8-2019

Trust architecture and reputation evaluation for internet of things

Juan CHEN

Zhihong TIAN

Xiang CUI

Lihua YIN

Xianzhi WANG
Singapore Management University, xzwang@smu.edu.sg

Citation

CHEN, Juan; TIAN, Zhihong; CUI, Xiang; YIN, Lihua; and WANG, Xianzhi. Trust architecture and reputation evaluation for internet of things. (2019). *Journal of Ambient Intelligence and Humanized Computing*. 10, (8), 3099-3107.

Available at: https://ink.library.smu.edu.sg/sis_research/5144

Journal of Ambient Intelligence and Humanized Computing (2019) 10:3099–3107
https://doi.org/10.1007/s12652-018-0887-z

ORIGINAL RESEARCH

Trust architecture and reputation evaluation for internet of things

Juan Chen[1] · Zhihong Tian[1] · Xiang Cui[1] · Lihua Yin[1] · Xianzhi Wang[2]

Received: 23 January 2018 / Accepted: 30 March 2018 / Published online: 4 June 2018

Abstract

Internet of Things (IoT) represents a fundamental infrastructure and set of techniques that support innovative services in various application domains. Trust management plays an important role in enabling the reliable data collection and mining, context-awareness, and enhanced user security in the IoT. The main tasks of trust management include trust architecture design and reputation evaluation. However, existing trust architectures and reputation evaluation solutions cannot be directly applied to the IoT, due to the large number of physical entities, the limited computation ability of physical entities, and the highly dynamic nature of the network. In comparison, it generally requires a general and flexible architecture to manage trust in such a dynamic environment as IoT. In this paper, we present IoTrust, a trust architecture that integrates Soft Defined Network (SDN) in IoT, and a cross-layer authorization protocol based on IoTrust. IoTrust and the protocol together provide a new insight for research on trust management in the IoT. For trust establishment, we further propose a Behavior-based Reputation Evaluation Scheme for the Node (BES) and an Organization Reputation Evaluation Scheme (ORES). Both our theoretical analysis and simulation results validate the efficiency of BES and ORES.

Keywords Internet of things · Sensors · Trust architecture · Reputation evaluation

1 Introduction

Internet of Things(IoT) creates a world where physical entities are seamlessly integrated into information networks to provide advanced and intelligent services for human beings (Alrawais et al. 2017; Guo et al. 2017; Dabbagh and Rayes 2017). The IoT entities generally include sensor nodes, RFID tags and wireless communicating devices (e.g. readers, mobile phones) connected to the Internet in a smart environment (Memos et al. 2017; Sedjelmaci et al. 2017). The proliferation of IoT greatly empowers people to control their lives. Generally, a tag is attached to an object and can only communicate with a reader nearby. Until now, a huge number of readers deployed by business or government organizations to provide service for commercial or public use (Yan et al. 2014).

Since physical entities including readers, tags and various application servers in IoT need to collaborate with each other, it is important for them to identify the trustworthy partners.

Despite the wide use of trust protocols for P2P (Chen et al. 2014; Cho et al. 2012) and ad hoc sensor networks (Ganeriwal et al. 2008; Jiang et al. 2015), there is little work on trust management for IoT (Sicari et al. 2015). Reputation is a concept closely related to trust relations and has been widely used in many knowledge domains ranging from social sciences to digital sciences. In fact, reputation is often seen as one measure by which trust or distrust can be built based on good or bad past experiences and observations based on collected referral information. In recent years, the concept of reputation has proven useful in many areas of research in computer science, particularly in the context of distributed and collaborative systems where trust and security issues are critical. We summarize the main challenges of trust management for IoT as follows. First, traditional trust management solutions cannot be simply and directly applied to the IoT due to the different standards, communication stacks, and weak computation ability of entities (Shen et al. 2018; Li et al. 2018; Gao et al. 2018; Liu et al. 2017). Second, most works about trust in IoT systems are designed for specific applications and

✉ Zhihong Tian
tianzhihong@gzhu.edu.cn

[1] The Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou 510006, China

[2] Living Analytics Research Centre, Singapore Management University, 80 Stamford Road, Singapore 178902, Singapore

therefore cannot be applied to other applications (Chen et al. 2016; Jayasinghe et al. 2016; Nitti et al. 2014). Third, IoT has a huge number of heterogeneous entities with limited storage space and computation resources while existing work does not scale well to accommodate this requirement (Nitti et al. 2014). Fourth, IoT represents a dynamic environment which evolves with new nodes joining and existing nodes leaving. Thus, it requires a flexible infrastructure to allow newly joining nodes to build up trust quickly with a reasonable degree of accuracy. Lastly, they are dependent on specific assumptions such as the availability of feedback and known ownership (Hellaoui et al. 2016; Bernabe et al. 2016).

We aim to design a scalable and general trust management framework for IoT to address the above challenges. To this end, we first present a general trust architecture integrating Soft Defined Network (SDN), an emerging technology that can meet the need of current IoT requirements of heterogeneity and flexibility (Kuang et al. 2016). Then, we present a cross-layer authorization protocol based on the architecture and two reputation evaluation schemes for the node and organization, respectively. In a nutshell, we make the following contributions in this paper:

- We present IoTrust, a trust architecture integrating SDN for IoT, which consists of the object layer, the node layer, the SDN control layer, the organization layer, and the reputation management layer. Since the SDN control layer decouples the control functionality from the data routing and processing, IoTrust facilitates optimization and configuration of a network in an efficient and automated manner and provides interoperability among heterogeneous IoT network. The general and flexible infrastructure can be applied to various types of applications to solve the scalability issues in a dynamic IOT environment.
- We present a cross-layer authorization protocol based on IoTrust. Specifically, only the reader authorized by the tag related organization can access to the tag. Moreover, the reader's operations on the tag will be recorded for the node's reputation evaluation.
- We present a Behavior-based Reputation Evaluation Scheme for the Node (BES) and an Organization Reputation Evaluation Scheme (ORES). Based on the node's behavior, BES decides the node's state by which node's reputation is evaluated. Then, ORES evaluates the organization's reputation based on all its nodes' current states. The theoretical analysis supports our simulation results, indicating the efficiency of BES and ORES.

The rest paper is organized as follows. Section 2 introduces typical trust management work in IoT. We then present the soft-defined trust architecture with a cross-layer authorization protocol in Sect. 3. Section 4 proposes reputation evaluation schemes for node and organization in details followed by the performance evaluation. The simulation is given in Sect. 5. Finally, we conclude the paper in Sect. 6.

2 Related work

There are two approaches for trust in computer networks: the first based on policies. For example, SPINS (Perrig et al. 2002), develops a trusted network. The second approach is based on reputation (Chen et al. 2014; Cho et al. 2012), which is defined as a probability that an agent is trustworthy.

In recent years, the concept of reputation has shown itself to be useful in many areas of research in computer science particularly in the wireless body area networks, cloud computing (Wu et al. 2016, 2014; Huang et al. 2017), and social networks (Yuan et al. 2017; Chen et al. 2017; Shen et al. 2015), where interesting issues of trust and security manifest themselves.

Despite active research efforts in the related topics (Ganeriwal et al. 2008; Jiang et al. 2015), few researchers focus on the trust management in the context of the IoT. In fact, reputation is often seen as one measure by which trust or distrust can be built based on good or bad past experiences and observations (Chen et al. 2016; Raya et al. 2008) or based on collected referral information (Bernabe et al. 2016; Hellaoui et al. 2016; Jayasinghe et al. 2016).

Chen et al. 2016 proposed a trust management framework for service oriented architecture (SOA) based IoT systems. Trust is based on entities' previous interactions and experiences. It uses distributed collaborative filtering to select trust recommendations. It dynamically adjusts the protocol's parameters for different environments. Also, it considers four types of malicious attacks. Jayasinghe et al. (2016) propose a novel trust computational model based on three trust metrics (TMs); Knowledge, Recommendations, and Reputations for Social Internet of Things. However, both (Chen et al. 2016) and (Jayasinghe et al. 2016) are designed for specific applications, e.g. service provision.

Jorge (Bernabe et al. 2016) focused on the trust control technologies. Hellaoui (Hellaoui et al. 2016) presented an efficient adaptive security model for the IoT. It allows evaluating the trust related to the presence of security threats and performing, consequently, adaptive security decisions. Both (Hellaoui et al. 2016) and (Bernabe et al. 2016) are dependent on specific assumptions, such as feedback must be available, ownership is known, and so on. Raya et al. (2008) evaluates data reports with corresponding trust levels using Bayesian inference. However, Bayesian inference depends on prior knowledge about events which may be unavailable.

Other related work either does not scale well or falls unsuitable for dynamic Soft-defined IoT network (Nitti et al. 2014). Thus, trust management for Soft-defined IoT remains an open issue.

3 Trust architecture with a cross-layer authorization protocol

We first present IoTrust, a trust architecture integrating SDN for IoT according to different functions of entities. Then, a cross-layer authorization protocol is proposed based on IoTrust. IoTrust with the cross-layer authorization protocol provides new insights for research on trust-based interaction in IoT. This is because our soft-defined trust architecture enables trust relationship establishment among highly dynamic entities managed by different organizations.

3.1 IoTrust

There are five types of entities: tag-attached objects or tags, nodes, controllers, organizations and the RMC (Reputation Management Center). According to the functions of different entities, IoTrust divides the IoT into five layers including the object layer, the node layer, the SDN control layer, the organization layer and the reputation management layer. Figure 1 shows the bottom object layer consists of a large number of moving tag-attached objects. Before joining the IoT, each tag or object must choose and then register with an organization. This layer is the data source. Above the object layer is the node layer which consists of different kind of nodes such as readers, sensors and so on. This layer manages data collection from the object layer. Specifically, nodes retrieve data from nearby tags and then return the required results to the organization layer. The SDN control layer lies between the node layer and the organization layer. This layer can program the bottom node network to react differently depending on the nature of the node, its potential for maliciousness, and the resources it requires. Moreover, this layer is in charge of predicting network traffic and implement mobility management in the IoTrust architecture. Specifically, controllers in this layer should be carefully deployed and designed according to their different functions such as flow scheduling, mobility management and so on. The organization layer is composed of different commercial or government organizations. Each organization deploys a certain number of nodes to perform operations on tags such as data retrieval. Since IoT is spread across a large area which can not be covered by nodes from one organization, it is necessary for different organizations and nodes to cooperate with each other. However, a malicious node or an organization among good ones can launch different attacks after the node gains access to the tag, thereby severely damage the network. In order to identify the good nodes and organizations from malicious ones, reputation is used to measure how good the node or organization is. IoTrust thus evaluates the reputation of each node and organization by the reputation evaluation schemes introduced in Sect. 4 by RMC on the top reputation management layer. The tag related organization will grant the authorization to the good node which receives an operation request from good organization. The authorization protocol will be introduced in the following subsection.

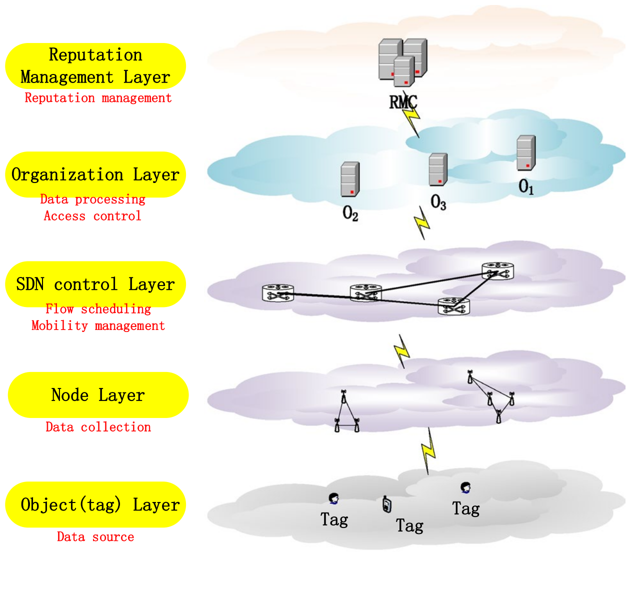

Fig. 1 Five-layer IoTrust architecture

3.2 Cross-layer authorization protocol

The cross-layer authorization protocol is used to authorize the good node to access to the tag. The node can interact with the tag directly if it stays within the tag's communication range. Note that only the node authorized by the tag related organization can be trusted by the tag. Therefore, before accessing to the tag, the node must obtain the authorization from the tag related organization. The tag related organization decides whether or not to authorize the node's access according to the node's reputation and the user registered organization's reputation. The reputation evaluation for nodes and organizations will be introduced in Sect. 4.

The main idea of the cross-layer authorization protocol is shown in Fig. 2. Specifically, the cross-layer authorization protocol performs the following nine steps.

1. The user sends a request to the user related organization O_U for the specified operation on a tag-attached object known as the target tag.
2. The organization O_U sends the request message $INFO\_REQ =< ID_U, ID_T, O_{per} >$ which will then be broadcasted to the node layer, where ID_U, ID_T and O_{per} stand for the ID of O_U, the ID of the target tag T and the requested operation.
3. The node R which discovers that the target tag T stays within its communication range is the target node. R will send $INFO\_REQ$ to T for accessing request.

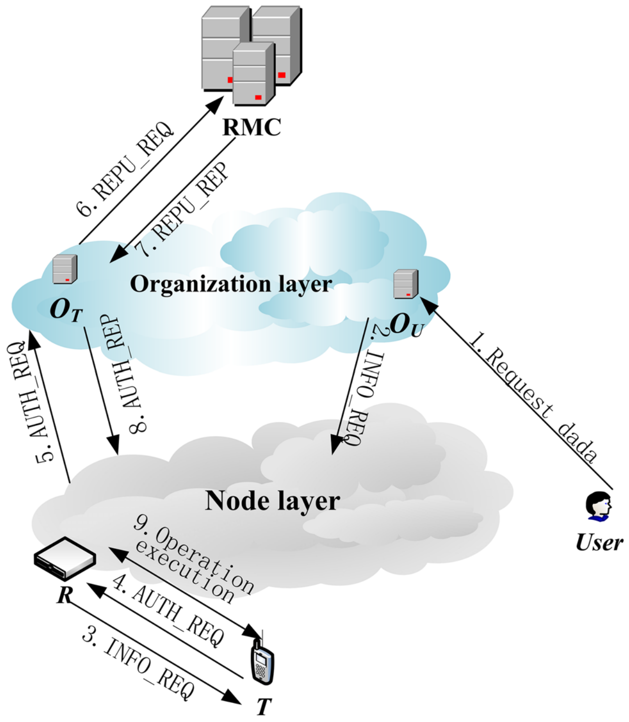

Fig. 2 Cross-layer authorization process

4. The tag T replies R with an authorization request message $AUTH\_REQ$ including ID_T and ID_{OT}, where ID_{OT} is the ID of the tag-related organization.
5. Target node R sends $AUTH\_REQ$ to O_T through the node layer and SDN control layer.
6. The tag related organization O_T interacts with the RMC to obtain R's and O_U's reputation. Specifically, O_T sends the $REPU\_REQ$ to the RMC for reputation request.
7. RMC replies O_T with the message $REPU\_REP$ including R's and O_U's reputation.
8. The organization O_T determines whether R should be granted access to T. If both R's reputation and O_U's reputation meet O_T's requirements, O_T gives R the authorization and responses R with an authorization message $AUTH\_REP$.
9. After being authorized, R can perform operations on T.

    - Once authorized, R can perform either a good or a malicious operation. For safety consideration, the attacked nodes that often perform malicious operations should be prevented from accessing to tags. However, it is difficult for a tag to defend against the attacked node. On the one hand, a tag usually has limited energy. On the other hand, a malicious operation may be performed by either an attacked node or (occasionally) an unattacked node in case of a temporary breakdown as it is impractical for a tag with limited computation capability to identify an attacked node from a node in temporary breakdown. Therefore, we choose the RMC with powerful energy and computational ability to identify the attacked node according to its reputation. Each node's reputation is determined by its previous behavior such as its operations on different tags.

4 Reputation evaluation schemes

For safety consideration, attacked nodes must be identified and then prevented from accessing to the tag. Different from unattacked nodes, attacked nodes usually perform a malicious behavior. So, we identify an attacked node according to its behavior which is measured by its reputation. We then propose a Behavior-based reputation Evaluation Scheme (BES) for nodes in Sect. 4.1. Furthermore, an Organization Reputation Evaluation Scheme (ORES) will be introduced in the following Sect. 4.2.

4.1 Behavior-based reputation evaluation scheme for nodes

Based on the node's behavior, BES decides the node's state by which node's reputation is evaluated (See Fig. 3). Firstly, tag T in the object layer records evidence ED which includes the operations performed by reader R. Then, when interacting with the next node, T will include ED as part of the message which will be sent to O_T by the node. After that, O_T determines and then submits R's behaviors to RMC. Finally, RMC updates R's reputation by R's state which can be determined by R's behaviors at regular intervals. In all, the node reputation evaluation process includes node behavior verification, node state verification, and node reputation evaluation. Specifically, BES consists the following three steps as described in Algorithm 1.

- *Node's behavior determination based on evidence* Before performing operations on a tag T, the node R must be authorized by the tag's organization O_T. Thus, R sends an authorization request message $AUTH\_REQ$ to O_T. Once being authorized, the node can have the right to do the operation on the tag. When the operation is completed, the tag will generate an evidence ED which is used to record the operation of the node. Specifically, ED=$< ID_R, OP, seq, rand >$ where ID_R is the ID of the node. 'OP' is the performed operation such as reading, writing or deleting data. '$rand$' is a random number generated by the tag. 'seq' is a sequence number which is initialized to 1 and will be increased by one after each operation. When the tag is requested by the next node R', ED will then be sent to the tag's organization O_T by R' as part of $AUTH\_REQ$=$< ID_T, ID_{R'}, OP', ED, \varphi >$. Spe-

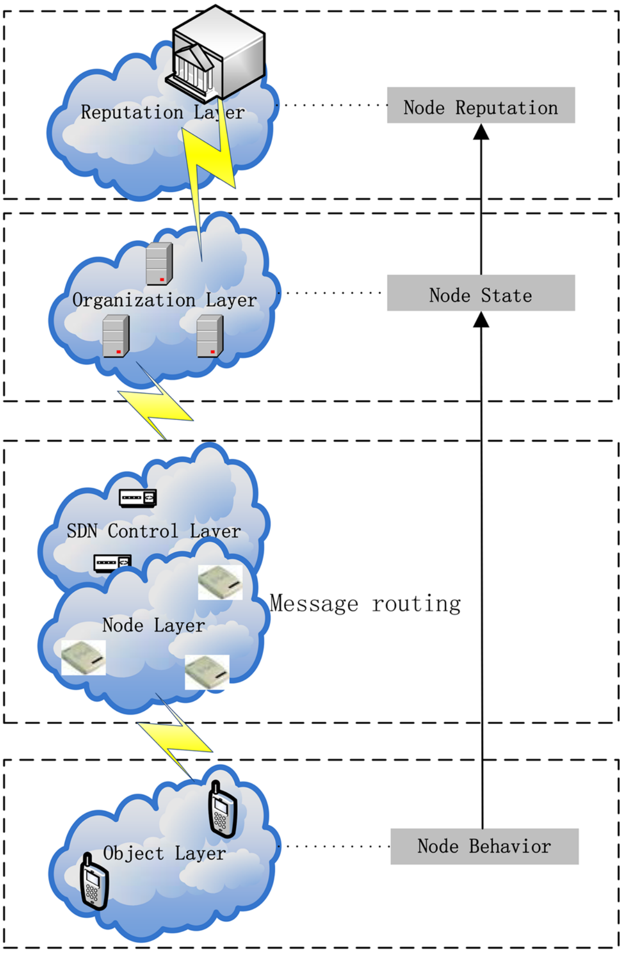

Fig. 3 Three steps for node reputation evaluation

cifically, φ=$E_k(H(ED))$ which is obtained by first hashing ED as $H(ED)$ and then encrypting $H(ED)$ by key k, where k is the symmetric key shared by T and O_T. Once receiving $AUTH\_REQ$, O_T will verify φ by calculating $E_k(H(ED))$ firstly and then comparing $E_k(H(ED))$ with the φ. If the received $AUTH\_REQ$ pass the verification, O_T will obtain R's operation from ED and determine R's behavior as follows.

1. Node R performs *normal* behaivor if it only does operation permitted by O_T.
2. Node R performs *fault* behavior if it does unpermitted operation probably due to its random breakdown. This kind of *fault* behavior such as data dropping or injection may not be allowed by O_T but won't do harm to T.
3. Node R performs *malicious* behavior if it does operation strictly prohibited by O_T such as complete data wiping.

Table 1 Node state based on its major behavior

Behavior	State
Normal	Good
Fault	Temporary breakdown
Malicious	Attacked

Obviously, R's malicious behavior can be captured accurately since each operation executed by R will be sent to O_T.

- *Node's state determination* RMC will determine node R's state according to the 'Major Behavior' during a fixed period of time since RMC can obtain each behavior of R from different organizations. The 'Major Behavior' is the behavior which occurs most frequently. For example, if the *normal*, *fault* and *malicious* behavior occur 2,4 and 6 times during 10 min, the 'Major Behavior' is *malicious*. We then have that the state of R is *Attacked* according to Table 1.
- *Node's reputation evaluation* After obtaining the state of R, namely P_R, RMC will compute R's reputation p_R according to Algorithm 1. Specifically, if R is in a good state, P_R will be updated to the maximum reputation value p_0, where p_0 is the initialization reputation value of a node; otherwise, if R is being temporarily breakdown or attacked, P_R will be reduced to $\alpha * p_0$ or the lowest value 0. The parameter α is an impact factor affecting the reputation of breakdown node, where $0 < \alpha \leq 1$.

```
Algorithm 1 Node's Reputation Evaluation
Input: $\Upsilon_1, \Upsilon_2, \Upsilon_3$ //$\Upsilon_1$ is the number of times the normal behaviors occur. $\Upsilon_2$ is the number
    of times the fault behaviors occur.$\Upsilon_3$ is the number of times the malicious behaviors
    occur.
Output: $P_R$ //$P_R$ is the current reputation of node $R$
behavior=$argmax\{\Upsilon_i | i = 1, 2, 3\}$
    // Node state determination
if $behavior$ == 1 then
    State=good
else if $behavior$ == 2 then
    State=temporary breakdown
else
    State=attacked
end if
    // Node reputation computation
if State==good then
    $p_R$= $p_0$
else if State==temporary breakdown then
    $p_R$= $\alpha * p_0$
else
    $p_R$=0
end if
return $p_R$
```

4.2 Organization reputation evaluation scheme

Before joining in the network, an organization requests for a certificate from RMC and then it can be trusted by other organizations as well as the RMC. Since the number of organizations is far less than that of nodes or tags, the computation or storage cost for reputation evaluation of an organization won't cause too much burden to RMC. Specifically, the organization's reputation Φ will be calculated at regular intervals based on all its nodes' current state. Given that there are N_{total} nodes deployed by the organization. The number of good, attacked and breakdown nodes are N_{good}, $N_{attacked}$ and $N_{breakdown}$. The reputation of the organization will be computed according to Eq. (1). Specifically, Φ_0 is the initialization reputation value of an organization. β and τ are reputation decay factors for an attacked and breakdown node respectively, where $0 < \beta, \tau \leq 1$ and $\beta < \tau$.

$$\Phi = \left(N_{good} \backslash N_{total} + \beta N_{attacked} \backslash N_{total} + \tau N_{breakdown} \backslash N_{total}\right)\Phi_0. \tag{1}$$

4.3 Performance analysis

We use the detection accuracy of abnormal (malicious and fault) behavior to measure the performance of BES and ORES. In particular, the evidence *ED*'s protection level including integrity, authenticity, freshness, and non-repudiation is chosen to measure the detection accuracy of abnormal behavior. This is because each node's behavior is recorded in each evidence, based on which BES and ORES evaluate the reputation of nodes and organizations. Therefore, only when the security of the evidence *ED* is guaranteed, BES and ORES are effective. The evidence will be verified by the tag's organization as described in the following Algorithm 2.

Algorithm 2 The verification of the evidence security

```
Input: $\Upsilon_1, \Upsilon_2, \Upsilon_3$ //$\Upsilon_1$ is the number of times the normal behaviors occur. $\Upsilon_2$ is the number
    of times the fault behaviors occur.$\Upsilon_3$ is the number of times the malicious behaviors
    occur.
Output: $P_R$
        //obtain the key shared between tag $T$ and $O_T$
        //$key[T]$ is the symmetric key shared between $T$ and $O_T$
k = key[T]
d = hash(ED)
        // check if the evidence '$ED$' has been modified
        // $E_k(d)$ denotes the ciphertext obtained by encrypting $d$ under key $k$
if $E_k(d) \neq \varphi$ then
    return INVALID
end if
        //check if the received random number 'rand' has ever been used
        //$T.rand$ records all random numbers accepted from $T$
if $'rand' \in T.rand$ then
    return INVALID
end if
        //check if some evidence has been maliciously dropped
        //$T.seq$ is the previous sequence number of $T$ stored in $O_T$
if $seq \neq T.seq + 1$ then
    return INVALID
else
    $T.seq = seq$
    Add(rand, T.rand) // add the random number 'rand' into $T.rand$
    return VALID
end if
```

Specifically, both BES and ORES are capable of thwarting three types of attacks to ensure the integrity, authenticity, freshness, and non-repudiation of *ED* according to the following analysis.

- BES and ORES can defend against the modification attack and protect *ED*'s integrity and authenticity. This is because the organization O_T can discover *ED*'s modification by checking $\varphi = E_k(H(ED))$ according to Sect. 4.1.
- BES and ORES can defend against the replay attack and thus *ED*'s freshness is preserved. This is because the replayed *ED* can be verified if the '*rand*' which is a unique identifier is a previously used one.
- BES and ORES can defend against the message dropping attack and ensure the non-repudiation of *ED*. The organization O_T can verify that *ED* is discarded if $seq \neq T.seq$ $+1$, where '*seq*' and '$T.seq$' are sequence numbers included in two consecutive evidences received from the same tag.

5 Simulation results

In this section, we apply our trust architecture and reputation schemes to the IoT system covering over 1000 × 800 m^2. The system includes one RMC, 3 organizations, 30 tags and a large number of nodes. In order to be tracked by authorized users, each tag has to register at one organization. All tags are moving at a speed of 3 m/s in the network. Each organization deploys its own nodes in areas where it requests data frequently. The available communication distance between a node and a tag is no more than 30 m. The maximum communication distance between two nodes is 150 m. Both the reputation of an organization and a node are initialized to 1.

Figures 4 and 5 show the effect of different node densities on the organization reputation evaluated by ORES and Bayes-based method (Raya et al. 2008). Given that the node density η is the number of nodes which are able to listen to the communication between a tag and a node on average.

We can observe from Fig. 4 how the organization reputation changes over time when the node density is low. Each organization deploys and manages 30 nodes and thus the node density is $\eta = 0.32$. Fifty percent of nodes has been attacked. Both ORES and Bayes-based method evaluate the organization reputation by the number of attacked nodes being detected. Then we have that the more accurate the detection result is, the more accurate the organization reputation is. It is observed that the organization reputation for ORES decreases over time as the number of detected attacked nodes grows. This is because ORES is able to detect the attacked nodes successfully by their malicious behaviors recorded in evidence. That evidence will be successfully transmitted to the tag related organization. We can also observe that after a period of time which

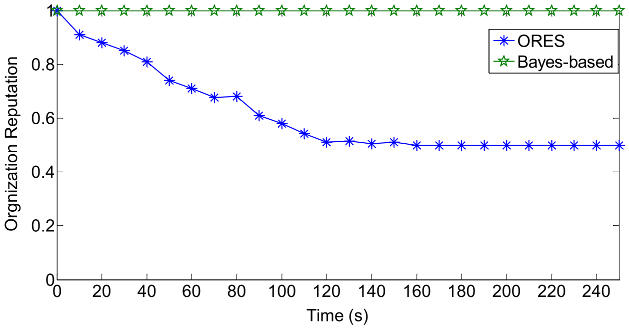

Fig. 4 Organization reputation changes over time under low node density

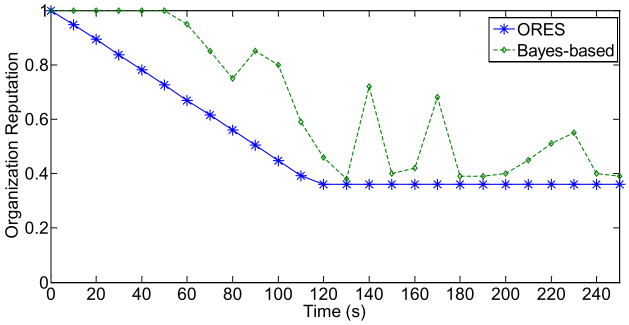

Fig. 5 Organization reputation changes over time under high node density

is 120 s in Fig. 4, the organization reputation for ORES becomes stable. After 120 s, all attacked nodes (45 nodes) have been detected. Different from ORES, the organization reputation for the Bayes-based method keeps unchanged since attacked nodes cannot be detected. In the Bayes-based method, the communication between a node and a tag can hardly be monitored by another node if nodes are sparsely deployed. So the node's behavior (whether good or malicious) during the communication process cannot be observed by any other node. It is obvious that ORES outperforms the Bayes-based method with a low node density deployment.

Figure 5 shows how the organization reputation changes over time when the node density is high. Each organization deploys 100 nodes, 80% of which is attacked. Other parameters' setting is the same as Fig. 4. It can be seen that the organization reputation decreases over time for ORES and Bayes-based method overall. Take note that the organization reputation for Bayes-based fluctuates greatly. This is because ORES can detect each malicious behavior while Bayes-based method cannot. Specifically, for the Bayes-based method, the communication process between a node and a tag will be missed, if no other node within the communication range of the node and the tag. Thus, ORES can detect attacked nodes with a higher probability than the Bayes-based method even in a high node density network. In all, ORES can detect attacked nodes with a higher probability whether in a low or high node density network.

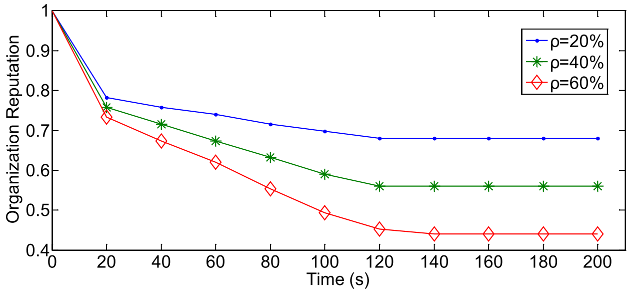

Fig. 6 The effect of the percentage of attacked nodes

We can observe from Fig. 6 how the organization reputation changes with different ρ, where ρ is the percentage of attacked nodes. Each organization deploys 100 nodes, each of which is attacked or breakdown. Figure 6 illustrates that the organization reputation decreases over time since more attacked nodes and temporary breakdown nodes have been detected. We can further observe that as ρ decreases, the organization reputation decreases obviously. The results show clearly that the number of attacked nodes has a more significant impact on the organization reputation than that of temporary breakdown nodes. This is because temporary breakdown nodes may recover and can then return to a normal state while attacked nodes cannot. Thus, the more attacked nodes the organization owns, the lower the organization reputation is.

Figure 7 shows how the moving speed of tags affects the number of detected attacked nodes for BES. In this simulation, we set that 30% of the nodes has been attacked. Each organization deploys 100 readers and 5 tags. It can be seen from Fig. 7 that the number of attacked nodes being detected increases with the growth of the speed of tags. This is because tags can encounter readers frequently and then capture the readers' behavior with a high possibility if tags are moving quickly.

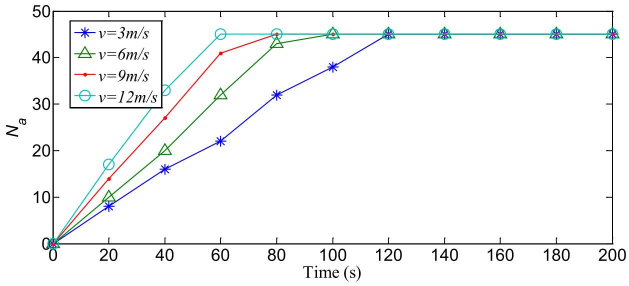

Fig. 7 The effect of moving speed of the tag

6 Conclusion

In this paper, we have presented a trust architecture integrating SDN, called IoTrust, with a cross-layer authorization protocol. IoTrust can be applied to various types of applications to solve the scalability issue in an IoT dynamic environment. In addition, we propose two reputation evaluation schemes for node and organization, respectively. Theoretical analysis shows that the proposed reputation evaluation schemes can defend against modification attack, replay attack, and message dropping attack and achieve higher detection accuracy of attacked nodes. Simulation results support our theoretical analysis and validate the efficiency of the proposed reputation evaluation schemes.

Our future work includes extension and further validation of the proposed techniques to address the remaining challenges in the trust management for IoT. For example, we will enhance the proposed model to adapt our reputation architecture and its reputation schemes to other IoT protocols. Another important research direction is the detection of malicious user and organization behaviors. Typically, such a malicious behavior could be the collusion across those entities with the aim of generating fake reputation values for a targeted node. Other promising directions include designing a mechanism for managing reputation for RMC and exploring how variations in the presence ratio of ill-behaved and well-behaved entities would lead to a notion of reputation reflecting the wider system.

Acknowledgements This research is supported in part by the Natural Science Foundation of China under Grants No. 61572153 and No. 61702223; 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.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

References

Alrawais A, Alhothaily A, Hu C, Cheng X (2017) Fog computing for the internet of things: security and privacy issues. IEEE Internet Comput 21(2):34–42

Bernabe JB, Ramos JLH, Gomez AFS (2016) Taciot: multidimensional trust-aware access control system for the internet of things. Soft Comput 20(5):1763–1779

Chen R, Bao F, Chang MJ, Cho J-H (2014) Dynamic trust management for delay tolerant networks and its application to secure routing. IEEE Transa Parallel Distrib Syst 25(5):1200–1210

Chen R, Guo J, Bao F (2016) Trust management for soa-based iot and its application to service composition. IEEE Trans Serv Comput 9(3):482–495

Chen Z, Peng L, Gao C, Yang B, Chen Y, Li J (2017) Flexible neural trees based early stage identification for ip traffic. Soft Comput 21(8):2035–2046

Cho JH, Swami A, Chen R (2012) Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks. J Netw Comput Appl 35(3):1001–1012

Chongzhi G, Xuan L, Shibing X (2018) Cloud-assisted privacy-preserving profile-matching scheme under multiple keys in mobile social network. Cluster Comput. https://doi.org/10.1007/s10586-017-1649-y

Dabbagh M, Rayes A (2017) Internet of things security and privacy. In: Rayes A, Salam S (eds) Internet of things from hype to reality. Springer, pp195–223

Ganeriwal S, Balzano LK, Srivastava MB (2008) Reputation-based framework for high integrity sensor networks. ACM Trans Sensor Netw (TOSN) 4(3):15

Guo J, Chen R, Tsai JJP (2017) A survey of trust computation models for service management in internet of things systems. Comput Commun 97:1–14

Hellaoui H, Bouabdallah A, Koudil M (2016) Tas-iot: trust-based adaptive security in the iot. In: Local Computer Networks (LCN), 2016 IEEE 41st Conference on

Huang H, Guo S, Wu J, Li J (2017) Service chaining for hybrid network function. IEEE Trans Cloud Comput. https://ieeexplore.ieee.org/document/7962178/

Jayasinghe U, Truong NB, Lee GM, Um T-W (2016) Rpr: a trust computation model for social internet of things. In: Ubiquitous intelligence & computing, advanced and trusted computing, scalable computing and communications, cloud and big data computing, internet of people, and smart world congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld, 2016 Intl IEEE Conferences

Jiang J, Han G, Wang F, Shu L, Guizani M (2015) An efficient distributed trust model for wireless sensor networks. IEEE Trans Parallel Distrib Syst 26(5):1228–1237

Kuang L, Yang LT, Qiu K (2016) Tensor-based software-defined internet of things. IEEE Wirel Commun 23(5):84–89

Li J, Zhang Y, Chen X, Xiang Y (2018) Secure attribute-based data sharing for resource-limited users in cloud computing. Comput Secur 72:1–12

Liu Q, Wang G, Li F, Yang S, Jie W (2017) Preserving privacy with probabilistic indistinguishability in weighted social networks. IEEE Trans Parallel Distrib Syst 28(5):1417–1429

Memos VA, Psannis KE, Ishibashi Y, Kim B-G, Gupta BB (2017) An efficient algorithm for media-based surveillance system (eamsus) in iot smart city framework. Future Gen Comput Syst 83:619–628

Nitti M, Girau R, Atzori L (2014) Trustworthiness management in the social internet of things. IEEE Trans Knowl Data Eng 26(5):1253–1266

Perrig A, Szewczyk R, Tygar JD, Wen V, Culler DE (2002) Spins: security protocols for sensor networks. Wireless Netw 8(5):521–534

Raya M, Papadimitratos P, Gligor VD, Hubaux J-P (2008) On data-centric trust establishment in ephemeral ad hoc networks. In: INFOCOM 2008. The 34th Conference on Computer Communications. IEEE

Sedjelmaci Hichem, Senouci SM, Taleb T (2017) An accurate security game for low-resource iot devices. IEEE Trans Vehr Technol 66(10):9381–9393

Shen H, Gao C, He D, Wu L (2015) New biometrics-based authentication scheme for multi-server environment in critical systems. J Ambient Intell Hum Comput 6(6):825–834

Shen J, Gui Z, Ji S, Shen J, Tan H, Tang Y (2018) Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. J Netw Comput Appl 106:117–123

Sicari S, Rizzardi A, Grieco LA, Coen-Porisini L (2015) Security, privacy and trust in internet of things: the road ahead (2015). Comput Netw 76:146–164

Wu J, Igor B, Chris G, Hossain E, Massimo V, Haibo L (2014) Context-aware networking and communications: : part 1 [guest editorial]. IEEE Commun Mag 52(6):14–15

Wu J, Song G, Jie L, Deze Z (2016) Big data meet green challenges: big data toward green applications. IEEE Syst J 10(3):888–900

Yan Z, Zhang P, Vasilakos AV (2014) A survey on trust management for internet of things. J Netw Comput Appl 42:120–134

Yuan C, Li X, Wu QMJ, Li J, Sun X (2017) Fingerprint liveness detection from different fingerprint materials using convolutional neural network and principal component analysis. 53(4):357–372. http://www.techscience.com/doi/10.3970/cmc.2017.053.357.pdf