Towards Trust Analytics in Cyber Physical Systems of Industry 4.0

Marina Harlamova

Institute of Applied Computer Systems, Riga Technical University,
1 Kalku, Riga, LV-1658, Latvia
marina.harlamova@edu.rtu.lv

Abstract. In dynamic cyber physical systems such as Industry 4.0, ensuring secure and stable operating environment is a top priority. To support reliable communication in industrial network and prompt elimination of participants that express malicious behavior, a concept of trust is introduced for Industry 4.0 production facilities through a conceptual trust handling framework. The framework implies trust phases on node and network level in trust data gathering and trust data assessment phases. Constructs embedded in the framework support analytical approach to trust, allowing access to production data, revealing security issues in the system and suggesting areas for improvement by means of sensor data collection and processing, network traffic analysis, access control mechanisms, and other means.

Keywords: Trust Framework, Trust Analytics, Cyber Physical Systems, Industry 4.0.

1 Introduction

The emerging industrial revolution, known as Industry 4.0, is expected to embed latest technological advances, such as Industrial Internet of Things (IoT), cloud computing, predictive analytics, advanced robotics, artificial intelligence, and enhanced sensing units, into a single wireless factory network. The industrial environment involves both human and artificial participants and imposes human-human, artefact-artefact, and human-artefact relationships in the system. Given high degree of networking and communication, such a system requires advanced security and monitoring mechanisms [1-2]. In this paper we propose to support security analytics in Industry 4.0 environment by embedding trust framework into the Industry 4.0 environment. The concepts behind the solution are described in [3]; this paper extends the discussion by evaluating the framework from analytical perspective by introduction of trust phases. Each phase enables access to data that can be used for security analytics of operating industrial environment.

The paper is organized as follows. The related works regarding development of the trust handling framework are listed in Section 2. The notion of trust phases is introduced in the framework in Section 3. Analytical trust properties and functions ex-

pressed by the framework are discussed in Section 4. The approach to framework evaluation using relevant trust metrics is presented in Section 5. Brief conclusions and further research directions are given in Section 6.

2 Related Work

Trust has been a widely disputed study topic amongst researchers for decades. Albeit originating from area of social sciences, the concept of trust has been modified and integrated to other fields of study over years. Quantifiable trust is now embodied in various security and performance improvement solutions in computer and information systems, especially when it comes to highly autonomous distributed systems, where human intervention is unfeasible. Lately, there has been an increased interest in embedding trust in security solutions of Industry 4.0, e.g. using trust-based communication for performance enhancement [1] or efficient resource distribution [2] in Industrial IoT.

This paper continues the investigation of trust handling framework constructs proposed for Industry 4.0 and highlights aspects to be used for trust analytics. In [3], the trust concept, its interpretations in social sciences, IT and computer sciences, and ad-hoc distributed sensing systems were investigated to understand how trust relates to properties expressed by Industry 4.0 environment. A case study [4] of a smart production line installed on premises of Aalborg University was used to reveal Industry 4.0 features that are required by industry workers. It was determined that *data availability*, *centralized code base* and *wireless connectivity* are features that are expected by users in future CPS industrial networks. A conceptual framework for trust handling in such environment was constructed and is described in [5]. There, the trust handling solution was evaluated with regards to mentioned features, as well as standard security requirements and underlying network configuration challenges.

Combined research from prior work [3], [5] uncovered trust dimensions that are to be considered in Industry 4.0 wireless networks: *Data integrity*, *Cooperation*, *Credibility*, *Performance and process*, *Access control* and *Recommendation*. Fusion of human and artificial trust required two trust levels to be defined: network-level trust and node-level trust; preliminary analysis suggested two types of trust: initial trust and continuous trust. In the proposed trust framework, trust assessment per node, when a new element joins the network, was suggested through *Node initial trust module* construct. Trust evaluation is maintained in continuous trust constructs *Node continuous trust module* and *Network continuous trust module*. Trust functions that produce quantifiable trust evaluation were suggested. Collected local trust values are to be carried to *Node trust engine* and *Network trust engine*. Total node trust value and total network trust value are calculated as a final output to determine node's or network's trustworthiness. Total trust values can be integrated into system monitoring solutions (suggested *Alarm system module*) to ensure transparency and quality of services in the system.

3 Trust Phases

Only few attempts have been made at amalgamation of trust models and frameworks, even less so in industrial manufacturing area. Systems that share some properties of Industry 4.0 CPS networks, such as cloud services and wireless sensor networks, commonly use reputation-based methods to evaluate trust. Wireless sensor network reputation-based trust systems are often composed of the following blocks: data collection and sharing, trust calculation, decision making and dissemination [6]. Analytical framework for trust management for cloud services [7] is also structured similarly, having 3 layers of trust: the trust feedback sharing layer, the trust assessment layer, and the trust result distribution layer. Thus, to support trust analytics in Industry 4.0, similar structuring is used in this work by introducing trust phases. Trust handling phases for proposed Industry 4.0 trust handling framework are displayed in Figure 1; a significant difference between the proposed framework for Industry 4.0 wireless network and application areas of trust models in reviewed works is that in the proposed solution there is no trust distribution phase. Sharing collected feedback is highly important in distibuted ad-hoc mechanisms, such as distributed cloud services or wireless sensor networks. In case of smart production facilities, the envisioned network setup is strongly centralized. Therefore, instead of feedback distibution phase, trust storing phase is introduced. This phase is not explicitly seen in Figure 1; evaluation metrics cover the steps before and after storing trust: from Trust decision step to Trust awareness step.

Trust information is collected in the first phase: *Trust data gathering*. Next, in *Trust data assessment* phase node dimension-level trust scores are combined to result in a node total trust score. From network perspective, overall network trust level is also analysed in this phase. Lastly, in *Trust storing* phase (combined steps of trust decision and trust storage) evaluation of calculated trust scores is performed. In the next section, trust mechanisms of trust data gathering and assessment phases that support analytical operations in Industry 4.0 environment are described in detail.

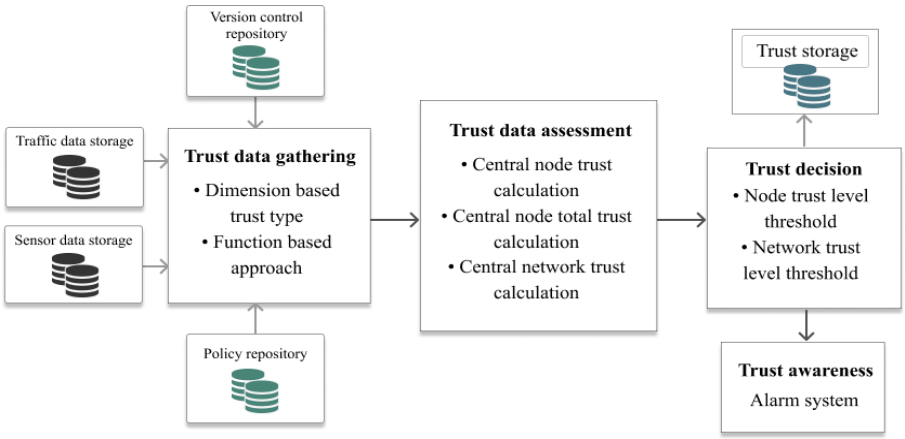

Fig. 1. Trust handling phases in proposed framework

4 Trust Gathering and Assessment: Analytical Properties and Functions

In this section the methods that enable trust analytics in each trust phase of the proposed framework are shown. In trust data gathering phase, each proposed trust dimension (i.e. Data integrity, Cooperation, Credibility, Performance and process, Access control and Recommendation) implies trust mechanisms that can be used in trust data assessment phase to determine trust level of node or network. Trust storing phase is not considered, since it does not reveal potential sources of data for security analysis. Trust determination mechanisms are described in Table 1 according to the node and network level trust dimensions and trust functions. The last column of the table shows the constructs of the trust handling framework described in [5].

Table 1. Analytical methods to evaluate various types of trust

Trust dimension	**Trust function**	**Trust mechanism (gathering phase)**	**Trust mechanism (assessment phase)**	**Supporting framework construct**
Node level				
Access control	Identification, Authentication, Authorization	User profile data registration	User credential processing	Node initial trust module
Data integrity	Sensor reading inspection	Sensor data collection and pre-processing	Sensor data processing and anomaly detection (ML tools)	Node continuous trust module
	Data packet inspection	Traffic data collection and pre-processing	Traffic data processing and anomaly detection (ML tools)	
Cooperation / Recommendation	Packets forwarded			Node continuous trust module/ Node trust engine
	Packet delivery ratio			
	Average end-to-end delay			
	Throughput			
	Data streams established			
	Timely data transmission			
Initial credibility / Continuous credibility	Vendor data validation	Vendor attribute data collection	Vendor data comparison against existing records	Node initial trust module/ Node continuous trust module
	Firmware validation	Firmware version collection	Firmware data comparison against existing records	
	Software validation	Software version collection	Software data comparison against existing records	

Trust dimension	Trust function	Trust mechanism (gathering phase)	Trust mechanism (assessment phase)	Supporting framework construct
Network level				
Performance and process	System availability	Statistical data collection	Statistical data processing (BI tools)	Network continuous trust module
	SLA fulfilment			
	Qualitative/ quantitative metrics			
	Traffic monitoring		Traffic data processing and anomaly detection (ML tools)	

5 Evaluation Using Relevant Trust Metrics

In this section, trust assessment metrics from similar trust models and frameworks are collected to validate the proposed framework. This approach contributes to previous evaluation of the conceptual framework provided in [5]. Discovered evaluation metrics from related works are applied to each trust phase and discussed further in the section; metric's level of relevance and importance is assessed; for relevant metrics, fulfilment methods are described and supporting framework components are listed.

5.1 Trust Data Gathering Phase

For trust data gathering phase evaluation metrics are collected in Table 2. Evaluation results are presented in Table 3. For each metric, the addressed problem and its evaluation possibilities in the trust handling framework [5] are discussed.

Table 2. Collected evaluation metrics for trust data gathering phase

Source	Scalability	Accuracy	Technique	Adaptability	Consistency	Confidentiality	Trust type consideration
Alzaid H. et al [6]			✓				✓
Janani, V. S. et al [8]		✓					
Noor, T. et al [7]						✓	
Palmer, G. et al [9]				✓			
Ren, Y. et al [10]	✓	✓		✓	✓		
Ye, Z. et al [11]			✓		✓		

Scalability. *Addressed problem:* Are proposed dimension functions able to operate if production factory network grows in size or scale? The issue of scalability is addressed due to dynamic nature of Industry 4.0 wireless networks. Large sets of elements can be added to a factory networks. It is crucial that the proposed framework remains functional as the network grows in complexity. From technical perspective, adequate storage units have to be selected for storage of large data amounts, as well as devices with large computational power are needed for statistical analysis of ever growing amount of collected sensor data. *Evaluation:* Conceptual framework is not limited to selection of trust dimension functions; functions are selected depending on industrial needs. The scalability aspect has to be considered when choosing which trust functions to implement, in particular, for recommendation and cooperation trust dimensions.

Accuracy. *Addressed problem:* Do defined trust functions provide input for rigorous, credible trust result? At data collection step, raw data, as well as calculated function results have to be as accurate as possible to provide correct input for total trust level calculation. *Evaluation:* Selected functions are crucial for trust accuracy – the more appropriate the trust function, the more believable the calculated trust result will be. Additional elements such as sensor data module and network traffic data module should be configured to ensure the highest possible quality of stored data, avoiding data losses and eliminating false reports that lead to incorrect trust evaluations.

Technique. *Addressed problem:* Are selected trust functions appropriate for particular setting or application? *Evaluation:* Since the conceptual framework does not suggest selection of particular functions, for continuous trust evaluation, this metric should be considered as the next step when implementation approach is selected. As for initial trust evaluation, there is the universal rule defined that elements that do not pass first two checks of *access control* and *credibility* are not allowed to join the network.

Adaptability. *Addressed problem:* Is it possible to reuse a functioning trust framework in different setting? Does the framework support a scenario of trust weighing, i.e. more important and determined trustworthy nodes are either able to have more weight in neighbour trust determination? In dynamic, complex network setting, it is not always reasonable to determine trust levels by the same rules for small nodes, such as newly added passive sensing elements, and large elements, such as module controller, that simultaneously has a larger impact in the system (has control capabilities) and also has been in the network for a while. *Evaluation:* The issue of adaptability is not pointed out in the proposed framework. Again, dimension trust calculating functions shall be aligned with element importance hierarchy in the network. Some trust dimensions, such as *access control* and *initial/continuous credibility*, are not affected by element significance, as the framework suggests that all newly joined elements are treated equally.

Consistency. *Addressed problem:* Does the framework enforce direct trust score routing to central computational elements? Generated trust scores shall always have consistent origin; it shall be possible to track the route and sender of the trust score. Trust scores are not compromised or modified while in transfer to central trust computing elements. *Evaluation:* The proposed framework covers this need by assuming

that calculated dimension-level trust values are carried directly to either central node trust or central network trust engine. No trust score routing is enabled. This aspect should be covered on technical implementation level.

Table 3. Framework evaluation: trust data gathering phase

Require-ment	**Relevance (low/ medium/ high)**	**Importance (low/ medium/ high)**	**Fulfilment meth-od**	**Supporting framework construct**
Scalability	low	high	N/A	N/A
Accuracy	high	high	Is implied by data integrity trust dimension	• Node continuous trust module
Technique	medium	high	Initial trust: ac-cess control and initial credibility dimensions	• Node initial trust module
Adaptability	low	medium	N/A	N/A
Consistency	high	medium	Trust is routed to central processing element	• Node initial trust module • Node continuous trust module • Network continu-ous trust module
Confidentiali-ty	medium	high	Is implied by access control trust dimension	• Node initial trust module
Trust type consideration	low	low	N/A	N/A

Confidentiality. *Addressed problem:* Are appropriate mechanisms enabled in the framework to ensure transferred data is confidential? The aspect of confidentiality covers the need to expose required information only to parties that request it and have sufficient privileges to use it. Certain information should remain available only for network participants that are involved in particular process. *Evaluation:* From technical realisation view, the usage of cryptographic techniques for data transfer in CPS network is mandatory to fulfil this network trust evaluation metric. By itself the conceptual framework offers access control mechanisms using functions of identification, authentication, and authorization. More granular role control is needed, if access to elements in the network has to be separated. Optionally, some element signatures can be anonymized during data transfer with ability to encode the sender only in the central trust engine element.

Trust type consideration. *Addressed problem:* Does the framework cover the scenario where certain trust dimension score has a higher weight than the others?

Evaluation: Depending on the framework application, different trust dimensions can be weighted differently, or even disabled if not needed. Proposed framework considers *access control* and *initial credibility* dimensions to be of higher priority. The type of trust sent from these trust modules is discrete. Hence, if an element does not pass access control check, it is excluded from the network. If it passes this check, but fails to have credible vendor/software/firmware properties; it is also excluded from the network. Else, in case a newly joined element passes the initial trust test, its further trust evaluation is continuous.

5.2 Trust Data Assessment Phase

Trust assessment is the second step of trust handling in proposed framework. Metrics are summarized in Table 4. Evaluation results are presented in Table 5.

Table 4. Collected evaluation metrics for trust assessment phase

Source	Scalability	Mobility	Efficiency	Technique	Adaptability	Security	Integration
Alzaid H. et al [6]	✓			✓			
Janani, V. S. et al [8]		✓				✓	
Noor, T. et al [7]	✓			✓	✓	✓	✓
Palmer, G. et al [9]					✓		
Ren, Y. et al [10]	✓		✓		✓		
Ye, Z. et al [11]				✓			

Scalability. *Addressed problem:* Is trust assessment calculation possible for a growing production factory network? Scalability is raised as an evaluation metric for phase of trust data collection and this issue extends also to trust calculation phase. In addition to selecting appropriate trust functions for a network that is about to expand, central trust calculating elements must have sufficient computing power to support large-scale trust calculations. Trust assessment must happen with low latency and on-demand, regardless of network size. *Evaluation:* This criterion is out of the scope of the conceptual framework. If the network is expected to grow, trust calculation performance tests have to be done in different dimensions before deploying the system.

Mobility. *Addressed problem:* How will trust assessment results change if an assessed node is moved elsewhere in the network? *Evaluation:* Central trust engines that do local and total trust calculation per trust dimension do not consider the location of the node in the proposed framework. For initial trust module, with dimensions of *access control* and *initial credibility*, this evaluation metric is not applicable. Trust values from this module are not changed if the element is moved. Location-dependent dimensions, such as *recommendation* and *cooperation*, however, are based on neigh-

bour node trust input. Methodology for trust assessment of these dimensions is not offered by the framework.

Efficiency. *Addressed problem:* How efficient are trust communication and calculation costs in the framework? *Evaluation:* In proposed framework trust computation is centralized. Node dimension-level trust and node total trust is calculated centrally. In closed factory environment with constant power supply it is a logical solution to avoid overhead, as opposed to wireless sensor networks, where calculation is local. As for trust communication from trust engines, enabling high interactivity in the network contributes to complexity of the system. The framework offers common trust communication and trust storage points after calculation is done, such as alarm system module and trust storage unit.

Technique. *Addressed problem:* Are selected trust calculation methods appropriate for particular setting or application? *Evaluation:* Proposed framework does not suggest selection of particular statistical or mathematical methods for trust derivation. Techniques such as trust rating, weight assignment, probabilistic functions, as well as Bayesian and neural network principles and Fuzzy logic can be used, for instance, for calculation of *recommendation* or *cooperation* dimensions. The same applies to total node trust function calculation.

Table 5. Framework evaluation: trust data assessment phase.

Requirement	**Relevance (low/ medium/ high)**	**Importance (low/ medium/ high)**	**Fulfilment method**	**Supporting framework construct**
Scalability	low	high	N/A	N/A
Mobility	medium	high	*[trust score is affected by this factor]*	N/A
Efficiency	high	high	• Centralized trust processing • Centralized trust storing • Anomaly reporting	• Node trust engine • Network trust engine • Alarm system module • Trust storage
Technique	low	high	N/A	N/A
Adaptability	low	low	N/A	N/A
Security	medium	high	Is implied by access control, performance and process trust dimension	• Node initial trust module • Network continuous trust module • Network trust engine
Integration	high	medium	Total trust is multidimensional	• Node trust engine • Network trust engine

Adaptability. *Addressed problem:* Is it possible to reuse the trust assessment mechanism in other settings? Does the framework support element-specific trust thresholds? *Evaluation:* This metric is not fulfilled by proposed framework. In the framework, all elements in the network are treated equally regardless of their role in the network.

Security. *Addressed problem:* How well is central assessment element fortified? In networks with high degree of centralization, gaining access to central control element can result in complete network shutdown. Trust scores are stored centrally. Trust function modification should be available only to eligible network administrators. *Evaluation:* The framework is aligned with network security requirements. It suggests security dimensions of access control, data integrity and availability. Consideration of these requirements in initial and continuous trust modules, as well as using secure communication channels, protect data that is handed to central trust processing engines. Network should be protected from external world using firewalls to avoid unauthorized access.

Integration. *Addressed problem:* Is trust handled as a multidimensional value? Combining several trust dimensions is likely to increase the accuracy of total trust score. *Evaluation:* Integration metric is fulfilled in the framework by offering six different approaches to measure node-level trust. Moreover, a higher abstraction level trust value for the network, that combines node trust levels to form a network reliability and security overview, is proposed.

5.3 Trust Storing Phase

In this section, for trust storing phase, cloud service trust model evaluation metrics [7] are used. Evaluation is summarized in Table 6.

Response time. *Addressed problem:* How fast can trust scores be retrieved from storage? Trust scores have to be retrieved timely in order to provide most accurate data to trust monitors of the network, as well as use newest scores for total and network trust calculations. *Evaluation:* This metric is not directly observed in the framework. Response time measurement for specific storage methods has to be performed.

Redundancy. *Addressed problem:* How high is the redundancy degree in the proposed framework? Unnecessary trust duplication processes should be eliminated in the network to avoid scalability and processing challenges, for instance, when trust calculation is requested several times on the same node from different requesters. Inefficient storage of trust and feedback values cause waste of storage resources, affecting the overall performance of the system. *Evaluation:* Detailed process analysis is required to detect and eliminate duplication processes and optimize trust data storage. The proposed framework suggests the use of one common trust storage unit for node and network trust values. There are separate storage units for collected sensor data, collected network traffic, a separate policy repository and a separate version control repository.

Security. *Addressed problem:* How well are trust storage elements fortified? Similarly as for trust assessment phase, securing trust storage unit is crucial to ensure trust data integrity and provide data for trust calculation at any given moment. *Evaluation:*

Proposed framework does offer direct mechanisms of securing storage units. For covering this metric, mechanisms such as secure communication protocols, firewalls on endpoints, and service audits are required.

Table 6. Framework evaluation: trust storing phase

Requirement	Relevance (low/ medium/ high)	Importance (low/ medium/ high)	Fulfilment method	Supporting framework construct
Response time	low	low	N/A	N/A
Redundancy	medium	medium	• Centralized trust storing	• Policy repository • Version control repository • Trust storage
Security	medium	high	• Centralized trust processing • Centralized trust storing • Anomaly reporting	• Node/network trust engine • Alarm system module • Trust storage

6 Conclusions

The paper describes how components of a conceptual trust handling framework for cyber physical system networks of Industry 4.0 [5] support trust analytics in an industrial setting. Trust handling in the framework is organized in *trust data gathering*, *trust data assessment* and *trust storing* phases. *Trust data gathering* phase deals with data collection from different sources for further trust level calculation in *trust data assessment* phase. Analytical trust mechanisms and framework constructs that support the mechanisms are described on node and network level in both phases. On a node level, in *trust data gathering* and *trust data assessment* phases, user profile data, exchanged sensor data and network traffic data (using machine learning tools), element vendor-embedded data, firmware and software data are collected as input for analytical operations and are processed. As for network level, access to overall network statistical data can be enabled in trust handling framework using both machine learning tools (anomaly detection) and business intelligence tools (reporting).

The work is concluded with continued evaluation of the proposed framework. This paper focuses on evaluation using metrics from related works. Each described analytical trust phase is validated against relevant metrics. Additionally, metric level of relevance and level of importance is determined to demonstrate proposed framework's level of contribution to the addressed trust problems. It is concluded that, for three defined trust phases of the proposed framework, important metrics of efficiency,

accuracy, technique, confidentiality, mobility and security are fully covered or partly supported by the proposed trust solution. A necessary remark is that current evaluation is not exhaustive; many metrics cannot be measured in conceptual trust solution until trust functions and calculation methodologies are selected.

It is a matter of further research to continue analysis of constructs in proposed trust framework. Separate trust function evaluation could prove to be beneficial for determining which analytical methods of trust are more relevant in a specific Industry 4.0 production factory setup.

Acknowledgement: this research was partly done within the Erasmus+ Strategic Partnership "Improving Employability through Internationalisation and Collaboration" (EPIC) project, with the support of the Erasmus+ programme of the European Union.

References

1. Zhu, C., Rodrigues, J. J. P. C., Leung, V. C. M., Shu, L., Yang, L. T.: Trust-Based Communication for the Industrial Internet of Things. IEEE Communications Magazine 56(2), 16-22 (2018).
2. Jeong, S., Na, W., Kim, J., Cho, S.: Internet of Things for Smart Manufacturing System: Trust Issues in Resource Allocation. IEEE Internet of Things Journal (Early Access).
3. Harlamova, M., Kirikova, M.: Towards the Trust Model for Industry 4.0. In: 13th International Baltic Conference, DB&IS 2018, Lupeikiene, A., Vasilecas, O., Dzemyda, G. (eds.), Springer International Publishing (2018).
4. Manufacturing Academy of Denmark. (2018). MADE casekatalog. Retrieved February 23, 2018, from http://www.made.dk/media/1720/made-casekatalog-2016-one-page.pdf
5. Harlamova, M., Kirikova, M.: Trust Handling Framework for Networks in Cyber Physical Systems of Industry 4.0. In: Perspectives in Business Informatics Research 17th International Conference, BIR 2018, Stockholm, Sweden, September 24-26, 2018, Proceedings, Zdravkovic, J., Grabis, J., Nurcan, S., Stirna, J. (Eds.), Springer (2018).
6. Alzaid, H., Alfaraj, M., Ries, S., Jøsang, A., Albabtain, M., Abuhaimed, A.: Reputation-Based Trust Systems for Wireless Sensor Networks: A Comprehensive Review. In: Fernández-Gago C., Martinelli, F., Pearson S., Agudo I. (eds) Trust Management VII. IFIPTM 2013. IFIP Advances in Information and Communication Technology, vol 401. Springer, Berlin, Heidelberg (2013).
7. Noor, T., Sheng, Q., & Bouguettaya, A.: Trust Management in Cloud Services. 1st edn. Springer International Publishing, Switzerland (2014).
8. Janani, V. S., Manikandan, M. S.: Efficient trust management with Bayesian-Evidence theorem to secure public key infrastructure-based mobile ad hoc networks. EURASIP Journal on Wireless Communications and Networking (2018).
9. Palmer, G., Selwyn, A., Zwillinger, D.: The "Trust V": Building and Measuring Trust in Autonomous Systems. In R. Mittu, D. Sofge, A. Wagner, & W. F. Lawless, Robust intelligence and trust in autonomous systems , pp. 55-78. Springer US (2016).
10. Ren, Y., Zadorozhny, V., Oleshchuk, V., Li, F.: A Novel Approach to Trust Management in Unattended Wireless Sensor Networks. IEEE Transactions on Mobile Computing 13(7), 1409–1423 (2014).
11. Ye, Z., Wen, T., Liu, Z., Song, X., Fu, C.: An Efficient Dynamic Trust Evaluation Model for Wireless Sensor Networks, Journal of Sensors, 1–16 (2017).