrate. In the first case, the mean values of prediction probabilities for the 11 nodes are assumed to be 0.5, and the variances are 0.3. The means of P- and Q-reliance probabilities for all edges are assumed to be 0.9 and 0.1 respectively. The variances for reliance probabilities are 0.1. This is a scenario that individual nodes' sensing capabilities is limited. They need to work collaboratively to make predictions. The nodes rely on shared information in decision making. The CPS are working in a "collaborative" mode. The ability perceptions of all nodes, including the capability, influence, overall ability, and the second-order ability perception are shown in Fig. 3a, where the mean values are denoted by dots and standard deviations are denoted by error bars. Notice that a variance of 0.3 already overestimates variation. The corresponding standard deviation is over 0.7, whereas a probability value is between 0 and 1. Typically the variance of perceptions should be less than 0.3.

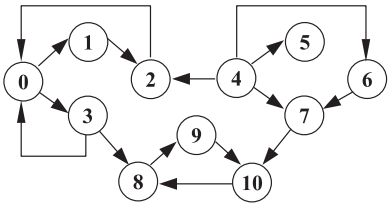


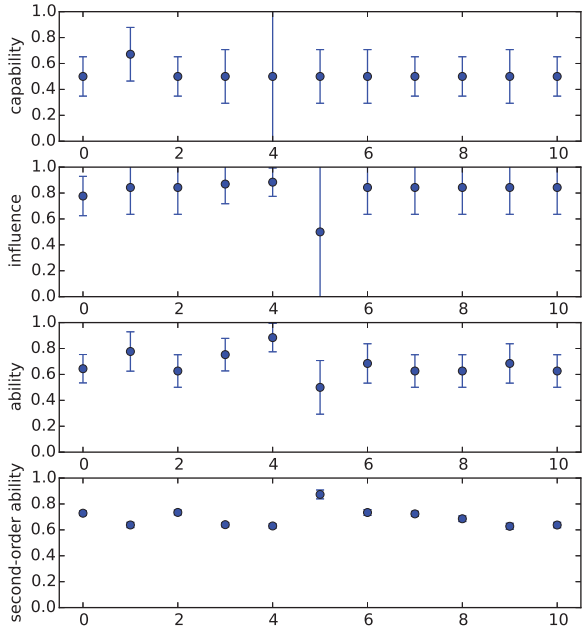
Figure 2: A simple graph with 11 nodes

From the result, it is seen that additional information from other nodes reduces the variance of prediction capability. When a node has no source nodes such as node 4, the variance of prediction capability is large. Similarly, the variance of influence is not reduced when nodes do not share information with others, such as node 5. Incorporating both capability and influence, the overall abilities are expected to increase when nodes work in the collaborative mode. Here, the means of abilities are mostly greater than 0.5. The variances also reduce. When the perceptions are incorporated in the second-order abilities, the variances are further reduced.

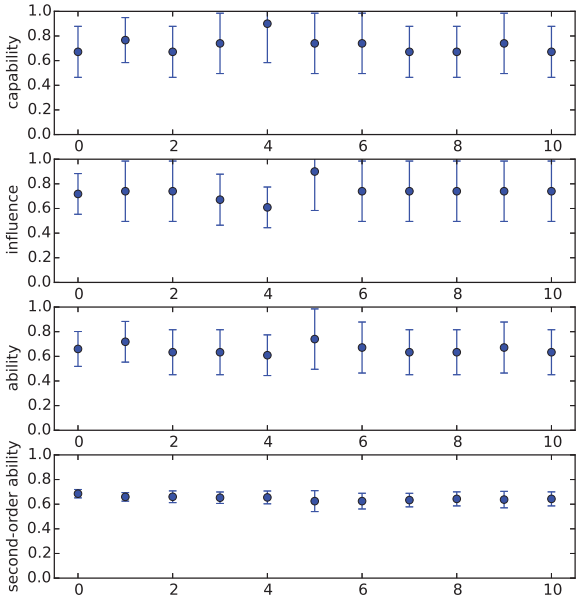
In the second scenario, nodes work in an "independent" mode. The mean values of prediction probabilities are 0.9, whereas the variances are 0.1. The means of P- and Q-reliance probabilities are 0.5, and their variances are 0.3. The nodes rely much more on individual predictions. The ability perceptions are shown in Fig. 3b. It is seen that variance reduction of the overall ability from capability and influence is not as significant as in the previous collaborative scenario. The changes of mean values by incorporating more information are not as dramatic as in the previous case, where the perceived trustworthiness for nodes 4 and 5 can fluctuate significantly from first order to second order.

3.2 Benevolence

Benevolence is a measure of the trustor's belief that how likely the trustee is motivated to do good to trustor, instead of for its own benefit. It captures the intention and motivation of the trustee. The degree of benevolence is low if the motivation is originated from ergocentric gain, and high from mutual benefits. Benevolence between individuals is critical for information sharing. Without such aspect of trust, large-scale data sharing in CPS networks is not possible. *Reciprocity* is proposed here to measure the extent that the partners whom we share information with reciprocally share information with us. There are also some other characteristics associated with benevolence such as loyalty and dependability. *Motive* as the second metric proposed here is to measure the level of good intention and motivation for interactions within the community.



(a) Perceived abilities of the 11 nodes in a collaborative scenario.



(b) Perceived abilities of the 11 nodes in an independent scenario.

Figure 3: The first- and second-order abilities of nodes in the model of Fig. 2 in two scenarios.

3.2.1 Deterministic reciprocity The pairwise deterministic *reciprocity* of node j with respect to node i, $r_{i,j}$, is measured by the shortest topological distance, in terms of the number of hops in the network that node j shares information with node i, as

$$r_{i,j} = \exp(-h_{j\to i}) - \exp(-h_{i\to j}) + \exp(-h_{i\to j} - h_{j\to i}), \quad (28)$$

where $h_{j\to i}$ is the minimum number of hops or the shortest topological distance for information flow from node j to node i. Note that $h_{i\to i} = 0$ and $r_{i,i} = 1$. When $i \neq j$, $\partial r_{i,j}/\partial h_{j\to i} < 0$ and $\partial r_{i,j}/\partial h_{i\to j} > 0$.

3.2.2 Perceived reciprocity With the further consideration of reliance probabilities as weights of edges in probabilistic graphs, the expected value of the perceived reciprocity of node j with respect to node i is calculated as

$$\mathbb{E}(R_{i,j}) = D_{KL}(p_{i\to j}||p_{j\to i}) - D_{KL}(p_{j\to i}||p_{i\to j}) + b_0, \quad (29)$$

where $D_{KL}(P||Q)$ is the Kullback-Leibler divergence from probability distribution Q to P, $p_{j\to i} = \Pi_{j\to i} p_{ab}$ is the product of all P-reliance probabilities where information flows through along the shortest path from node j to node i, and p_{ab} corresponds to the P-reliance probability from node a to node b along the path. Similarly, we have $p_{i\to j} = \Pi_{i\to j} p_{cd}$. When path $j \to i$ does not exist, the principle of maximum entropy is applied, thereof $p_{i\to j} = 0.5$. b_0 is a reference threshold of neutral value, which is predetermined such that $\mathbb{E}(R_{i,j}) > b_0$ when node j has a high reciprocity with respect to node i, and $\mathbb{E}(R_{i,j}) < b_0$ otherwise. To make the value range of reciprocity be between 0 and 1, the reference threshold is typically set as $b_0 = 0.5$. Additional scaling can be applied if necessary to keep the value range. Notice that $\mathbb{E}(R_{i,i}) = b_0$ because $D_{KL}(p_{i\to i}||p_{i\to i}) = 0$.

The variance of the perceived reciprocity can be calculated from the variances of P-reliance probabilities. Assuming the independence between the perceptions of P-reliance probabilities, the variance will be associated with the high-dimensional Gaussian distribution formed by these perceptions.

High-dimensional Gaussian distributions are costly to calculate and use. If there are m hops in the path from node j to node i, the variance associated with $p_{j\to i}$ will be an m-dimensional Gaussian distribution. To simplify the calculation for ease of application, a one-dimensional Gaussian distribution is used here for estimation purpose. The variance associated with the perceived reciprocity is conservatively estimated as

$$\mathbb{V}(R_{i,j}) = \min(\sum_{j\to i} \tau_{ab}^{-1} + \sum_{i\to j} \tau_{cd}^{-1}, V_{max}), \quad (30)$$

where τ_{ab} and τ_{cd} are the precisions associated with the P-reliance probabilities along paths $j \to i$ and $i \to j$ respectively, and V_{max} is the theoretical maximum value of variance. As discussed in Section 3.1.5, for a value range from 0 to 1 as probability, an upper bound of variance is around 0.5. The theoretical limit can be $V_{max} = 1.0$. When a path $j \to i$ does not exist, the associated variance is set to be V_{max}. At the same time, $\mathbb{V}(R_{i,i}) = 0$.

3.2.3 Motive Motive measures the motivation and intention of information sharing in a community. A high level of motive for a node indicates that it shares high-quality information with neighbors for the purpose of improving the overall functionality and performance of the community, whereas a low level of motive shows an ergocentric purpose instead of community-oriented benefit.

In the context of probabilistic graph model, the expected value of the perceived *motive* of node j is defined as

$$\mathbb{E}(M_j) = {p_j}^{d_j}, \quad (31)$$

where p_j is the prediction probability associated with node j, and $d_j = |\mathcal{D}_j|$ is the number of destination nodes with respect to node j. The baseline of motive ($M_j = 1$) is when the node has no destination nodes and does not share information with others. Compared to those sharing accurate predictions with others, a node sharing low-quality predictions with others tends to have a lower level of motive. Particularly, the more neighboring nodes it shares inaccurate predictions with, the less trustable the node is. In this case, the expected value of motive reduces quickly for low p_j as d_j increases.

The variance associated with the perceived motive of node j is related to the precision τ_j of the perceived prediction probability p_j as

$$\mathbb{V}(M_j) = \tau_j^{-1}. \quad (32)$$

3.2.4 Overall benevolence With the considerations of both reciprocity and motive, the expected overall benevolence perception of node j respect to node i is

$$\mathbb{E}(B_{i,j}) = \frac{\mathbb{V}^{-1}(R_{i,j})\mathbb{E}(R_{i,j}) + \mathbb{V}^{-1}(M_j)\mathbb{E}(M_j)}{\mathbb{V}^{-1}(R_{i,j}) + \mathbb{V}^{-1}(M_j)}, \quad (33)$$

according to Bayes' rule. The variance associated with the perception is

$$\mathbb{V}(B_{i,j}) = (\mathbb{V}^{-1}(R_{i,j}) + \mathbb{V}^{-1}(M_j))^{-1}. \quad (34)$$

Notice that $\mathbb{E}(B_{i,i}) = b_0$ and $\mathbb{V}(B_{i,i}) = 0$.

3.3 Integrity

Integrity is associated with the perceived characteristics of reliability, predictability, honesty, and consistency. Integrity is a relatively well studied topic in the context of cyber security. It is essential to protect the operation of CPS and the networks. The quantification of integrity needs to consider the risk of deception attacks and replay attacks. In deception attack, adversary or compromised nodes send false information such as incorrect

measurement, incorrect time of measurement, incorrect metadata (e.g. who measured the data), etc. to others. In replay attack, data transmitted between nodes are intercepted or delayed so that the decisions of the receiving nodes are maliciously manipulated.

Suppose that the prior belief of integrity for node j is $\mathbb{E}(I_j) = g_j$ with imprecision or variance $\mathbb{V}(I_j) = \omega_j^{-1}$. The likelihood that node j is free from deception attack and maintains its integrity can be quantified as the deviation between its state variable value and the average state variable value in its neighborhood Ω_j where the same quantity of interest is measured and detected, as

$$P(x_j|x_{i\in\Omega_j}) = g_j^S \propto \exp\left[-\frac{(x_j-\hat{x}^{(j)})^2}{2\sigma_x^2}\right], \tag{35}$$

where $\hat{x}^{(j)} = \frac{1}{|\Omega_j|}\sum_{i\in\Omega_j} x_i$ is the average prediction of the neighboring nodes with respect to node j, and σ_x^2 indicates the natural variation between sensing units as the random error.

Based on Bayes' rule, the perception of integrity about node j can be updated to

$$\mathbb{E}(I_j|x_{i\in\Omega}) = \frac{g_j\omega_j + g_j^S\sigma_x^{-2}}{\omega_j + \sigma_x^{-2}}, \tag{36}$$

when new information about the behaviors of nodes is obtained.

The likelihood function can also be formulated to incorporate the temporal factor. If the $x_j(t_k)$ denotes the predicted state value by node j at time t_k, the likelihood can be extended to capture the node's own consistency as

$$P\left(x_j(t_k)|x_j(t_{k-1},\ldots,t_0)\right) = g_j^T \propto \exp\left[-\frac{(x_j(t_k)-\bar{x}_j)^2}{2\sigma_x^2}\right] \tag{37}$$

where $\bar{x}_j = \frac{1}{k}\sum_{i=0}^{k-1} x_j(t_i)$ is the average value of previous predictions by node j at time stamps from t_0 to t_{k-1}. The perception of integrity can be similarly updated to

$$\mathbb{E}(I_j|x_{i\in\Omega}, x_j(t_{k-1},\ldots,t_0)) = \frac{g_j\omega_j + g_j^S\sigma_x^{-2} + g_j^T\sigma_x^{-2}}{\omega_j + 2\sigma_x^{-2}}. \tag{38}$$

4 Metrics Estimation in Networks

To demonstrate how the probabilities and trust metrics can be estimated from network traffic data, a ring network with 9 nodes, as shown in Fig. 4, is used to demonstrate the proposed trust metrics. The ring network is built in networks emulator ns-2 [38], which simulates detailed packet-level communication in networks [39]. Network protocols such as transmission control protocol (TCP), user datagram protocol (UDP), file transfer protocol (FTP), etc. are emulated. In this example, simplex data flow is used with single directional traffic, $0 \to 1 \to \cdots \to 8 \to 0$. Other settings of the networks include: network speed 10M bits per second for each connection, delay 2 ms, maximum queue size is 20 packets. In addition, the probability of packet drop for each

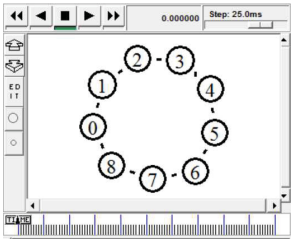


Figure 4: A ring network with 9 nodes

connection is 1% in the emulator. TCP is used to establish connection between each pair of data source and destination. FTP application is used to send data.

Some example statistics of communication for 60 seconds in the ring network are listed in Table 1. Data are generated as a result of sensing and prediction. The P-reliance probability is estimated as the ratio between data received by destination and data sent by source. Therefore, the P-reliance probabilities are $p_{01} = 1$, $p_{02} = 0.9996$, $p_{10} = 0.9773$, $p_{12} = 1$, and $p_{21} = 0.9701$, $p_{20} = 0.9811$. It is also assumed that sending more data indicates higher prediction probability. Therefore, the prediction probability for each source node is estimated as the ratio between the size of data it generates and a reference maximum possible value. Here the reference maximum value is set to be 28000. Therefore, the prediction probabilities of source nodes are $p_0 = 0.9655$, $p_1 = 0.6317$, and $p_2 = 0.1834$, as shown in Table 1. Note that nodes other than #0, #1, #2 are assumed to be simple relay nodes for communication without sensing and prediction capabilities. The Q-reliance probabilities are not considered in this example. With the prediction and P-reliance probabilities, the capability, influence, and ability of nodes can be calculated according to Eqs.(16-17), (20-21) and (22-23). It is assumed that the variance associated with each prediction or reliance probability is 0.01. The expected values of capability, influence, and overall ability for #0 are 0.9746, 0.9884, and 0.9847. Similarly, the ability metrics for #1 are 0.8673, 0.8697, and 0.9158. The ability metrics for #2 are 0.7277, 0.7115, and 0.8268. The deterministic and perceived reciprocity for each pair are calculated according to Eqs.(28) and (29) respectively, and the results are listed in Table 2.

5 Strategic Network Design

A strategic network for a CPS node is a trustable network or society that the node is willing to collaborate with. The design of a strategic network is to maximize the expected utility, where utilities U's as design criteria are chosen based on the trust metrics. In this section, two criteria are used to illustrate. In the first criterion, the utility function is defined as the node's reciprocity and benevolence. In the second criterion, the utility is individual's ability.

Table 1: Statistics of communication in the network in Fig. 4

Pair	packets sent	packets received	P-reliance prob.
#0 to #1	17220	17220	1.0
#0 to #2	9813	9809	0.9996
#1 to #0	3260	3186	0.9773
#1 to #2	14427	14427	1.0
#2 to #1	2074	2012	0.9701
#2 to #0	3061	3003	0.9811
Source	packets sent	Ref. maximum	Prediction prob.
#0	27033	28000	0.9655
#1	17687	28000	0.6317
#2	5153	28000	0.1834

Table 2: Reciprocity metrics for the nodes in Fig. 4

Pair	deterministic reciprocity	perceived reciprocity
#0 to #1	-0.3674	0.5099
#1 to #0	0.3677	0.6799
#0 to #2	-0.1343	0.5074
#2 to #0	0.1345	0.5236
#1 to #2	-0.3674	0.5132
#2 to #1	0.3677	0.7406

To exhaustively search and choose the optimum combination of n from a total of N nodes is an NP-hard problem and not feasible for large networks. A more efficient searching strategy is to use heuristic or greedy algorithms. Starting from the source node, greedy algorithms selectively add nodes sequentially if the objective function value increases. Here, a breadth-first search (BFS) greedy algorithm is developed to demonstrate the optimization process. Starting from the reference node, a subgraph is formed and updated iteratively by inserting a new node from the neighboring nodes of the current graph. For each iteration, if the value of utility function for the new subgraph is non-decreasing from the previous one, the new node is accepted. The greedy algorithm allows for quick formation of the strategic network, but obviously could potentially miss the true optimum solution. Other algorithms for combinatorial problems can also be applied.

5.1 Benevolence criteria

If the utility function is based on reciprocities, it can be defined as the weighted average reciprocity in the society with respect to the reference node. For instance, for node i, the utility based on deterministic reciprocity is defined as

$$U^{(i)} = \sum_{j \in V^{(i)}} w_j \bar{r}_j \tag{39}$$

where $\bar{r}_j = (1/n_j)\sum_{k \in V^{(i)}} r_{j,k}$ is the average reciprocity of node j among its n_j neighboring nodes in the society of node i. The average reciprocity of a node indicates how well other nodes treat it reciprocally. Determining the self-interest weights w_j's has an effect on how much emphasis on the reference node's benefit verses other nodes when forming strategic partnerships. For a 'selfish' approach, $w_i = 1$ and $w_j = 0 (\forall\, j \neq i)$ with respect to reference node i. For an 'altruistic' approach, $w_i = 0$ and the weights associated with other nodes are equal. Similarly, the utility based on average perceived reciprocity can be defined similarly with the deterministic reciprocity in Eq. (39) replaced by the probabilistic reciprocity perception.

To illustrate, a directed graph containing 40 nodes, shown in Fig. 5, is constructed, where the edge connections between nodes are randomly generated. The heavy tail at the end of an edge in the figure denotes an arrow, indicating an incoming vertex (e.g. the information flow direction from node 35 to node 36 is shown). The probability that there is an edge between two nodes is set to be 0.08. The prediction, P-, and Q-reliance probabilities are randomly generated from an uniform distribution between 0 and 1. Similarly, the variances associated with the prediction and reliance probabilities are randomly generated from a uniform distribution between 0 and 0.5.

With the utility function defined as the average deterministic reciprocity, the resulting optimum networks with selfish and altruistic weights are shown in Fig. 6. Furthermore, with the utility defined as the average probabilistic reciprocity perception, the optimum results are shown in Fig. 7, where the selfish case is the same as the deterministic one.

As a further generalization, the average benevolence perception is used as the utility, where the reciprocity in Eq. (39) is replaced by benevolence. The optimum networks in the previous example are shown in Fig. 8.

5.2 Ability criteria

The reference node's ability can be used as the optimization criterion. In addition to the prediction capability, ability also measures how influential a node is in a society. Therefore, the natural objective of a node to build a strategic network around itself is to maximize its influence within the network if its prediction capability is fixed.

The utility based on the k^{th}-order ability in Eq.(26) with respect to node i can be defined as

$$U^{(i)} = \mathbb{E}^{(k)}(A_j(\theta|+,-)) \tag{40}$$

The strategic network of node i can be obtained by finding the network where the ability of the reference node is maximized.

The optimization process is applied to the random graph model in Fig. 5. The optimum network with respect to node 0 using the first-order ability as utility is shown in Fig. 9, where the evolution of the utility during the search is also shown. Similarly,

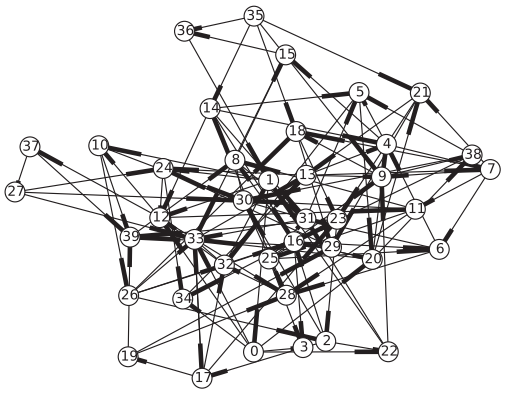
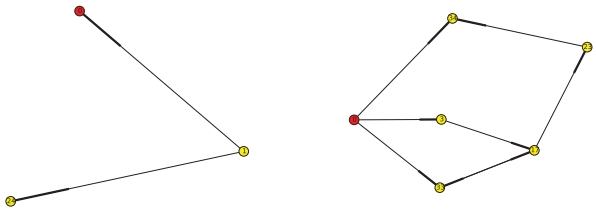


Figure 5: A random graph with 40 nodes



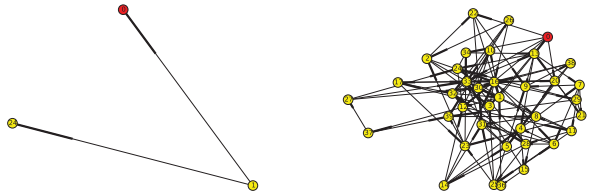
(a) $w_0 = 1$ (b) $w_0 = 0$

Figure 6: Trustworthy strategic network of Node 0 from Fig. 5 with deterministic reciprocity as utility.

when the second-order ability is used as utility, the results are shown in Fig. 10.

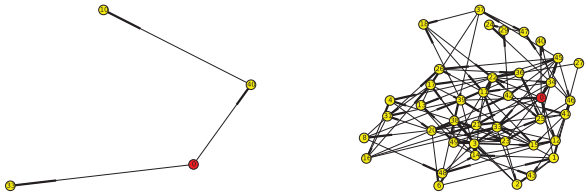
Higher-order abilities instead of the second-order one in Eq. (40) can be similarly used as the criterion in network optimization. When higher-order abilities are used, the influence of a node in the network gains more weights in calculating abilities, which is emphasized more in obtaining the optimum network.

Note that the integrity of nodes is not used in designing a node's strategic network. Because the integrity of an individual node is mostly independent from the topological relationship between those nodes. The network rarely has effects on how an individual node behaves or how it is compromised when attacked. The goal of the strategic network with respect to a reference node is building a trustable community which the reference node can rely on and work with. Nevertheless, if the integrity of networks instead of individual nodes is concerned and the goal is to maintain the integrity of the network, optimization in this case becomes straightforward and is to increase the size of the network as much as resources allow. Introducing redundancy can increase the reliability, resilience, and thus the integrity of the system. This can also be seen in the perception based integrity measure in Eq.(38), where the large variation among nodes, caused by individual compromised nodes, helps reduce the impact of the individual's swing and keeps the overall perception stable.



(a) $w_0 = 1$ (b) $w_0 = 0$

Figure 7: Trustworthy strategic network of Node 0 from Fig. 5 with probabilistic reciprocity as utility.



(a) $w_0 = 1$ (b) $w_0 = 0$

Figure 8: Trustworthy strategic network of Node 0 from Fig. 5 with general benevolence as utility.

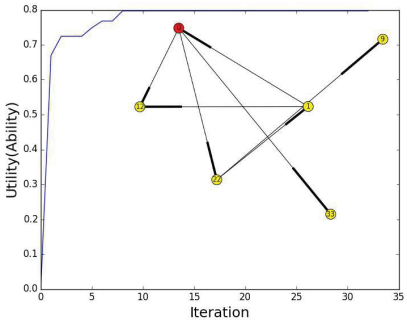


Figure 9: Utility evolution during search and the resulting trustworthy network of Node 0 from random graph in Fig. 5 where the first-order ability is applied as the utility for optimization.

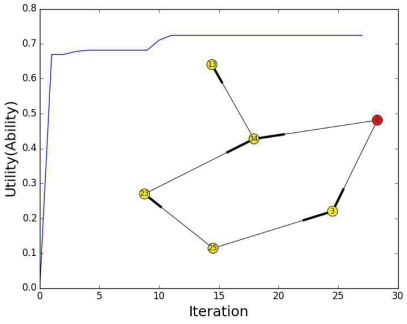


Figure 10: Utility evolution during search and the resulting trustworthy network of Node 0 from random graph in Fig. 5 where the second-order ability is applied as the utility for optimization.

6 Concluding Remarks

In this paper, a perception based trust framework is described in order to include human user and societal aspects in trust. The trustworthiness of CPS nodes in a networked environment is quantified by three independent metrics, including ability, benevolence, and integrity. Ability indicates how capable a CPS node is to provide accurate sensing, reasoning, and prediction, and how influential a node is in affecting other's decision making process. Benevolence measures the motivation of information sharing and how much reciprocity a node may receive from its neighbors during information and data exchange. Integrity shows the level of reliability, predictability and security of a node in the network.

The three quantitative metrics can be obtained objectively from the statistical data of performance as well as perceptual reputation, including prediction and reliance probability values. The perceptual models can also be applied when beliefs are elicited from experts as subjective probabilities. The calculation of trustworthiness metrics is all based on the Bayesian approach. The only assumption made in the model is the Gaussian distributions of perceptions.

The proposed modeling method can be regarded as a mesoscale model of networks, where detailed network communication protocols between nodes is not considered, nor detailed sensing and control mechanisms within each node. The mesoscale model needs to be compared with fine-grained bottom-up models in the future. In addition, multi-valued state variables can be considered in future work. Multi-objective optimization can be also applied when multiple criteria are used simultaneously.

Acknowledgment

This work is supported in part by National Science Foundation under grant CMMI-1663227.

REFERENCES

[1] Horváth, I., and Gerritsen, B. H., 2012. "Cyber-physical systems: Concepts, technologies and implementation principles". In Proceedings of The 9th International Symposium on Tools and Methods of Competitive Engineering (TMCE2012), pp. 19–36.

[2] Horváth, I., and Gerritsen, B. H., 2013. "Outlining nine major design challenges of open, decentralized, adaptive cyber-physical systems". In ASME 2013 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, American Society of Mechanical Engineers, p. V02BT02A001.

[3] Grimm, M., Anderl, R., and Wang, Y., 2014. "Conceptual approach for multi-disciplinary cyber physical systems design and engineering". In Proceedings of The 10th International Symposium on Tools and Methods of Competitive Engineering (TMCE2014), pp. 61–72.

[4] Wang, Y., 2016. "System resilience quantification for probabilistic design of internet-of-things architecture". In ASME 2016 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, ASME, p. V01BT02A011.

[5] Wang, Y., 2018. "Resilience quantification for probabilistic design of cyber-physical system networks". *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part B,* ***4***(3), p. 031006.

[6] Grabner-Kräuter, S., and Kaluscha, E. A., 2003. "Empirical research in on-line trust: a review and critical assessment". *International Journal of Human-Computer Studies,* ***58***(6), pp. 783–812.

[7] Keung, S. N. L. C., and Griffiths, N., 2010. *Trust and reputation*. Springer, London, pp. 189–224.

[8] Golbeck, J., et al., 2008. "Trust on the world wide web: a survey". *Foundations and Trends® in Web Science,* ***1***(2), pp. 131–197.

[9] Ruan, Y., and Durresi, A., 2016. "A survey of trust management systems for online social communities–trust modeling, trust inference and attacks". *Knowledge-Based Systems,* ***106***, pp. 150–163.

[10] Yu, B., and Singh, M., 2000. "A social mechanism of reputation management in electronic communities". pp. 154–165.

[11] Lee, S., Sherwood, R., and Bhattacharjee, B., 2003. "Cooperative peer groups in nice". In INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, Vol. 2, IEEE, pp. 1272–1282.

[12] O'Doherty, D., Jouili, S., and Van Roy, P., 2012. "Towards trust inference from bipartite social networks". In Proceedings of the 2nd ACM SIGMOD Workshop on Databases and Social Networks, ACM, pp. 13–18.

[13] Li, X., Zhou, F., and Du, J., 2013. "Ldts: A lightweight

and dependable trust system for clustered wireless sensor networks". *IEEE transactions on information forensics and security,* ***8***(6), pp. 924–935.

[14] Zhou, P., Jiang, S., Irissappane, A., Zhang, J., Zhou, J., and Teo, J. C. M., 2015. "Toward energy-efficient trust system through watchdog optimization for wsns". *IEEE Transactions on Information Forensics and Security,* ***10***(3), pp. 613–625.

[15] Chen, Z., Tian, L., and Lin, C., 2017. "Trust model of wireless sensor networks and its application in data fusion". *Sensors,* ***17***(4), p. 703.

[16] Reddy, V. B., Venkataraman, S., and Negi, A., 2017. "Communication and data trust for wireless sensor networks using d–s theory". *IEEE Sensors Journal,* ***17***(12), pp. 3921–3929.

[17] Barber, K. S., and Kim, J., 2001. "Belief revision process based on trust: Agents evaluating reputation of information sources". In Trust in Cyber-societies, R. Falcone, M. Singh, and Y.-H. Tan, eds., Vol. 2246, Springer, pp. 73–82.

[18] Yu, B., and Singh, M. P., 2002. "Distributed reputation management for electronic commerce". *Computational Intelligence,* ***18***(4), pp. 535–549.

[19] Patel, J., Teacy, W. L., Jennings, N. R., and Luck, M., 2005. "A probabilistic trust model for handling inaccurate reputation sources". In Trust Management, P. Herrmann, V. Issarny, and S. Shiu, eds., Springer, Springer, pp. 193–209.

[20] Wang, Y., Cahill, V., Gray, E., Harris, C., and Liao, L., 2006. "Bayesian network based trust management". In Autonomic and Trusted Computing, L. T. Yang, H. Jin, J. Ma, and T. Ungerer, eds., Springer, pp. 246–257.

[21] Kim, H., Lee, H., Kim, W., and Kim, Y., 2010. "A trust evaluation model for qos guarantee in cloud systems". *International Journal of Grid and Distributed Computing,* ***3***(1), pp. 1–10.

[22] Li, X., Ma, H., Zhou, F., and Gui, X., 2015. "Service operator-aware trust scheme for resource matchmaking across multiple clouds". *IEEE transactions on parallel and distributed systems,* ***26***(5), pp. 1419–1429.

[23] Kant, V., and Bharadwaj, K. K., 2013. "Fuzzy computational models of trust and distrust for enhanced recommendations". *International Journal of Intelligent Systems,* ***28***(4), pp. 332–365.

[24] Nafi, K. W., Kar, T. S., Hossain, M. A., and Hashem, M., 2013. "A fuzzy logic based certain trust model for e-commerce". In Informatics, Electronics & Vision (ICIEV), 2013 International Conference on, IEEE, pp. 1–6.

[25] Ashtiani, M., and Azgomi, M. A., 2016. "Trust modeling based on a combination of fuzzy analytic hierarchy process and fuzzy vikor". *Soft Computing,* ***20***(1), pp. 399–421.

[26] Chahal, R. K., and Singh, S., 2017. "Fuzzy rule-based expert system for determining trustworthiness of cloud service providers". *International Journal of Fuzzy Systems,* ***19***(2), pp. 338–354.

[27] Mayer, R. C., Davis, J. H., and Schoorman, F. D., 1995. "An integrative model of organizational trust". *Academy of management review,* ***20***(3), pp. 709–734.

[28] Colquitt, J. A., Scott, B. A., and Lepine, J. A., 2007. "Trust, trustworthiness, and trust propensity: A meta-analytic test of their unique relationships with risk taking and job performance". *Journal of Applied Psychology,* ***92***(4), pp. 909–927.

[29] Yang, M.-H., Lin, B., Chandlrees, N., and Chao, H.-Y., 2009. "The effect of perceived ethical performance of shopping websites on consumer trust". *Journal of computer information systems,* ***50***(1), pp. 15–24.

[30] Büttner, O. B., and Göritz, A. S., 2008. "Perceived trustworthiness of online shops". *Journal of Consumer Behaviour,* ***7***(1), pp. 35–50.

[31] Benamati, J., Serva, M. A., and Fuller, M. A., 2006. "Are trust and distrust distinct constructs? an empirical study of the effects of trust and distrust among online banking users". In System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on, Vol. 6, IEEE, pp. 121b–121b.

[32] Lauer, T. W., and Deng, X., 2007. "Building online trust through privacy practices". *International Journal of Information Security,* ***6***(5), p. 323.

[33] Chen, H., 2012. "The influence of perceived value and trust on online buying intention.". *Journal of Computers,* ***7***(7), pp. 1655–1662.

[34] Scherer, S., and Wimmer, M. A., 2014. "Conceptualising trust in e-participation contexts". In International Conference on Electronic Participation, Springer, pp. 64–77.

[35] Li, X., Hess, T. J., and Valacich, J. S., 2006. "Using attitude and social influence to develop an extended trust model for information systems". *ACM sigmis database,* ***37***(2-3), pp. 108–124.

[36] Fuller, M. A., Serva, M. A., Baroudi, J., et al., 2010. "Clarifying the integration of trust and tam in e-commerce environments: implications for systems design and management". *IEEE Transactions on Engineering Management,* ***57***(3), pp. 380–393.

[37] Wang, Y., 2018. "Trust quantification for networked cyber-physical systems". *IEEE Internet of Things Journal*.

[38] LBL, Xerox-PARC, UCB, and USC/ISI, 1995. "The network simulator ns-2". *https://www.isi.edu/nsnam/ns/*.

[39] Wang, Y., 2018. "Trustworthiness in designing cyber-physical systems". In Proceedings of The 12th International Symposium on Tools and Methods of Competitive Engineering (TMCE2018), pp. 1–12.