Chapter 1
A Distributed Trust Management Model for the Internet of Things (DTM-IoT)

Mohammad Dahman Alshehri, Farookh Hussain, Mahmoud Elkhodr, and Belal Saeed Alsinglawi

Abstract The Internet of Things (IoT) is a paradigm that facilitates autonomous communications among various IoT devices with minimal human intervention. This raises many security challenges, which are critical and must be addressed to allow for the wide deployment of IoT. Trust must be provisioned among the various heterogeneous IoT devices. In this paper, a distributed trust management model is proposed. The model offers solutions to trust management and negotiations in the IoT. It is inspired by clustering techniques that are adopted in WSNs. After introducing the structural design and the main components of the trust model, we demonstrate how our new approach supports trust negotiations and management in the IoT.

1.1 Introduction

The management and provision of trust in the Internet of Things (IoT) are essential for the security and trustworthiness of communications in the IoT [1]. While

M. D. Alshehri
Centre for Artificial Intelligence, School of Software, Faculty of Engineering and Information Technology, University of Technology Sydney, Ultimo, NSW, Australia

Computer Science Department, Taif University, Taif, Saudi Arabia
e-mail: Mohammad.Alshehri@uts.edu.au

F. Hussain (✉)
Centre for Artificial Intelligence, School of Software, Faculty of Engineering and IT, University of Technology Sydney, Ultimo, NSW, Australia
e-mail: Farookh.Hussain@uts.edu.au

M. Elkhodr
School of Engineering and Technology, College of Engineering and Technology, Central Queensland University, Sydney, NSW, Australia
e-mail: m.elkhodr@cqu.edu.au

B. S. Alsinglawi
Western Sydney University, Sydney, NSW, Australia
e-mail: belal.alsinglawi@ieee.org

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_1

numerous IoT communication and interaction models have been the focus of various research studies, such as in [2, 3, 11], solutions that provide trustworthy communications between nodes based on a clustering technique remain unexplored. Existing research such as [3] provides a solution for the smart community for IoT by addressing low cost and power. However, adequate attention has not been given to trust and trust management establishment for IoT devices. The IoT encompasses various applications and devices such as smart products that connect to the Internet using sensors and actuators, which requires management of data, its sharing and analysis mechanisms [2, 4]. Therefore, trust management protocols are needed for trust establishment among the diverse range of IoT devices. The need for trust management in the IoT becomes apparent given the sheer size of the IoT. For instance, [5] points out that the IoT has a growing number of IoT devices, especially in storage and computation. IoT networks should also allow individual nodes to gain trust rapidly and accurately while evolving to adapt to the dynamicity involved around nodes joining and leaving the network on a regular base. The complexity in IoT communications imply that trust management protocols, designed for the IoT, should be highly resilient to trust-based attacks to ensure security protection in hostile environments. Trust management is also necessary given the heterogeneity of communications and the volume of IoT devices.

Among the various issues challenging trust management in the IoT such as lightweight characteristics of IoT devices, perhaps, scalability should be a key consideration in the design of trust protocols in the IoT [6]. This is because most of the existing trust management solutions such as those proposed in [3, 6, 7] did not address the scalability issue, thereby undermining their applicability to large-scale IoT networks.

Trust management and security in the IoT are fundamental to establish trustworthy connections [8–14]. There is a lack of research on trust management in the IoT. More specifically, previous frameworks failed to consider cluster-based approaches and focused mainly on individual solutions at the node level. In [15], the authors proposed a fuzzy reputation method for trust management in the IoT. However, this model is mainly designed to work with wireless sensor networks (WSNs). It focuses more on quality of service (QoS) metrics such as energy consumption, rather than establishing trust among IoT devices.

Similarly, other works such as [4] proposed a trust management protocol that takes into account QoS trust metrics and social trust. In order to update trust values, the authors relied, in their proposed method, on indirect recommendations and direct observations. However, the research is limited to static IoT scenarios. It does not consider the rich and dynamic interactions envisioned in the IoT. Given that the IoT is growing exponentially, solutions such as those proposed in [4] are not applicable to IoT scenarios that involve dynamic interactions.

To fill this gap, this paper introduces the Distributed Trust Management Model (DTM-IoT). The structural design of the proposed DTM-IoT is provided in Sect. 1.2. Section 1.3 presents the components of DTM-IoT. We first describe the architecture of the model, which focuses on the distribution of the IoT nodes based on the dynamic trust value of clusters. We will then elaborate in more details the main components of the proposed model, which consists of the Cluster Node (CN) component and the Master Node (MN) component. These nodes are responsible for managing the trust management in an IoT network. Conclusion and future works are provided in Sect. 1.4.

1.2 The DTM-IoT Structural Design

The DTM-IoT provides trustworthy communication among devices that are involved in a communication as part of an IoT network. The DTM-IoT architecture allows various IoT devices and applications to establish a trusted communication among themselves, thus paving the way towards a secure communication. The architecture of the DTM-IoT is presented in Fig. 1.1. The DTM-IoT encompasses four types of devices. The first type is a general device, which is a basic physical device. It has default trust value. A device with an actuator is the second type of DTM-IoT device. The role of these devices is to receive the *trust value* command over the Internet. The third type of DTM-IoT devices have sensors which fetch the trusted data from the IoT environment and transfer the data over the Internet. A

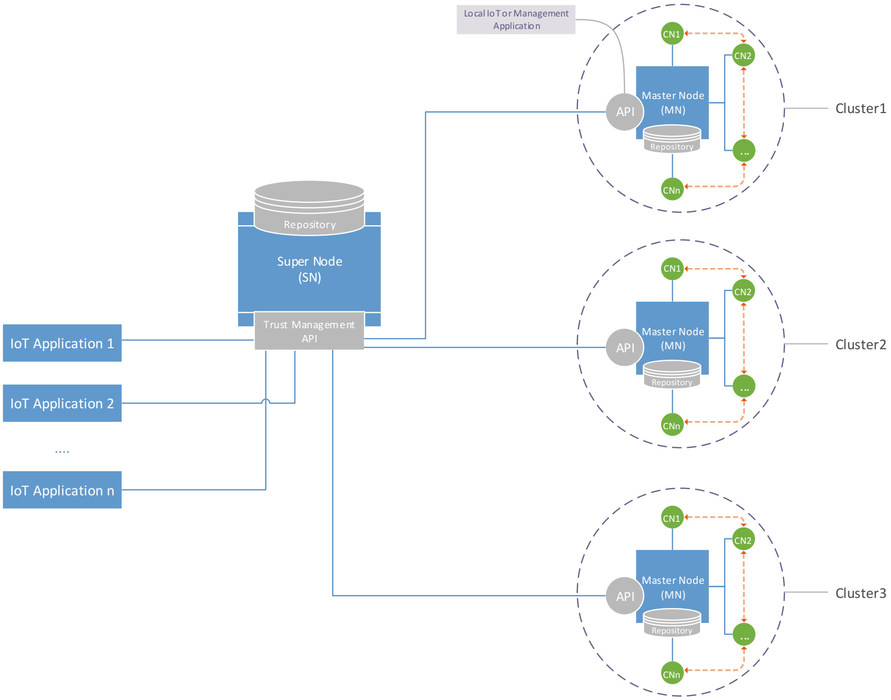

Fig. 1.1 DTM-IoT dynamic architecture

hybrid device is the last type of DTM-IoT device which has both trusted actuation and sensing capabilities. The DTM-IoT provides trustworthy communication among these nodes (devices).

The DTM-IoT architecture is a distributed architecture that consists of Cluster Node (CN), Master Node (MN) and a Super Node (SN). In this architecture, as shown in Fig. 1.1, the DTM-IoT adapts the structure that is used by traditional network management approaches. The DTM-IoT architecture consists of a Cluster Node (CN), which resides on a node, and a Master Node (MN). The Cluster Node (CN) acts as a communication node that has the responsibility for transporting the data generated or collected by CN to their MN. The MN manages many CNs in the Cluster. The MN also stores the received data, sent by CN in the cluster, in a repository at MN.

The Super Node (SN) is the base node in the DTM-IoT. It is responsible for ensuring trust in an IoT network. The SN contains an API, referred to as the trust management API. This API allows the SN to communicate with the Master Node (MN) in a given cluster. The SN also has a repository that stores the trust values and addresses of MNs and CNs. The repository of SN is hierarchical (tree-structured). Each entry relevant to a CN is addressed through the MN's unique ID. Therefore, the repository of SN does not store any data collected from the CN. It only stores its trust value and address information, i.e. through which MN and CN can be accessed. An IoT application running with the SN can provide services based on combining data collected from various CNs. Therefore, IoT applications and services are built on top of the IoT, by supporting communications among nodes through the SN.

The DTM-IoT architecture provides a centralised model of several clusters and a MN that allows for central trust management of things over local area networks. On the other hand, the DTM-IoT distributed architecture of several MNs and Clusters creates a trust distributed system where CNs communicate in a cooperative rather than a stand-alone manner. This flexibility in architecture is designed for the specific communications requirements of the IoT. This is important since IoT devices may play different roles in both centralised and distributed operation setups, especially for trust management in the IoT.

1.3 The DTM-IoT Mechanisms

In this section, we will introduce the various components of the DTM-IoT.

1.3.1 The Cluster Node (CN) Components

The Cluster Node (CN) is an IoT node which stores the trust value of a cluster in the MN repository. It stores the trust attributes of the cluster.

Table 1.1 IoT Cluster Node Trust Management Attributes

Trust Management Attributes (TMA)
ID
PKI
Trust value
Firmware version
IP, MAC address, network name or others
Battery life
Location (as a heterogeneous node)

In particular, CN is represented using the Trust Management Attributes (TMA). These attributes represent parameters such as the communication status of CN. A TMA is used to establish communication among other nodes in each cluster, based on the trust management criteria. TMAs are also used to maintain the data CN collects. They are also used to maintain information relating to CN activities. The formalisation of TMA offers a method to maintain and store CN trust information and other information collected by the MN repository. Table 1.1 shows the Trust Management Attributes (TMA) that represent a Cluster Node (CN).

We, therefore, define a CN as the IoT object that represents the device and its trust behaviour. CNs are accessed through the trust management repository by various IoT applications and the MN. CNs are a representation of IoT nodes that include not only the normal nodes, like a wireless sensor node, but also the trust communication module, software and driver (i.e. CN trust agent) that allow communication among nodes and the MN in the cluster. This is what is called the heterogeneous IoT node. A CN has a unique identification and trust attributes. The TMA can be defined and implemented for IoT nodes to the MN in the clusters. Table 1.1 shows that the TMAs are descriptions of the IoT node based on trust attributes. For instance, the ID is used to identify a unique IoT node. A public key infrastructure (PKI), trust value, firmware version and the rest of these TMAs are also used as identifiers or descriptions for IoT nodes. These trust attributes assist MNs to decide which nodes are appropriate to offer an authority to access and join the proper cluster, based on the similarity of trust value between the node and the cluster. These trust attributes support the CN in establishing a trusted communication among the CNs in the cluster. Therefore, the TMA will ultimately provide an opportunity for the CNs to be the trusted smart node.

Figure 1.2 models CNs and demonstrates that there are two main modules for a trust agent. The trust communication module is responsible for establishing communications that are trustworthy among other CNs and communicates with the MN. The trust agent services module is responsible for the services execution (such as generating low trust value level alerts or handling IoT trust actuation instructions). Therefore, the trust agent controls the communications between two important IoT nodes in the cluster. It controls the communication between CN and MN by sending the collated data to the MN and dealing out the requests sent by MN and correspondingly controls the communications between the CN and the other CNs in the cluster. The responsibilities of the CN trust agent are:

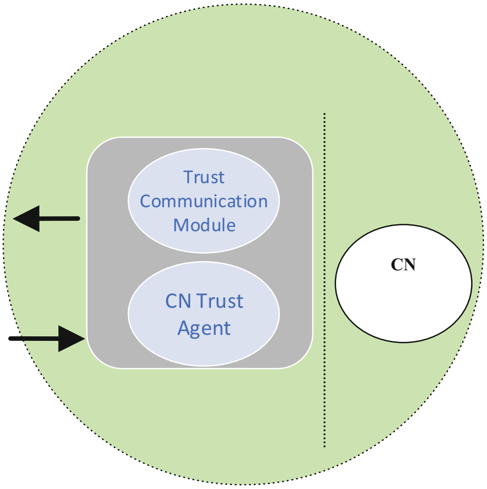

Fig. 1.2 Cluster Node (CN) components

- Establish a trust communication with the other CNs.
- Communicate and send data updates to the MN.
- Receive trust instructions of actuation from the MN.
- Manage responses and requests from/to the MN to join in/out the cluster.
- Send notifications of trust value levels to the MN.

1.3.2 The Master Node (MN) Components

Cluster is an IoT trusted CN application that performs the cluster operational roles of receiving and generating requests to retrieve trust value information from IoT nodes. A MN can also receive activity-based trust notification reports on CNs generated by their trust agent. MN controls the communication among nodes in the cluster to be trusted. It also manages the whole cluster so that it is secured and trusted. A MN maintains a trust value repository, which stores the trust value and other information about all CNs in the cluster. The MN accesses CNs' data stored in this repository. An MN also communicates with the Super Node (SN) to update it about its activity and to send a trust value of the whole cluster to be stored in SN repository.

A MN includes and provides a trust management Application Programing Interface (API) to receive IoT services from other nodes out of the cluster.

Information, which is stored in the MN repository, can be requested over the Internet once the API allows IoT applications to communicate with a MN. The API also allows trust management applications to control and monitor the CNs. The trust management API is used to communicate topology information over the Internet about the clusters and IoT network to the SN. The SN is a higher main IoT node that is responsible for the whole trust IoT network and is located above the MNs

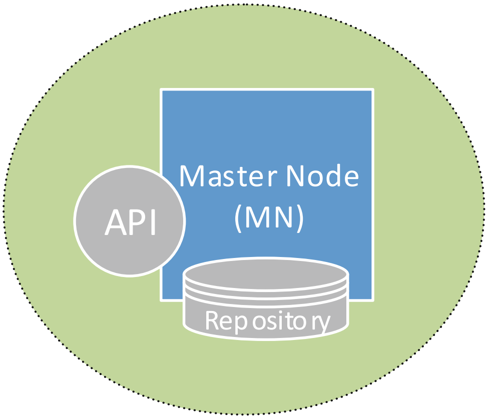

Fig. 1.3 Master Node (MN) components

and clusters. Under the supervision of the MN, the IoT applications run on top of the SN and send requests to access MN's data. Figure 1.3 shows the infarctions between MN and CNs in the cluster. To provide trustworthy communication in the cluster, the MN includes several modules that offer security, trust management and privacy abilities, among other IoT trust operational services.

1.3.3 The Cluster Components

The intention of the Trust Management IoT platform is to build upon dividing IoT nodes into different clusters based on their trust value. Based on each cluster's trust value, nodes will request to join into clusters. This method provides efficient and trusted IoT communication, by applying the trust value of the cluster for each node in the IoT. This allows for fast communication, easy control and longer battery life, since the request will be generated from nodes based on the trust value of the corresponding clusters. Nodes within the clusters contact the MNs to get authorisation to join or redirect the node. They request joining the appropriate cluster based on its trust value.

The cluster has two main functions. The first function is to maintain IoT communication by providing trustworthy communication. This allows nodes that have similar trust values to join into clusters. The cluster will then deal with other clusters rather than nodes. Another function of clusters is to provide additional communication capabilities for IoT networks through the application of trust management attributes for the cluster components (MN, CNs). Figure 1.4 shows the main components of MN.

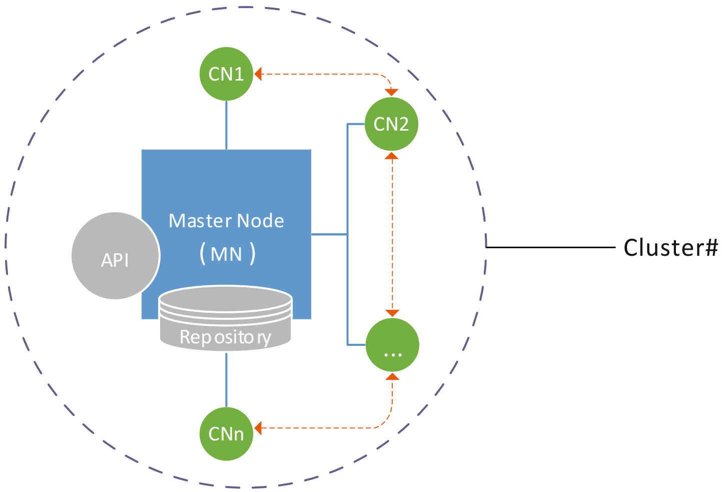

Fig. 1.4 Cluster components

1.4 Conclusion and Future Work

This paper introduced the Distributed Trust Management for Internet of Things (DTM-IoT) model. This proposed model consists of a Super Node (SN), a Master Node (MN) and a Cluster Node (CN). The DTM-IoT provides IoT devices with a mechanism that allows them to negotiate and establish trust among them. The model relies on a distributed architecture, in which the Super Node assigns trust values to cluster components. The communication between the Super Node and the Cluster component is facilitated by the Master Node. Future works involve the design of a network simulation in order to evaluate the proposed model. The simulation aims to demonstrate how a new node can join the IoT network and gains trust and thus engages in a secure communication with other nodes. The simulation work will also involve the design of a threat model to evaluate the trust management services provisioned by the DTM-IoT.

References

1. Alshehri, M. D., & Hussain, F. K. (2015). 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). Cham, Switzerland: Springer.
2. Alshehri, M. D., & Hussain, F. K. (2018). A centralized trust management mechanism for the internet of things (CTM-IoT). In *12th International conference on broad-band wireless computing, communication and applications. BWCCA 2017* (Vol. 12, pp. 533–543). Cham: Springer. https://doi.org/10.1007/978-3-319-69811-3_48.
3. Li, X., Lu, R., Liang, X., Shen, X., Chen, J., & Lin, X. (2011). Smart community: An internet of things application. *IEEE Communications Magazine, 49*(11), 68–75.

4. Bao, F., & Chen, I.-R. (2012). Dynamic trust management for internet of things applications. In *Proceedings of the 2012 International Workshop on Self-aware Internet of Things* (pp. 1–6). New York: ACM.
5. Chen, R., Bao, F., Chang, M., & Cho, J.-H. (2014). Dynamic trust management for delay tolerant networks and its application to secure routing. *IEEE Transactions on Parallel and Distributed Systems, 25*(5), 1200–1210.
6. Bao, F., & Chen, R. (2012). Trust management for the internet of things and its application to service composition. In *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)* (pp. 1–6). Piscataway, NJ: IEEE.
7. Chen, R., Guo, J., & Bao, F. (2016). Trust management for SOA-based IoT and its application to service composition. *IEEE Transactions on Services Computing, 9*(3), 482–495.
8. Chen, C., & Helal, S. A. (2011). Device-centric approach to a safer internet of things. In *International workshop on networking and object memories for the internet of things (NOMe-IoT)* (pp. 1–6). New York: ACM.
9. Ren, W. (2011). QoS-aware and compromise-resilient key management scheme for heterogeneous wireless internet of things. *International Journal of Network Management, 21*(4), 284–299.
10. Roman, R., Najera, P., & Lopez, J. (2011). Securing the internet of things. *Computer, 44*(9), 51–58.
11. Alshehri, M. D., Hussain, F. K., & Hussain, O. K. (2018). Clustering-driven intelligent trust management methodology for the internet of things (CITM-IoT). *In Mobile Netw Appl., 23*, 419–431. https://doi.org/10.1007/s11036-018-1017-z.
12. Zhou, L., & Chao, H.-C. (2011). Multimedia traffic security architecture for the internet of things. *IEEE Network, 25*(3), 35–40.
13. Alam, M., Ferreira, J., Mumtaz, S., Jan, M. A., Rebelo, R., & Fonseca, J. A. (2017). Smart cameras are making our beaches safer: A 5G-envisioned distributed architecture for safe, connected coastal areas. *IEEE Vehicular Technology Magazine, 12*(4), 50–59.
14. Jan, M.A., Usman, M., He, X., & Rehman, A.U. (2018). SAMS: A Seamless and Authorized Multimedia Streaming framework for WMSN-based IoMT. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2018.2848284
15. Chen, D., Chang, G., Sun, D., Li, J., Jia, J., & Wang, X. (2011). TRM-IoT: A trust management model based on fuzzy reputation for internet of things. *Computer Science and Information Systems, 8*(4), 1207–1228.