Reputation-Based Framework for Internet of Things

Juan Chen[1(✉)], Zhengkui Lin[1], Xin Liu[2], Zhian Deng[1], and Xianzhi Wang[3]

[1] School of Information Science and Technology,
Dalian Maritime University, Dalian 116026, China
juanchencs@gmail.com
[2] School of Information and Communication Engineering,
Dalian University of Technology, Dalian 116024, China
[3] School of Computer Science and Engineering,
University of New South Wales, Sydney, NSW 2052, Australia

Abstract. Internet of Things (IoT) is going to create a world where physical objects are integrated into traditional networks in order to provide intelligent services for human-beings. Trust plays an important role in communications and interactions of objects in IoT. Two vital tasks of trust management are trust model design and reputation evaluation. However, current literature cannot be simply and directly applied to the IoT due to smart node hardware constraints, very limited computing and energy resources. Therefore a general and flexible model is needed to meet the special requirements for IoT. In this paper, we firstly design LTrust, a layered trust model for IoT. Then, a Reputation Evaluation Scheme for the Node (RES-N) has been presented. The proposed trust model and reputation evaluation scheme provide a general framework for the study of trust management for IoT. The efficiency of RES-N is validated by the simulation results.

Keywords: Internet of Things · Reputation evaluation scheme
Trust management

1 Introduction

Internet of Things (IoT) is going to create a world where wireless devices are integrated into networks in order to provide intelligent services for human beings. The increasingly popularity of IoT greatly helps people to control and enjoy their lives. Generally, a tag which is attached to an object can only communicate with a nearby reader. A large number of readers are deployed by different organizations to provide service for commercial or military use. Thus, readers of different organizations need to work together for object information tracking and retriving. For instance, each organization manages many application servers, through which parents would like to trace the information of their child wearing tag-attached hand chain. Firstly, they will send the request to one of an application

X. Gu et al. (Eds.): MLICOM 2017, Part I, LNICST 226, pp. 592–597, 2018.
https://doi.org/10.1007/978-3-319-73564-1_59

servers managed by an organization. Then, the request will be sent to the IoT. Once a reader finds the target child, it tries to return the requested message to the application server.

Though there are lots of trust protocols for traditional wired and wireless networks such as P2P [1,2] and ad hoc sensor networks, little research has been done on trust management for IoT [3]. Previous work about trust in IoT are designed for some specific applications and therefore cannot be applied to other applications [4]. In addition, new nodes join in and existing nodes leave from IoT frequently. Trust management must address this issue to allow newly joining nodes to build up trust quickly with a reasonable degree of accuracy [5–7].

In order to overcome the above issues in previous work, we propose a reputation-based framework for IoT in this paper. Firstly, we propose LTrust, a four-layered trust model. The layered model can be applied to various applications. Furthermore, a reputation evaluation schemes for the node has been proposed respectively. The proposed trust model and reputation evaluation scheme provide a general framework for the study of trust management for IoT.

The rest paper is organized as follows. In Sect. 2 the four-layered trust model is proposed. In Sect. 3 our reputation evaluation scheme for the node is explored in detail. Finally, we conclude the paper in Sect. 5.

2 Layered Trust Model

We present LTrust, a layered trust model for IoT according to different functions of entities. LTrust provides new insights for research on trust-based interaction in IoT.

We classify the entities in IoT into four typies including tag-attached objects or tags, nodes, organizations and the RMC (Reputation Management Center). Then LTrust is designed as a four-layered model including the object layer, the node layer, the organization layer and the reputation management layer. The bottom object layer which is responsible for real-data collection consisting of a large number of moving tag-attached objects. Before joining the IoT, each tag has to register at an organization. The node layer, consisting of nodes such as readers, sensors and so on, lies above the object layer. This layer manages data retrieval and then routs data from the object to an organization. Specifically, nodes retrieve data from tags nearby and then return required results to the organization. Above the node layer is the organization layer which composed of different commercial or government organizations. Each organization deploys a certain number of nodes to perform operations on tags such as data update or retrieval. Since nodes from one organization can not cover the large area in IoT, it is necessary for different organizations and nodes to work together. However, a malicious node or an organization among good ones can launch attacks on the tag, thereby cause severely damage to the network. Thus, reputation is used to identify malicious nodes from good ones. Based on LTrust, we then evaluate the reputation of each node by the reputation evaluation schemes which will be introduced in Sect. 3 by RMC. According to the node's reputation, the tag's organization will decide whether grant the authorization to the node which requests to access to the tag.

3 Reputation Evaluation

For safety consideration, we have to prevent attacked nodes from accessing to the target tag. Different from good nodes, attacked nodes usually perform malicious behavior. So, we identy an attacked node according to its behavior. Specifically, we propose a Reputation Evaluation Scheme for the Node in the following Subsect. 3.1.

3.1 Reputation Evaluation Scheme for the Node

The node's reputation is evaluted based on the node's state which will be obtained by the node's behavior in RES-N. The tag T will record the node's behavior as evidence ED. Then, T will include ED as part of the response message when interacting with the next node R_n. After that, the message will be sent to O_T by the node R_n. Once receiving the response message, O_T determines and then submits R's behavior to RMC. Finally, RMC updates R's reputation by R's state which is determined by R's behavior. In all, the node reputation evalutation process includes the following three steps.

- ***Node's Behavior Determination***
  In order to perform operations on tag T, the node R must be authorized by the tag's organization O_T. Therefore, R requests authorization from O_T by sending a request message $AUTH\_R$ to O_T. Once being authorized, R can access to the tag. When the interaction between T and R is completed, T will generate an evidence ED to record the operation of the node. Specifically, $ED = <ID_R, OP, rand, seq>$ where ID_R is the identity of R. 'OP' stands for the performed operation such as data reading, writing or updating. 'seq' is a sequence number which is initialized to 1 and will be increased by one after each operation. '$rand$' is a random number generated by the tag. When the tag is requested by the next node R_n, ED will be included in $AUTH\_R = <ID_T, ID_{R_n}, OP_n, ED, \varpi>$ and sent to the tag's organization O_T by R_n. Specifically, $\varpi = E_k(Hash(ED))$ which is obtained by first hashing ED as $Hash(ED)$ and then encrypting $Hash(ED)$ by key k, where k is the symmetric key shared by T and O_T. Once receiving $AUTH\_R$, O_T firstly verifies ϖ. If the received $AUTH\_R$ pass the verification, O_T will then obtain R's operation from ED and determine R's behavior as follows. Obviously, R's behavior, either normal or malicious, can be observed accurately since each operation of R will be sent to O_T.
  (a) *normal* behaivor is detected, if node R only performs operation permitted by O_T.
  (b) *fault* behaivor is detected, if node R performs unpermitted operation occasionally probably due to its random breakdown. This kind of *fault* behaivor such as data dropping or injection may not be allowed by O_T but won't do harm to T.

(c) *malicious* behaivor is detected, if node R performs operation strictly prohibited by O_T such as compeletly wipe data.

- ***Node's State Determination***
  After obtaining R' behaviors from different organiztions, RMC can determine node R's state according to R's 'Major Behavior'. The 'Major Behavior' is the behavior which occurs most frequently. For example, if the *malicious*, *fault* and *normal* behavior occurs 6, 4 and 2 times during 10 min, the 'Major Behavior' is *malicious*. According to Table 1, we then find that the status of R is *Attacked* .

Table 1. Node state based on its major behavior

Behavior	Status
Normal	*Good*
Fault	*Temporary breakdown*
Malicious	*Attacked*

- ***Node's Reputation Evaluation***
  Once obtaining the state of R, RMC can compute R's reputation p_R. If the state of R is good, p_R will be updated to the maximum reputation value p_0, where p_0 denotes the initialization reputation value of a node. Or else, if R is in temporary breakdown or even attacked states, p_R will be reduced to $\zeta * p_0$ or even 0. Specifically, ζ is an impact factor affecting the reputation of a breakdown node, where $0 < \zeta \leq 1$.

4 Simulation

In this section, we implement RES-N in a network covering over 1000*800 square meters. There are one RMC, 3 organizations, 30 tags and a large number of nodes. The moving speed of each node is 3 m/s. The available communication distance between a node and a tag is less than 30 m. The maximum communication distance between two nodes is 150 m. Both the reputation of a node and an organization are initialized to 1.

Figure 1 shows how the moving speed of tags affects the number of attacked nodes being detected for RES-N. We set that 30% of the nodes has been attacked. Each organization deploys 100 readers and 5 tags. We can observe from Fig. 1 that the number of attacked nodes being detected grows over time. This is because tags can encounter more readers and then capture the readers' behavior over time with a high possibility.

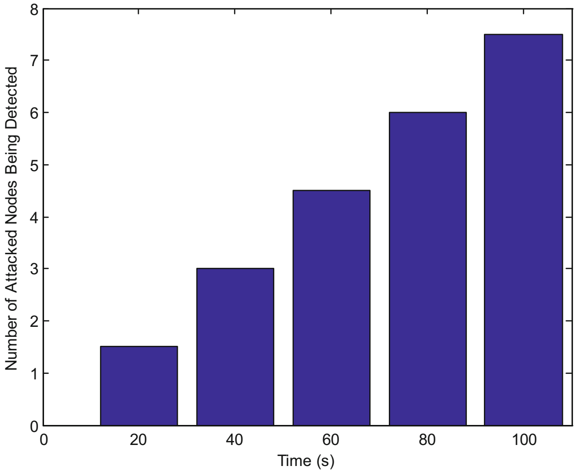

Fig. 1. Number of attacked nodes being detected over time

5 Conclusion

In this paper, we studied the trust issues in the IoT. In order to provide a general framework for trust management in IoT, we firstly design LTrust, a layered trust model for IoT. Then, a Reputation Evaluation Scheme for the Node (RES-N) and an a Reputation Evaluation Scheme for the Organization (RES-O) have been presented. The efficiency of RES-N and ORES is valided by the simulation results.

Acknowledgement. This research is supported in part by the Natural Science Foundation of China under grants No. 61300188 and 61601221; by the Fundamental Research Funds for the Central Universities No. 3132016024 and No. 3132017129; by Scientific Research Staring Foundation for the Ph.D in Liaoning Province No. 201601081; by Scientific Research Projects from Education Department in Liaoning Province No. L2015056.

References

1. Chen, R., Bao, F., Chang, M.J., et al.: Dynamic trust management for delay tolerant networks and its application to secure routing. IEEE Trans. Parallel Distrib. Syst. **25**, 1200–1210 (2014)
2. Cho, J.H., Swami, A., Chen, R.: Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks. J. Netw. Comput. Appl. **35**, 1001–1012 (2012)
3. Sicari, S., Rizzardi, A., et al.: Security, privacy and trust in Internet of Things: the road ahead. Comput. Netw. **76**, 146–164 (2015)
4. Nitti, M., Girau, R., Atzori, L.: Trustworthiness management in the social Internet of Things. IEEE Trans. Knowl. Data Eng. **26**, 1253–1266 (2014)

5. Ganeriwal, S., Balzano, et al.: Reputation-based framework for high integrity sensor networks. ACM Trans. Sens. Netw. (TOSN) **4** (2008)
6. Hellaoui, H., Bouabdallah, A., et al.: TAS-IoT: trust-based adaptive security in the IoT. In: IEEE 41st Conference on Local Computer Networks, pp. 599–602 (2016)
7. Bernabe, J.B.: Ramos, et al.: TACIoT: multidimensional trust-aware access control system for the Internet of Things. Soft Comput. **20**, 1763–1779 (2016)