Survey of Trust Management on Mission-oriented Internet of Things

Youna Jung*

Computer and Information Sciences,
Virginia Military Institute
jungy@vmi.edu

Noah Goldsmith

Computer and Information Sciences,
Virginia Military Institute
goldsmithnk22@mail.vmi.edu

John Barker

Computer and Information Sciences,
Virginia Military Institute
barkerjc23@mail.vmi.edu

ABSTRACT

The Internet of Things (IoT) enables us to use diverse sensing data and control IoT devices, sometimes, networks remotely. This technology makes our lives easier and more comfortable. However, the services currently provided by IoT systems are limited within pre-defined sets of devices and it hinders the development of large-scale and complicated IoT services that could be provided through dynamic collaboration between IoT devices across networks. To realize the mission-oriented IoT (MIoT) systems, we must address the security issues of the MIoT systems. Among various security issues, in this paper, we focus on trust management on MIoT. We analyze existing work on trust management to see if they are suitable for the MIoT systems. Then, we identify potential issues and discuss challenges for the trust management on MIoT.

CCS CONCEPTS

• **Security and privacy** → Formal methods and theory of security; Trust frameworks.

ACM Reference Format:

Youna Jung, Noah Goldsmith, and John Barker. 2021. Survey of Trust Management on Mission-oriented Internet of Things. In *2021 3rd International Conference on Advanced Information Science and System (AISS 2021)* (AISS 2021), November 26–28, 2021, Sanya, China. ACM, New York, NY, USA, 5 pages. <https://doi.org/10.1145/3503047.3503076>

1 INTRODUCTION

The Internet of Things (IoT) is no longer a new technology. Currently, we live with more than 26.66 billion IoT devices scattered around the world [1] and a way to integrate heterogeneous IoT devices to provide complicated services in real time becomes one of the important topics. In general, IoT devices provide simple services with limited memory spaces and capabilities. To offer complex services, it is thus required for IoT devices to communicate and collaborate with each other. Among three types of group efforts including Coordination, Cooperation, and Collaboration, a best

strategy needs to be selected depending on the type of a service [2]. Regardless of its type, each group has a common goal among members. If an IoT device is involved in a group work to achieve a common goal, we define it as a Mission-oriented IoT (MIoT) device. For successful collaboration between MIoT devices, we must address two major issues, interoperability between devices and security. First, IoT devices have different communication protocols and diverse service levels from the sensory level to the cloud-based integrated service. To integrate heterogeneous IoT devices, we need a standardized way to define and implement the behavior of IoT devices across heterogeneous IoT platforms and application domains. The Web of Things (WoT), a global standard published by the World Wide Web Consortium (W3C), addresses this interoperability issue. An application of WoT into the disaster response domain is presented in [3]. Second, security must be guaranteed for IoT devices to join a group, share data, and perform actions to achieve a goal. These days many IoT devices are used in our everyday life and dealing with private and sensitive data that must be protected. In general, the weakest device that does not have enough resources to run security protocols or physical security easily becomes a target. If one device in an IoT network is compromised then an entire network becomes vulnerable as well. Therefore, it is critical to protect IoT devices and networks during collaboration not to reveal private and professional data. There are many security topics including authentication, access control, cryptography, intrusion detection, privacy, and trust management. Among these topics, we focus on trust management on collaborative IoT in this paper.

Trust is an important aspect. Towards secure and effective collaboration between MIoT devices, trust between members in a group must be established beforehand. To do so, it is important to select a MIoT device with a high reputation as a member of a group. To build a good reputation on MIoT, an IoT device must have a safe and sound security mechanism and reasonable collaboration history that shows how well the device contributes to achieve goals in groups. Establishing and maintaining trust between things could be a key to success in MIoT. There are existing works that address trust management on the Internet of Things. However, only a few works consider mission-oriented collaboration between things and trust measurements considering collaborative behaviors of things. To guide researchers who are interested in this topic, in this paper, we explore existing trust management on typical IoT and mission-oriented IoT and analyze the limitations and challenges. The rest of the paper is organized as follows. In Section 2, we introduce existing work on trust management on IoT networks and devices and then mission-oriented trust management on IoT. In Section 3, we discuss directions of future research and then conclude in Section 4.

*Corresponding Author: Youna Jung, Associate Professor in the Department of Computer and Information Sciences at Virginia Military Institute. Email: jungy@vmi.edu, Telephone: +1-540-464-7498.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from [permissions@acm.org](https://permissions.acm.org).

AISS 2021, November 26–28, 2021, Sanya, China

© 2021 Association for Computing Machinery.

ACM ISBN 978-1-4503-8586-2/21/11...\$15.00

<https://doi.org/10.1145/3503047.3503076>

2 TRUST MANAGEMENT ON IOT

As more IoT devices become available for personal and commercial use, the attack surface of IoT devices and networks is getting larger. Various IoT devices are spread out everywhere and all are connected to each other and other devices. If private data or confidential information related to companies' operations are captured by IoT devices and shared with unauthorized parties, it will bring a serious security crisis [4][5]. To avoid undesirable situations, we must employ proper mechanisms for data security and network security so that we can assure the confidentiality and integrity of data and information shared in IoT networks. On the other hand, we also need to build and maintain a trust management system among IoT devices who interact and share data with each other to mitigate security risks [6][7]. This solution would need to be lightweight, compact, and available in multiple different code bases in order to accommodate the vast amount of different IoT devices.

Two major components in a trust management system are Trust and Reputation that refer to the relationship between interacting Things. An IoT device's trust and reputation could be measured by others as expectation of competence and willingness to perform a given task. These kinds of metrics would allow for multiple mission oriented IoT devices that are connected by using their reputation [8]. Typically, trust management is effective in a system with highly interactive and heterogeneous devices working on the same goal [9][10]. A MIoT system is a good application domain of a trust management system for IoT. This is because a MIoT device requires that it is connected via trust to other devices. Lack of effective trust management on an MIoT may hinder the growth of the system in future [11][12] and or hinder its ability to effectively execute its mission. To help researchers who need trust management on MIoT systems, in this section, we introduce the existing definition of trust and a variety of methods for trust management for IoT devices and networks [10][11][12][13][14]. Then, we explore trust management considering mission-oriented behaviors of IoT devices. To do this, we will need to find effective measurement techniques to accurately measure the trust relationship between multiple IoT devices [7].

2.1 Trust on IoT Networks

Trust relationship could be built between IoT devices connected over decentralized networks, wired or wireless [5]. There are existing works on how to define trust on IoT networks (Trust Model) and how trust values could be utilized to make a decision whether to send particular types of data over a network or not [15]. Airehrour et. al. [15] define Trust in an IoT network as a reference to the confidence, belief and expectation about the reliability, integrity, security, dependability and character of an IoT node while defining Reputation with peer evaluations by other nodes nearby as a quantifiable limit of the observable experience one node has with its neighbors, either in direct or indirect manner. Zheng Yan et. al [8] defined Trust as a collection of 1 properties including Reputation, a history of activities to be considered before allowing a trust relationship between Things.

Establishing trust with an untrustworthy neighbor could significantly lower the efficiency and usability of entire IoT networks and place systems in an unsafe state. Therefore, many factors must be

thoroughly considered to form a trust relationship between neighboring IoT nodes. After forming a trust relationship, IoT nodes need to constantly assess the trustworthiness of peers in order to ensure that their interaction and collaboration are protected. Towards this goal, SecTrust [15], a secure trust routing framework for IoT, was proposed in 2016. The proposed system provides evaluations of neighboring nodes with recommendations and indirect trust values to help IoT nodes make decisions on trust relationships with other nodes. IoT nodes recommended by SecTrust are regarded as trustworthy nodes and able to interact with peer nodes successfully. In [16], IoT networks are used to build context-aware, edge diversity, and virtualized networks with IoT devices. This virtualized IoT network employs two major components, Context Manager and Trust Manager, to form and maintain trust relationships. The Context Manager collects diverse contexts including device, user, service and network contexts and the Trust manager builds trust between devices based on the context provided by the Context Manager. By doing so, we can create context-based virtualized networks that support context-aware, edge diversity, and virtualized networks with trustworthy IoT devices without concerns of insecure operations in networks. Guo et. al [11] proposes a reputation-based trust evaluation method in mesh networks. In a mesh network, an IoT device is connected to every other IoT device on the mesh network. To build this extreme interconnectedness among all nodes, each node in a mesh network must be evaluated based on their Reputation in order to evaluate Trust between each other. The ways to form Reputation for a node could vary depending on application domains such as social science/E-commerce, distributed/P2P systems, ad-hoc networks, or sensor Networks. For an E-commerce website, reputation could come from translation history and reviews of orders placed. Whereas, a P2P system could form a reputation based on the history of transactions that shows its capability to configure and connect many devices on the network. Ad-hoc and sensor networks could create reputations based on a record of previous interactions with diverse devices. In case that a device is new and does not have an interaction record, a reputation could be configured with a secret key. The domain-specific reputation-based trust management system enables IoT devices on a network to minimize information required to build and maintain trust relationships between devices.

As many heterogeneous IoT devices are connected through networks while sharing resources, there have been issues and conflicts. Salimitari et. al [17] identified two major issues on IoT networks as follows. First, the IoT devices may illegitimately draw additional benefits or [18] mislead a central authority from reaching a fair decision to secure more resources to complete their tasks. The trustworthiness of IoT devices that can be decided by the hubs could address this potential issue. The network hubs can calculate Things' Trust based on two pieces of evidence, 1) the reliability of the data they are collecting from devices and 2) feedback from peers. With evidence, an anomaly system evaluates whether the data provided by Things satisfies the system. If satisfied, give a 1 (True), otherwise, a 0 (False). Due to the heterogeneity of IoT devices, anomaly systems are sometimes not able to make a decision. In this case, the system gives a Thing Undecided. Based on the Trust values measured by anomaly systems, IoT devices can select peers to collaborate without security concerns. Another issue is that

different risk thresholds are required for different Things. For some IoT devices dealing with sensitive data must allow zero or lower tolerance than IoT devices on a personal network such as home appliances could allow for more risk-tolerance. To support secure IoT networks, we must have suitable trust management systems considering two issues described above. Unfortunately, there is no concrete solution to those issues yet.

2.2 Trust on IoT Devices

As the number of IoT devices used in our everyday life has increased explosively in recent years, there has been an urgent need for effective trust management systems for IoT devices. The heterogeneity of IoT devices and decentralized diverse IoT platforms makes the trust management on IoT devices much more complicated. Yet, the building and managing of trust among IoT devices across different IoT operating platforms is the key to success of IoT systems [9]. IoT systems therefore must have an effective method. To address this issue, we need to first define what trust is in IoT devices. In 2000, Grandison and Sloman [19] defined five types of Trust that we need to consider as below.

- Resource Access Trust - A device trusts another device to use the resources that it owns or controls. The type of resources could vary such as system application, software, or service that the device can control and/or manipulate.
- Service Provision Trust - A device trusts another to provide a service that the peer device does not have access to but needs for its operation.
- Certified Trust - A third party issues a certificate that shows that a device is trustworthy according to a set of criteria for a field that the device applies.
- Delegation Trust - A device allows another to make decisions on behalf of itself regarding the Resource Access Trust and/or the Service Provision Trust relationships.
- Infrastructure Trust - A device trusts the entire infrastructure including workstations, network components, local servers, and any services or security measures.

To measure an IoT device's trust effectively, we may indeed need to consider these diverse types of Trust indeed. Yuan and Li [20] proposed a trust calculation mechanism based on multi-source feedback information fusion for edge devices. They adopt a feedback information fusion algorithm developed using the objective information entropy theory which enables them to overcome the limitations of traditional trust schemes by assigning different weights to measuring factors. The proposed mechanism is developed for edge devices but it could be easily applied to IoT devices. To evaluate a device's Global Trust Degree (GTD), the mechanism uses three types of Trust: 1) Direct Trust calculated based on records of direct interaction between devices, 2) Peer-originated Trust calculated based on feedback from other edge devices, and 3) Broker-originated Trust provided by a variety of service brokers [20]. The feedback-based trust could be utilized to create a trust relationship between IoT devices even though not all devices share an edge based relationship.

In addition, a trust of IoT devices needs to be evaluated using multidimensional decision-making factors [20]. In general, trust in IoT is referred to as a competence in providing required service of

a device. Thus, it is a dynamic and complex concept. In case that an IoT system utilizes feedback-based trust, a single factor is especially not sufficient. The feedback-based trust requires IoT devices to work in conjunction with each other and share trust-relationships with them in order to maintain a certain level of trust during interaction. If the level of trust between them is dropped down and not met for interaction between them, IoT devices need to stop interactions for the safety of devices and in turn the entire IoT system. However, an IoT device that is not able to communicate with others easily becomes useless so each device having low trust values must be fixed. A way to identify and remedy a compromised device is one of the critical challenges.

2.3 Mission-Oriented Trust Management on IoT

To solve large-scale and/or highly complicated problems, collaborations among IoT devices could be one of the effective solutions. An example of application domain of the mission-oriented collaborative IoT systems is military systems. Inomoto et. al [21] proposed an IoT-based hierarchical system supporting three features: 1) Shared sensing infrastructure, 2) Dynamic sensing configuration, and 3) Heterogeneous IoT devices. The proposed system consists of accommodating diverse types of IoT devices that can perform system configurations dynamically while sharing their sensing data between other devices. In this system, individual IoT sensing devices are represented as the Soldiers. Each IoT device has a mission to be complete and they are often involved in a group to complete a large-scale mission. Note that the mission assigned to an IoT device could be changed according to a situation. To cope with such dynamically changing missions, the system provides an update of running missions in real time. Every IoT device is set up as a hierarchy related to the military analogy and must follow an instruction received from a Leader that represents an edge device controlling the device or a group the device belongs. The root of the hierarchy is a Commander, which is a regional server that manages the entire mission. This work shows us how the mission-oriented IoT system could be used in many areas. We can easily adopt this system to any application domains having a hierarchy and mission-oriented operations. Unlike traditional IoT systems, however, the MIoT system requires more maintenance on IoT devices and a system itself to coordinate communication and collaboration between soldiers, leaders, and a commander. It may undercut the strength of IoT that does not typically require maintenance. Another issue is trust management on MIoT systems. With heterogeneity of IoT sensing devices and diverse types of data, the problem of trust management is getting more complicated and requires more resources, and cost to analyze trust decision factors and calculate trust and reputation based on changing data.

To recruit IoT devices that are capable of tasks required to achieve a goal and support collaboration between them, security must be guaranteed. A trust management system can play a vital role in ensuring the security of the MIoT systems by measuring trust of IoT devices and networks, creating trust relationships among devices and/or between devices and networks, and maintaining trust relationships based on up-to-date data. Currently, there are several works that address trust management on IoT, especially focusing

on a way to evaluate them using multi-dimensional sources and revoke trust in certain situations. However, most of the work targets generic-purpose IoT systems and does not consider Trust and Reputation from the perspective of collaboration and goal achievement. In some cases, trust relationships in IoT are managed by operating systems [6]. However, MIIoT systems that are built with heterogeneous devices are usually associated with diverse hardware devices and operating systems. In addition, handling of trust could vary for each individual device. Therefore, existing work using operating systems to manage IoT trust is not suitable for highly diverse IoT systems. Some IoT systems use credentials issued by a domain controller to create a trust relationship and then re-establish the trust between an IoT node and the domain controller [22]. However, this approach may cause another security issue, the single point of failure (SPOF). If a node that has received a credential is compromised, the node could be used to access the domain controller. To limit the use of trust established, Temporary Trust is proposed [11]. A temporary trust could be created through a web browser, a shared computer, or a small IoT device. For an IoT device to access some resources, it must have a credential issued by an app or a web browser and then build a temporary trust that lasts for a short-term period only [19]. With the temporary trust, we can reduce the occurrence of a single point of failure. In addition, it might be a good idea for a MIIoT system to use temporary trust that lasts for the period of collaboration only between devices. For the IoT devices that are not able to use credentials due to their limited capacity, the Web of Trust that allows IoT devices to build a chain of trust [23]. In the web of trust systems, each device receives a list of trustworthy devices in a chain periodically or whenever a change is made. Each device has its own copy of the list. Once an IoT device is compromised, it is removed from the list and then not able to interact with others anymore.

3 DISCUSSION

As addressed above, only a few works have addressed trust management for collaboration although the trust management on the mission-oriented IoT (MIIoT) systems is critical. To accelerate research on this topic, we discuss issues and challenges to be addressed in this section.

- Decentralized trust management - In general, MIIoT systems are composed of diverse IoT devices having different levels of services and capacity. Often, a device has its own trust handling method. A device cooperates with others only if it shares a common goal with them. Otherwise, it performs its own task as usual. Therefore, a centralized and tightly coupled management may not be suitable for a highly diverse system. However, at the same time, it is required to have a group leader that collects data, calculates trust, and maintains trust relationships between IoT devices in a group. A leader could be an edge device, a network router, or a domain server. It is challenging to provide an organized way to manage trust among different devices while guaranteeing devices' autonomy. As a first step toward this goal, the feedback-based trust model [20] and the blockchain-based decentralized management [22] could be a stepping-stone.

- Prevention from the single point of failure - In the MIIoT system, security failure on an IoT device could ruin the entire collaboration in a group. In a decentralized management system allowing each device to have its own trust handling methods, the SPOF problem could be worse. If a single node is compromised, then it affects its group, in turn, and the entire system and network. Therefore, it is critical to have an effective method to identify a compromised device or node and isolate it in a timely manner in order to prevent the compromised device from accessing others.
- Mission-oriented trust evaluation - To increase the success rate of collaboration, a group must be organized with the proper devices that are trustworthy and capable of providing necessary resources and services required to achieve its mission. However, most existing trust management systems do not consider the cooperability of the IoT devices. An IoT device providing an excellent service to its customers may not be cooperative in a group. On the other hand, a device is good at a certain type of collaboration but in other types of group work. Therefore, a mission-oriented system must consider how effectively a device has contributed to groups' missions and what roles the device has taken in groups. The cooperability must be used to build a chain of trust as well.
- Real-time maintenance of data related to IoT devices and networks - Decision on trust relationships and device selections for a group heavily rely on data collected from IoT and edge devices. If data is outdated or incorrect, the group's collaboration could not be successful. Therefore, it is critical for the MIIoT systems to have a method to collect data from heterogeneous devices, interpret them correctly, and share those data with authorized devices only. In case of feedback data on cooperability of IoT devices, a system must decide which devices are needed to provide feedback on cooperability of others. If an evaluator providing feedback was involved in a collaboration that is similar to current group work, then we could give more weight to feedback from the evaluator. However, the details on how to find the best evaluators and how to weigh their feedback are still unsolved.

4 CONCLUSION

We are living in a world full of IoT devices deployed at both home and work. Currently, we use individual IoT devices or sometimes a small group of IoT devices connected to each other, which builds a small-size smart home or office environment. A small and static IoT group often provides services through collaboration between IoT devices belonging to the same group. In this case, the type of services and a collaboration protocol for each service are pre-defined in general. It is quite useful in an application domain providing a limited number of services. To fully utilize the capabilities and capacities of IoT devices, we need to support large-scale and/or dynamic collaboration between Things so that IoT devices organize a group to achieve a common goal through collaboration between them. Towards this goal, trust management in the mission-oriented IoT (MIIoT) systems is critical. Existing works on trust management in IoT do not satisfy the needs of the MIIoT system due to lack of consideration of the heterogeneity of devices, the autonomy of

devices, the diverse types of collaboration, the cooperability of devices, and so on. In this paper, we therefore introduce existing work on trust management models and systems on IoT and then address their limitations to apply to the MIoT systems. To promote future research on MIoT, we identify potential issues to be addressed and discuss some challenges. Once we find solutions to those issues and challenges, we will be able to expand the application domain of MIoT to many other areas in the future.

ACKNOWLEDGMENTS

This material is based upon work supported in part by the Jackson-Hope Fund of Virginia Military Institute and the Virginia Center for Undergraduate Research. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Virginia Military Institute.

REFERENCES

- [1] Bojan Jovanović. 2021. 45 Fascinating IoT Statistics for 2021: The State of the Industry. Retrieved April 2021 from <https://dataprot.net/statistics/iot-statistics/>
- [2] Youna Jung. 2019. Chapter 3. Bio-inspired Collaboration Schemes and Cyber Security. Nature-inspired Cyber Security and Resilience: Fundamentals, Technology and Applications. (April 2019), 51-74. <https://doi.org/10.1049/PBSE010E>
- [3] Youna Jung and Aaron Causey. 2019. HyDRS-WoT: Community-oriented Hybrid Disaster Response System using Web of Things. 21st International Conference on Information Integration and Web-based Applications and Services. ACM, (December 2019), 603-606
- [4] Anne H. Ngu, Mario Gutierrez, Vangelis Metsis, Surya Nepal, and Quan Z. Sheng. 2016. IoT Middleware: A Survey on Issues and Enabling Technologies. IEEE Internet of Things Journal, 4, 1, (February 2017), 1-20. <https://doi.org/10.1109/JIOT.2016.2615180>
- [5] Ikram Ud Din, Mohsen Guizani, Byung-Seo Kim, Suhaidi Hassan, and Muhammad Khurram Khan. 2018. Trust Management Techniques for the Internet of Things: A Survey. IEEE Access, 7, (November 2018), 29763-29787. <https://doi.org/10.1109/ACCESS.2018.2880838>
- [6] Amanda. Fixed: Trust Relationship Between Workstation & Domain Failed. 2020. MiniTool. Retrieved April 2021 from www.partitionwizard.com/partitionmanager/trust-relationship-failed.html
- [7] Kaitlin Boeckl, Michael Fagan, William Fisher, Naomi Lefkowitz, Katerina Megas, Ellen Nadeau, Ben Piccarreta, Danna Gabel O'Rourke, and Karen Scarfone. 2019. Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. National Institute of Standards and Technology Interagency or Internal Report 8228. (June 2019), 1-34. <https://doi.org/10.6028/NIST.IR.8228>
- [8] Zheng Yan, Peng Zhang, Athanasios V. Vasilakos. 2014. A survey on trust management for Internet of Things. Journal of Network and Computer Applications 24, (June 2014), 120-134. <https://doi.org/10.1016/j.jnca.2014.01.014>
- [9] Fenye Bao and Ing-Ray Chen. 2012. Dynamic Trust Management for Internet of Things Applications. Proceedings of the 2012 International Workshop on Self-Aware Internet of Things, (September 2012), 1-6. <https://doi.org/10.1145/2378023.2378025>
- [10] Ing-Ray Chen, Jia Guo, and Fenye Bao. Trust Management for SOA-Based IoT and Its Application to Service Composition. IEEE Transactions of Service Computing 9, 3, (May-June 2016), 482-495. <https://doi.org/10.1109/TSC.2014.2365797>
- [11] Jia Guo, Ing-Ray Chen, Jeffrey, and J.P. Tsai. 2017. A survey of trust computation models for service management in internet of things systems. Computer Communications 97, (January 2017), 1-14. <https://doi.org/10.1016/j.comcom.2016.10.012>
- [12] Ing-Ray Chen, Jia Guo, Fenye Bao, and Jin-Hee Cho. 2014. Trust Management in Mobile Ad Hoc Networks for Bias Minimization and Application Performance Maximization. Ad Hoc Networks 19, (August 2014), 59-74. <https://doi.org/10.1016/j.adhoc.2014.02.005>
- [13] Ing-Ray Chen, Jia Guo, and F. Bao. 2014. Trust management for service composition in SOA-based IoT systems. In Proceedings of the 2014 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, Istanbul, Turkey, 444-3449.
- [14] Jorg Daubert, Alexander Weismaier, and Panayotis Kikiras. 2015. A view on privacy & trust in IoT. In Proceedings of the 2015 IEEE International Conference on Communication Workshop (ICCW). IEEE, London, UK, 2665-2670.
- [15] David Airehrour, Jairo Gutierrez, and Sayan Kumar Ray. 2016. Lightweight Trust Design for IoT Routing. In Proceedings of 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress. IEEE, Auckland, New Zealand, 552-557.
- [16] Won Sang Chin, Hyun-soo Kim, Young Ju Heo, and Ju Wook Jang. 2015. A Context-based Future Network Infrastructure for IoT Services. Procedia Computer Science 56, (2015), 266-270. <https://doi.org/10.1016/j.procs.2015.07.207>
- [17] Mehrdad Salimitari, Shameek Bhattacharjee, Mainak Chatterjee, Yaser P. Fallah. 2020. A Prospect Theoretic Approach for Trust Management in IoT Networks under Manipulation Attacks. ACM Transactions on Sensor Networks 16, 3, (August 2020), 1-26.
- [18] Yu Liu, Kin-Fai Tong, Xiandong Qiu, Ying Liu, and Xuyang Ding. 2017. Wireless Mesh Networks in IoT Networks. In Proceedings of 2017 International Workshop on Electromagnetics: Applications and Student Innovation Competition. IEEE, London, UK, 183-185.
- [19] Tyrone Grandison and Morris Sloman. 2000. A survey of trust in internet applications. IEEE Communications Surveys & Tutorials 3, 4, (Fourth Quarter 2000), 2-16. <https://doi.org/10.1109/COMST.2000.5340804>
- [20] Jie Yuan and Xiaoyong Li. 2018. A Reliable and Lightweight Trust Computing Mechanism for IoT Edge Devices Based on Multi-Source Feedback Information Fusion. IEEE Access 6, (April 2018), 23626-23638. <https://doi.org/10.1109/ACCESS.2018.2831898>
- [21] Hikaru Inomoto, Sachio Saiki, Masahide Nakamura, and Shinsuke Matsumoto. 2016. Mission-Oriented Large-Scale Environment Sensing Based on Analogy of Military System. In Proceedings of the 18th International Conference on Information Integration and Web-Based Applications and Services. 414-421. <https://doi.org/10.1145/3011141.3011148>
- [22] Axel Moinet, Benoit Darties, and Jean-Luc Baril. 2017. Blockchain Based Trust & Authentication for Decentralized Sensor Networks. IEEE Journals & Magazine, (June 2017), 1-6.
- [23] Nikolaos Alexopoulos, Jörg Daubert, Max Mühlhäuser, and Sheikh M. Habib. 2017. Beyond the Hype: On Using Blockchains in Trust Management for Authentication. In Proceedings of 2017 IEEE Trustcom/BigDataSE/ICSS. IEEE Sydney, Australia, 546-553.
- [24] Geir M. Køien. 2011. Reflections on Trust in Devices: An Informal Survey of Human Trust in an Internet-of-Things Context. Wireless Personal Communications 61, 3, (December 2011), 495-510. <http://dx.doi.org/10.1007/s11277-011-0386-4>