A Centralized Trust Management Mechanism for the Internet of Things (CTM-IoT)

Mohammad Dahman Alshehri[1,2(✉)] and Farookh Khadeer Hussain[1]

[1] Faculty of Engineering and IT,
University of Technology Sydney, Ultimo, Australia
{Mohammad.Alshehri,Farookh.Hussain}@UTS.edu.au
[2] Computer Science Department, Taif University, Taif, Saudi Arabia

Abstract. The Internet of Things (IoT) is an extended network that allows all devices to be connected to one another over the Internet. This new network faces numerous challenges, but mainly security issues. One such issue is how the IoT's nodes can trust each other when they are connected over the Internet. There is a lack of studies that address the issue of trust management in IoT, or that provide a fully trustworthy framework. This paper proposes and delivers a centralized trust management mechanism for IoT by adding trust modules as a feature of the central trust manager, the Super Node (SN). To deliver a comprehensive approach, the SN includes other modules which are integrated with the whole IoT Trust Management framework to provide trustworthy communication between all nodes.

1 Introduction

The Internet of Things (IoT) can be described as a set of devices, considered to be smart, which interact collaboratively to fulfill a particular goal [13]. The advent of IoT has ushered in a vast array of smart services, including applications used by individuals and organizations, to handle the challenges they face as they interact and connect with devices anytime, anywhere [12]. With the increasing possibility of infusing smartness everywhere, these devices are being used to connect the physical world, where field operations take place, and the cyber world, where data processing and decisions are handled [8]. The interaction between devices and the physical world through the use of Internet protocols and standards make the collection of data from the environment possible [5]. In short, the IoT serves as a universal networking infrastructure that deploys data acquisition devices and communication resources to connect physical and virtual objects [8].

Issues of data security and authentication arise when data transfer from one cluster to another cluster takes place in the IoT [11]. The IoT is particularly challenged in the area of trust management. The heterogeneity of entities has limited storage, and protocols that are designed for trust management fail in the regulation of data as the result of limited capacity and resources [6].

The evolution of the IoT system also poses other significant challenges. According to [6], the evolution of the IoT system comes with the creation of nodes, requiring the protocol on trust management to allow the establishment of a highly accurate trust

L. Barolli et al. (eds.), *Advances on Broad-Band Wireless Computing, Communication and Applications*, Lecture Notes on Data Engineering and Communications Technologies 12,
https://doi.org/10.1007/978-3-319-69811-3_48

network. Another issue to surface is that the interconnectedness of IoT networks poses a significant risk, since the system will be subject to malicious attacks [5].

As discussed in [11], a centralized trust management mechanism will provide a sustainable means of communication in the IoT. The contributions of this paper are therefore as follows: (1) it provides an analysis of the trust management features of IoT; (2) it provides a novel centralized trust management mechanism for communication in IoT; (3) it describes the main component of the centralized mechanism, together with the features for each module in the mechanism; and (4) it presents a unique solution for IoT trust management issues.

The remainder of the paper is organized as follows. We give an overview of related literature in Sect. 2. In Sect. 3, we present a novel centralized trust management mechanism for IoT based on the Super Node (SN) and describe the overall framework of the mechanism and its components (API Module, Trust Management Module and Repository and Communication Module). The Conclusion is given in Sect. 4.

2 Related Works

We are undeniably heading towards a future in which the Internet of Things (IoT) will play a huge role. The IoT will connect the physical world and cyberspace in every way through the use of billions of smart objects [6]. The resultant high level of heterogeneity is expected to bring security threats to the Internet as a result of the interaction of humans, machines, and robots [2]. There is a pressing need to design a dynamic trust management protocol for IoT systems that considers the threat of both malicious and socially uncooperative nodes [2, 3]. However, little work has so far been done on the management of trust or security enhancement in the IoT environment, especially in respect of dealing with misbehaving nodes that are currently legitimate members of an IoT community [1, 3]. This has paved the way for studies that pertain to trust management protocols to be conducted.

One form of trust management to support service composition applications in IoT systems that is both adaptive and scalable is service-oriented architecture (SOA) [6]. This work uses distributed collaborative filtering to select feedback with the use of a devised similarity rating of the relationships detected [6]. It includes a filtering technique which determines the best way of combining direct and indirect trust to minimize bias in the presence of malicious nodes that might perform opportunistic service attacks. To ensure scalability, a framework is considered in [6] in which a capacity-limited node only retains the trust information of a subset of nodes of interest and performs a minimal computation to update trust. The method uses a trust protocol with limited storage space. However, this work fails to consider other attacker behavior models, including opportunistic collusion attacks, random attacks, and insidious attacks, to further test the resilience of adaptive and scalable trust protocol design [6].

A comparative analysis paper [2] calls for the creation of a unified vision in research to satisfy security and privacy requirements in a heterogeneous environment that involves a variety of technologies and communications standards. This is something that current works pertaining to trust management in the IoT system fail to establish.

Dynamic Trust Management for IoT Applications is the framework proposed by [3]. This "trust management protocol is characterized by a node that maintains its own trust assessment towards other nodes" [3]. For scalability, a node may restrict its trust evaluation to a limited set of nodes in which it is most interested [3]. The trust management protocol is encounter-based as well as activity-based. Nodes exchange their trust evaluation results with other nodes in the form of recommendations. Honesty, cooperativeness, and community interest are components of the multiple trust properties. The results indicate that this protocol converges to ground truth status in dynamic IoT environments and is resilient to misbehaving attacks [3]; however the work fails to test the protocol's resilience to a variety of changing environmental hostilities and attacks [3].

The Trust and Energy Awareness Secure Routing Protocol (TESRP) for WSN is the protocol proposed by [1]. This protocol makes use of a distributed trust model to determine and exclude misbehaving nodes. TESRP employs a multi-faceted routing strategy that considers "the trust level, residual energy, and hop-counts of neighboring nodes while making routing decisions" [1]. This strategy ensures data dissemination with trusted nodes as channels while balancing the energy consumption between trusted nodes by traversing shorter paths. Its limitation lies in the fact that it fails to evaluate TESRP in countering wormhole, selfish and Sybil attacks.

A survey of trust computation models for IoT systems for the purpose of service management has also been conducted [7]. This survey classifies existing trust computation models for service management in IoT Systems based on "trust composition, trust propagation, trust aggregation, trust update, and trust formation" [7]. It summarizes the advantages and disadvantages of each dimension and stresses the effectiveness of defense mechanisms against malicious attacks. The survey concludes that there are identified gaps in IoT trust computations.

Another survey investigates the properties of trust, proposes the objectives of IoT trust management, and provides a survey of the advances made towards a trustworthy IoT [14]. The survey proposes a holistic solution for IoT trust management trust management framework. It is "composed of IoT trust management composing modules and supporting modules for achieving intelligent and trustworthy IoT application/service based on social trust relationships" [14]. The survey calls for IoT entities based on "trust relationships and privacy in social trust mining" [14]. It proposes that lightweight security and privacy solutions should be developed based on trust relationship evaluation.

A "quantitative model of trust value based on multidimensional decision attributes" is proposed by [15]. The direct trust value of the monitored node is measured from a multitude of aspects, including but not limited to the packet forwarding capacity, repetition rate, consistency of packet content, delay, and integrity [15]. Having identified the problem that the trust evaluation of nodes in traditional methods is not objective, the model employs entropy theory. In calculating the indirect trust value, Dempster-Schafer theory is adopted to deduce and synthesize trust, and the statistics involved in the nodes' behavior. The simulation results show that this method effectively takes into account the subjective and objective evaluation of trust, thereby avoiding malicious nodes. The survey places less emphasis on practical needs and

demands such as power-efficient technologies, lightweight trust management, and IoT user trust [15].

The work in [10] proposes a reliable trust-based data aggregation protocol that is energy efficient called the ERTDA protocol. Based on observations of nodal behavior, the ERTDA protocol calculates, monitors, and evaluates the trust values of the nodes. It also detects and excludes compromised nodes. Simulation results show that the proposed protocol has the capacity to effectively improve "the accuracy of the aggregation, reduce the nodal mortality rate, reduce the nodal energy consumption, improve the reliability of the data transmission and extend the life of the networks" [10]. A certain proportion of compromised nodes in the network nevertheless sent the wrong data to the aggregation node in this study.

Another work has led to the design of a scalable, adaptive, and survivable trust management protocol in dynamic social IoT environments [4]. In the Community of Interest (CoI), nodes form into communities of interest by establishing social connections between entity owners. CoI identifies the best trust protocol settings in the presence of changing conditions and malicious nodes that perform trust-related attacks. However, the authors have yet to include secure routing and intrusion detection in such communities as Robot as a Service, in a cloud computing environment, or in communities of associated smart phones in their research endeavors [4].

A trust propagation method is suggested in [9] that exploits the unusual nature of social networks and incorporates a landmark-based method intended to improve the efficiency of trust prediction. The method involves the selection of a small number of social network landmark users that will serve as referees in trust propagation. Landmark users provide referrals on the trust ratio between two users who are indirectly connected. In evaluating the performance of the proposed method, comprehensive experiments are conducted using a real online social network [9]. The experimental results show that this method has greater efficiency than any of the other four methods of trust prediction. The extension of this work to social networks with more general settings and the use of larger datasets to evaluate the proposed trust prediction method is suggested in future studies [9].

3 A Centralized Trust Management Mechanism for IoT

In this section, we present a novel centralized approach for trust management in the Internet of Things (IoT). We demonstrate the overall mechanism and components of the proposed Trust Management Mechanism for the Internet of Things (TM-IoT), which is designed to provide trustworthy communication between IoT nodes.

Figure 1 shows the overall framework of the TM-IoT which includes a Super Node (SN) as the centralized trust manager node. To achieve trustworthy communication between nodes, we propose dividing the IoT environment into clusters. Each cluster has a local trust manager called a Master Node (MN). There are also multiple Cluster Nodes (CN) in each cluster which communicate with one another under MN supervision. The SN has a central repository to store the trust data for all MNs and CNs for the entire IoT framework, and MNs have local repositories in which the trust values for the CNs in each cluster are stored.

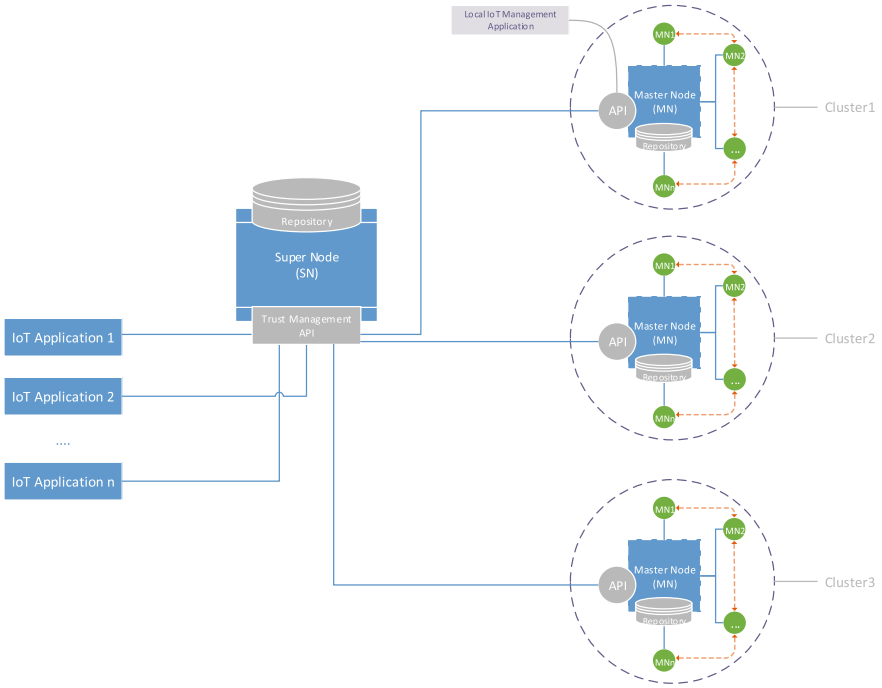

Fig. 1. A centralized trust management of IoT mechanism (TM-IoT)

3.1 Super Node (SN) Mechanisms and Modules

The Super Node (SN) provides centralized trust monitoring and mapping services for the TM-IoT. The concept of the SN is similar to that of a router, which carries out the function of directing traffic; however, the SN performs another function by providing a trust management service for the whole TM-IoT platform. The SN sends and monitors packets of Internet data between the MN and CNs in clusters, and between the MN and the IoT application. Any IoT application can access the SN remotely over the Internet. The IoT application can request trust data about any CN by forwarding a request to the MN of a particular cluster, or can provide trust data to IoT applications or other cluster nodes (CNs).

As noted above, the SN is the main node in the TM-IoT framework, and it communicates with many Master Nodes (MNs) of clusters. Communication between the SN and MNs takes place over HTTPS and via their APIs. The SN has a trust value repository for all the MNs in the TM-IoT framework, in which the trust values of each cluster's MN and the addresses of their CNs are stored. The SN repository does not store CN functions but works as a routing table to store the trust value data and network topology, and to direct which nodes should join which cluster in the TM-IoT framework.

The table of the SN repository has three fields:

- The Master Node ID (MNID): denoting which MN belongs to which cluster.
- The Cluster Node ID (CNID): lists the CNIDs of each cluster MN.
- IP addresses of MNs.

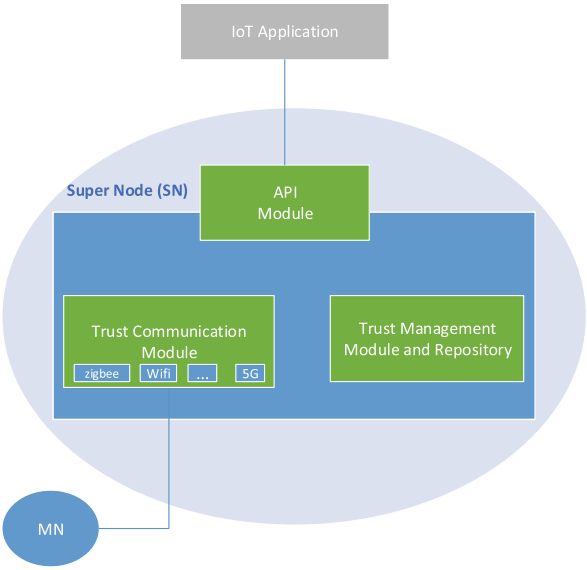

Fig. 2. Centralized IoT super node (SN) modules

The design of the Super Node (SN) uses a modular format to develop the capabilities and functionalities of the SN. Figure 2 shows the three main modules of the SN:

1. API Module
2. Trust Management Module and Repository
3. Trust Communication Module

These modules are described in the subsections that follow.

3.1.1 API Module

The Application Programming Interface (API) improves the interface communication for IoT applications. It assists IoT applications to be connected with each other in the TM-IoT. The API also allows IoT applications to reclaim the CN data which is stored in the repository over the Internet, and to send MN instructions to the relevant CN. The design pattern for the API is Representational State Transfer (REST), which supports independent languages and platforms such as UNIX, IOS, Android, and Windows, and thus does not require the use of a specific programming language such as Python (Fig. 3).

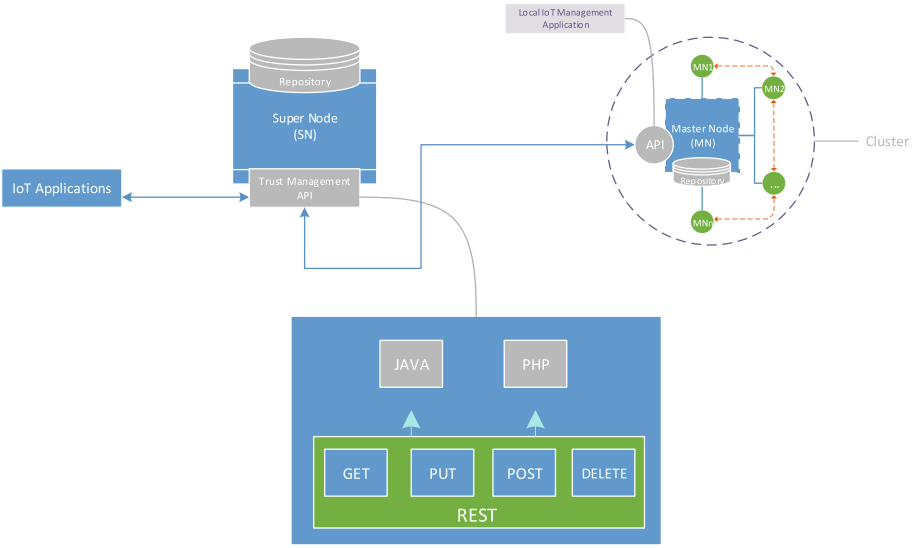

Fig. 3. API module components

- ***GET:*** used by the IoT application to request the CN data which is stored in the MN's repository.
- ***PUT:*** used by the MN application to send and update the data to the SN's repository.
- ***POST:*** used by the SN application to send SN instructions to the MN.
- ***DELETE:*** used by the MN application to delete data from the SN repository.

3.1.2 Trust Management Module and Repository

The Trust Management Model has two key responsibilities: trust communications between the SN and MNs, and communications between the MNs and CNs (including between the CNs in a cluster).

In the trust communication between SN and MN, the MN builds a contact with the SN by providing its main authentication data (MNID) to register it in the SN's repository. Once the MN is registered in the cluster, it is authorized to register the CNs. For trust communications between the MN and CNs, each CN should send its data identification (CNID) to the MN, which will check whether or not the trust value for the CN corresponds to the trust value of the cluster. If the CN trust value is accepted by the MN, the CN's trust value will be registered in the MN's repository and the CN will be allowed to join the cluster. It can then build trust communication between the MN and CN, and between the CN and other CNs in the same cluster.

3.1.3 The Trust Communication Module (TCM)

The Trust Communication Module (TCM) is the module which manages and controls trust communication between the Master Node (MN) and Cluster Node (CN), and between the cluster and the Super Node (SN). The communication in TCM consists of

two types of messages: management messages and trust value messages. Management messages for the whole framework are controlled by the SN and the MN in each cluster to obtain management information between the CN and MN, such as information node connections and the status of the IoT network. Trust value messages are used to obtain the trust value status of the CNs and send updates to the MN. These trust messages take two forms, *Receive* and *Send*. *Receive* messages are used by the SN to accept messages from the MN, and for the MN to receive new trust value information from the CNs. *Send* messages are managed by the CNs to send trust value updates to the MN, following which the MN updates the SN. The definition of these messages is given below.

Program listings or program commands in the text are normally set in typewriter font, e.g., CMTT10 or Courier (Table 1).

Table 1. Trust value status

TrV Index	Description	Status
0	Completely not trusted	Extremely harmful
0.1	Semi-not trusted	Very harmful
0.2	Risk trust	Risk
0.3	Low trust	Medium risk
0.4	Medium trust	Low risk
0.5	Semi-trust	Semi-safe
0.7	Trust	Safe
0.8	High trust	Safe
0.9	Very high trust	Safe
1	Completely trust	Completely safe

- ***Receive (CNID, TrV Array[]):*** The Receive() message receives the updated messages and other alerts from the CN to the MN, and from the MN to the SN. The Receive() message has two main parameters: the first parameter is the CNID, which is the exclusive identifier ID for the cluster node. The second parameter is the TrV Array[]. This is an array format which stores the message content of the new trust value of the CN and sends it to the MN.

  Receive message format

CNID	TrV
Receive Message []	

- ***SendUpdate (CNID):*** The SendUpdate() message is generated by the MN to request and send an update from the CN. The SendUpdate() message has one main parameter which is the unique ID of the cluster node to avoid any overlap or miscommunication.

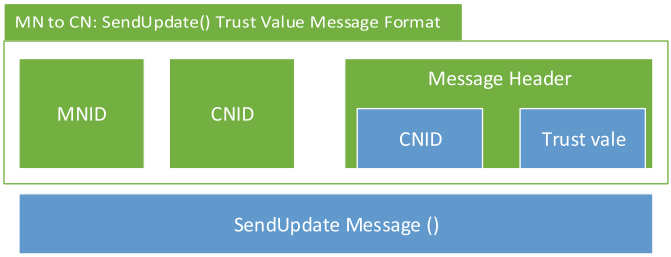

Fig. 4. SendUpdate trust value message format MN to CN

Figure 4 shows the format of the SendUpdate message sent by an MN to a CN. For example, SendUpdate(trust value) is used to obtain a new update about the trust value of a particular CN in the cluster.

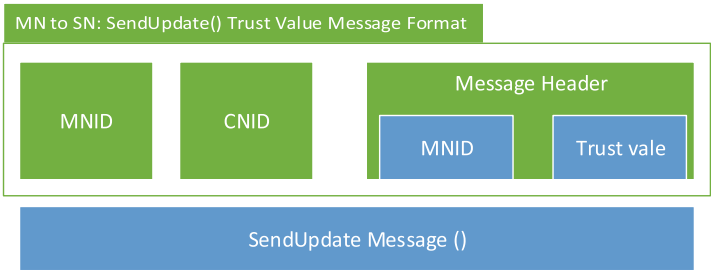

Fig. 5. SendUpdate trust value message format MN to SN

Figure 5 shows the format of the SendUpdate message sent by an MN to the SN. For example, SendUpdate(trust value) is used to update the SN about the MN trust value.

- ***Response (MessageID, CNID, Array[]):*** this is a message from the CN in reply to the MN SendUpdate() message. The message Response() has three main parameters: the MessageID, which is handled by the MN and used to match requests to responses. The second parameter is the CNID, which is the unique ID for the appointed CN. The last parameter is the content of Response() message, formatted in array[].

Figure 6 shows the format of the SendUpdate and Response message sent by an MN to a CN. The message header includes the time of the request and the message reply.

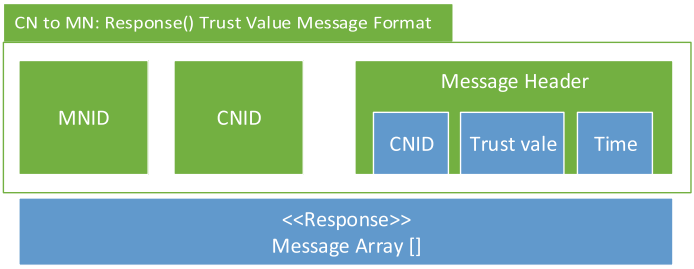

Fig. 6. Response trust value message format CN to MN

4 Conclusion and Future Works

The Internet of Things (IoT) faces many challenges, especially in security and trust management. A centralized trust management mechanism is one solution that can overcome IoT security challenges. In this paper, we have presented a novel centralized trust management mechanism for IoT. The main feature of this mechanism is the Super Node (SN), which is the central trust manager of the IoT trust management framework. We have explained the main components and modules of this novel mechanism, including the API module, Trust Management Module and Repository and Communication Module. We have demonstrated how the mechanism works efficiently to provide trust for IoT communication, and also how it is managed. In future, we will implement this mechanism in an IoT simulation tool and compare it with similar approaches.

References

1. Ahmed, A., Bakar, K.A., Channa, M.I., Khan, A.W.: A secure routing protocol with trust and energy awareness for wireless sensor network. Mobile Netw. Appl. **21**(2), 272–285 (2016)
2. Alshehri, M.D., Hussain, F.K.: A comparative analysis of scalable and context-aware trust management approaches for internet of things. In: International Conference on Neural Information Processing, pp. 596–605. Springer (2015)
3. Bao, F., Chen, I.-R.: Dynamic trust management for internet of things applications. In: Proceedings of the 2012 International Workshop on Self-aware Internet of Things, pp. 1–6. ACM (2012)
4. Bao, F., Chen, R., Guo, J.: Scalable, adaptive and survivable trust management for community of interest based internet of things systems. In: 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS), pp. 1–7. IEEE (2013)
5. Bello, O., Zeadally, S.: Intelligent device-to-device communication in the internet of things. IEEE Syst. J. **10**(3), 1172–1182 (2016)
6. Chen, R., Guo, J., Bao, F.: Trust management for SOA-based IoT and its application to service composition. IEEE Trans. Serv. Comput. **9**(3), 482–495 (2016)
7. Guo, J., Chen, R., Tsai, J.J.: A survey of trust computation models for service management in internet of things systems. Comput. Commun. **97**, 1–14 (2017)

8. Jabeur, N., Yasar, AU-H, Shakshuki, E., Haddad, H.: Toward a bio-inspired adaptive spatial clustering approach for IoT applications. Future Gener. Comput. Syst. (2017)
9. Lyu, S., Liu, J., Tang, M., Xu, Y., Chen, J.: Efficiently predicting trustworthiness of mobile services based on trust propagation in social networks. Mobile Netw. Appl. **20**(6), 840–852 (2015)
10. Ma, T., Liu, Y., Zhang, Z.: An energy-efficient reliable trust-based data aggregation protocol for wireless sensor networks. Int J Control Autom. **8**(3), 305–318 (2015)
11. Miao, J., Wang, L.: Rapid identification authentication protocol for mobile nodes in internet of things with privacy protection. JNW **7**(7), 1099–1105 (2012)
12. Ortiz, A.M., Hussein, D., Park, S., Han, S.N., Crespi, N.: The cluster between internet of things and social networks: review and research challenges. IEEE Internet of Things J. **1**(3), 206–215 (2014)
13. Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A.: Security, privacy and trust in Internet of Things: the road ahead. Comput. Netw. **76**, 146–164 (2015)
14. Yan, Z., Zhang, P., Vasilakos, A.V.: A survey on trust management for Internet of Things. J. Netw. Comput. Appl. **42**, 120–134 (2014)
15. Yu, Y., Jia, Z., Tao, W., Xue, B., Lee, C.: An efficient trust evaluation scheme for node behavior detection in the internet of things. Wirel. Pers. Commun. **93**(2), 571–587 (2017)