Distributed Trust Management Mechanism for the Internet of Things

Jingpei Wang[1], Sun Bin[1]
[1]Information Security Center,
Beijing University of Posts and Telecommunications,
Beijing 100876, China
Email: dq2003136230@yahoo.com.cn

Yang Yu[1,2], Niu Xinxin[1,2]
[2]National Engineering Laboratory for Disaster Backup and Recovery,
Beijing University of Posts and Telecommunications,
Beijing, China

***Abstract*—Trust management provides a potential solution for the security issues of distributed networks. However, there are rare researches about the trust mechanism for IoT in the literature. A new distributed trust management mechanism for IoT is established in this paper. Firstly, we extract three basic elements- service, decision-making and self-organizing, of trust management from the investigated trust solutions. Then, based on a service model, we establish a trust management framework for the layered IoT, which is decomposed into three layers: sensor layer, core layer and application layer. Finally, we use fuzzy set theory and formal semantics-based language to perform the layered trust mechanism. The proposed trust conception, layered service model and formal method provide a general framework for the study of trust management for the IoT, and further provide a significant reference for the development of sound trust models for IoT.**

Keywords-Internet of Things; trust management; formal semantics; trust decision-making

I. INTRODUCTION

The Internet of Things (IoT) is a novel paradigm that is of considerable interest in academia and industry [1]. However, the security risk is increasing rapidly due to its openness. Trust Management aiming at solving distributed security-related issues becomes a researching spot in recent years [2].

There are rare researches on the trust management in the context of the IoT. Liu focused on the trust control technologies in IoT [3]. Their research provided guidance for the design of the future IoT, but concrete solutions should be further investigated. There had been vast researches about trust management for sensor network [4] [5], perhaps these trust solutions can be contributed to the development of trust management for IoT as the sensor network is a vital component of the IoT, but until now, no related works had been found. The establishment of trust mechanism for IoT remains an open issue.

In this paper, we will establish a trust management mechanism for IoT. We divide the IoT into three orderly layers: sensor layer, core layer, and application layer, and use a formal semantics-based language to realize the trust mechanism, the result is providing a general framework for the development of trust management for IoT. The rest of the paper is organized as follows. Section II extracts some elements of trust management from the investigated trust solutions. We present the layered model and the trust management framework for IoT in Section III. In Section IV, the detailed procedures of trust management for IoT are discussed in the formal semantics. Section V gives the discussion, followed by the conclusion in Section VI.

II. SOME ELEMENTS OF TRUST MANAGEMENT

A large number of trust solutions appeared in various distributed networks, such as P2P, Ad hoc, WSN [2][4-7].

Bahtiyar et al. [2] proposed a mechanism for extracting trust information from the security system of a service based on the needs of an entity. Trust is used as a security metric between an entity and systems. Li [6] proposed a P2P trust model. An adaptive trusted decision-making method based on historical evidences window is used to improve system efficiency. In Ad hoc network, an entropy theory based distributed trust model provided a mechanism to select trusted paths [7]. The trust value of each path is obtained through multi-layer and multi-level calculation, and someone can choose credible routes to implement the interaction. For WSN, a cluster-based layered trust scheme [5] is characterized as a typical model. Based on the trust values, a node assigns a trust state to other nodes. We can calculate the trust value of the sensor nodes at each level, and choose a set of nodes to participate in the transaction.

From above investigated trust solutions, some elements or attributes of trust management can be extracted:

Service. It defines the role of the trust management. The basic idea of trust management is that the security decision needs to rely on the additional safety information provided by a trusted third party. Trust, as a "soft" third party, provides a service for the service requester and the service provider in a network system.

Decision-making- the purpose of the trust management. Trust is collected to judge the credibility of the cooperative nodes, based on which make a decision to deliver a service [2], select a credible routing [7] and transmit a data [4].

Self-organizing. It depicts the way of the trust management. Based on trust decision, a series of nodes or even sub-networks can be selected and self-organized to perform a certain task (i.e. forwarding the packages [6], sensing the data [5]) cooperatively in network scene (i.e. IoT).

Service, decision-making and self-organizing are the three basic essential elements. Based on these attributes, we propose our definition of trust mechanism.

Definition 1 (Trust mechanism *T*). **Trust management is a service mechanism that self-organizing a set of items based on their trust status to take an informed decision.**

Published by Atlantis Press, Paris, France.

III. THE LAYERED MODEL AND THE TRUST MANAGEMENT FRAMEWORK FOR IOT

From the aspects of service, IoT is regarded as a service provider (SP). The trust management aims to provide an auxiliary service that assisting the IoT to provide more qualified service to the service requester (SR). This relationship is depicted in Fig. 1. The relationship is bidirectional as the trust mechanism has both effects on the SR (for privacy protection) and SP.

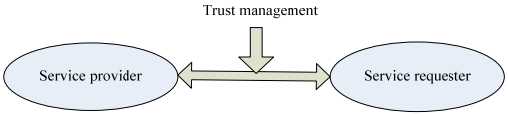

Figure 1. Service model

Considering that it is difficult to establish trust mechanism for the IoT as a whole, we will establish trust mechanisms for the layered IoT.

The layered structure is proposed based on the general application scene of IoT. With the help of IoT, an intelligent city can be able to aggregate the information coming from its infrastructures, achieving a holistic point of view that will be crucial to any decision-making processes. The sensor network perceives and gathers the surrounding information from the physical world, such as the weather, road condition and water distribution information in a desired region of the city. The collected information will be transmitted to the core network (e.g. wireless/wired access network and IP networks) after preliminary fusion and processing. At the application stage, the analysis and processing of the transmitted data will be performed, the decision is made, and the control information will be formed and feedback to the corresponding terminal. From this application, we can infer that sensor network, core network and application network (e.g. P2P) are the basic network structure of the IoT, as shown in Fig. 2.

The three network layers are sensor layer, core layer and application layer for short. The sensor layer includes physical devices (i.e. RFID), wireless sensor network, and Base station. Core layer mainly includes access network and Internet. The application layer includes various distributed networks (i.e. P2P, Grid, cloud computing), application system, and application interface. Fig. 2 also depicts the trust management for the IoT, which mainly includes three steps: trust extraction, trust transmission and trust decision-making. Notice that, requested information service and trust based service coexist in this model. Trust mainly pays attention to the selection mechanism and auxiliary decision, not the specific task, such as transmitting the data.

From Fig. 2 and Section II we understand that trust management should act as a role of self-organizing trusted nodes, networks, paths and trusted service to deal with the information flow, and preventing the privacy information from leaking to un-trusted SR. Self-organization is the key component and will be discussed detailed in this paper, and the privacy protection will be mentioned in the decision-making procedure. As we need to extract trust information for each layer of IoT, firstly we define three items for trust.

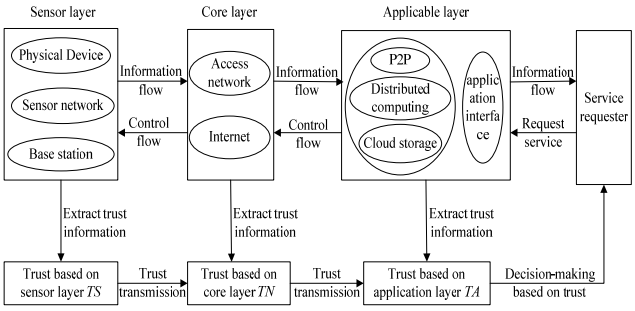

Figure 2. The structured model and trust management for IoT

Definition 2 (**Trust based on sensor layer *TS***). Define the trust information for the sensor network layer, denoted as a vector: $TS = \{X_S, TS_X, TS_{tar}, TS_{con}\}$.

Given a set of nodes $X_S = \{X_1, X_2, \dots, X_n\}$, a certain context TS_X, and a specified target TS_{tar}. The purpose of the trust mechanism is selecting a subset of nodes $X_s \subset X$ based on their trust degree TS_X to provide service. TS_{con} denotes control information, followed by multiple factors except TS_X, such as energy consumption, perception efficiency. Notice that X_i, $i \in [1, n]$ denotes the i-th node set, the number of X_i would be 1 if a single node is linked to the sensor network directly. And could above 1 if several nodes are cluster-based or group-based, then the iteration is necessary for inner cluster nodes to select trusted nodes. For the simplicity, we will set the same specified target TS_{tar} for the three layers: self-organizing for all the IoT nodes.

Similarly, we can define the trust based on core layer *TN:* $TN = \{X_N, TN_X, TN_{tar}, TN_{con}\}$, and the trust based on application layer *TA:* $TA = \{X_A, TA_X, TA_{tar}, TA_{con}\}$, where the four variables are the candidate nodes or sub-networks, the context, the specified target and the control information.

Trust mechanism is used to select a set of trusted access networks and certain routes to perform the data transmission in the core layer. The trust control TN_{con} includes some network factors (i.e. bandwidth, service price, routing efficiency). The investigated objects in the application layer are application services, such as processing data, storage. The trust value of these services can be calculated, and a series of services are selected to finish self-organizing. In fact, the control information of the users' policies and distinct preference in the application layer should be included, except for the trust values TA_X.

In the next Section, we will represent the defined trust and the trust management for IoT in the formal semantics.

IV. FORMALIZATION PROCESS OF TRUST MANAGEMENT

A. Extracting trust information

1) Trust based on sensor layer TS

The minimum granularity in sensor layer is a sensor node. One feasible method to measure the trust level of a node is to analyze its factors or rather trust attributes, which may be aggregated in a layered tree structure. The root denotes trust vector, the leaves denote the attributes. The depth of the tree is decided by the precision of the attributes.

The general form of the trust vector is $V_T=\{v_1,v_2,\ldots,v_m\}$ that can be obtained from the comprehensive evaluation of all the attributes in the trust tree. There are various methods for evaluating multi-factor variable. We apply fuzzy set theory to analyze the trust in IoT in this paper as fuzzy set theory [8] is an excellent tool to depict the uncertainty of a node, and the computational complexity is low.

In fuzzy set theory, a variable $V_T=\{v_1,v_2,\ldots,v_m\}$, $v_k(k=1, 2, \ldots, m)$ denotes the value of object T at the point k (k-level value) according to the defined membership functions in a given discourse domain. The problem now is how to obtain the V_T under a given trust tree.

We consider a particular condition that the depth of the trust tree t=1, suppose factors $F=\{f_1,f_2,\ldots,f_n\}$ denote n leaves, evaluation set $S=\{s_1,s_2,\ldots,s_m\}$ denote m evaluated values for every factor, evaluation matrix $R=F\times S=(r_{ij})_{n\times m}$, the weighted vector for the factor vector F is $W=\{w_1,w_2,\ldots,w_n\}$. Then the overall trust vector is denoted as $V_T=\{v_1, v_2,\ldots,v_m\}=(w_1,w_2,\ldots,w_n)\mathrm{o}(r_{ij})_{n\times m}$, where $v_j=\bigvee_{i=1}^{n}(w_i\wedge r_{ij})$, j=1,2,…,m. Generally, $t>1$, multiple iterated evaluation is needed to calculate the overall V_T. Firstly, classify the bottom n nodes into r subsets according to different r father nodes: $F_{sub}^{i}=\{f_{1i}, f_{2i},..., f_{l_k i}\}$, i=1,2,…,r, simultaneously satisfying $\sum_{k=1}^{r} l_k=n$, $\bigcup_{i=1}^{r}F_{sub}^{i}=F$, $F_{sub}^{i}\cap F_{sub}^{j}=\varnothing$, $i\neq j$. For each subset, the fuzzy comprehensive judgment is performed with the same method as the case of t=1. Given an evaluation set $S^i=\{s_1^i,s_2^i,...,s_m^i\}$ and a weighted vector $W^i=\{w_1^i,w_2^i,...,w_n^i\}$ for i-th subset, we can calculate the evaluating vector $V_T^i=W^i\circ\left(F_{sub}^{i}\times S^i\right)=(d_1^i,d_2^i,...,d_m^i)$, i=1, 2, … , r, then set the result V_T^i as the leaf node of the node in higher level, and again perform a fuzzy evaluation. Several iterations are done until the evaluated vector of root node V_T is achieved. In order to obtain the concrete values, the process of de-fuzzy is performed for the trust vector: $TS_X = f_d(V_T)$, where $f_d(\cdot)$ is a de-fuzzy function, and the simplest function is defined by the gravity law.

In sensor layer, $TS = \{X_S, TS_X, TS_{tar}, TS_{con}\}$, the core task is selecting a set of nodes from X_S based on TS_X under the control information TS_{con}. It is a process of sorting and filtering the TS_X under different thresholds, which are controlled by the TS_{con} dynamically, i.e. when defines the trust value based on the overhead, higher trust means lower overhead. Defining "low overhead" is valid (with the threshold Th_{TS}), then nodes whose trust below Th_{TS} will be selected. Notice that the nodes may be integrated into a cluster. We take the cluster as a whole. When a cluster is selected, the inner nodes in this cluster will be further evaluated so as to organize a subset of trusted nodes to on behalf of the entire cluster.

2) Trust based on core layer TN

Core network layer includes access networks and the Internet. We take the access networks and routes in the Internet as research objects. Suppose there are n optional access networks $AN = \{AN_1, AN_2,\ldots, AN_n\}$ and m retrievable routes in internet $IN = \{IN_1, IN_2, \ldots, IN_m\}$, we need to evaluate these routes (the selection of access network is also considered as routing for transmitting data), and select certain trusted routes to perform the task of data transmission. The control factors TN_{con} deciding the restricted conditions or thresholds of the trust level include network price, local regulars, linkage condition, etc.

Similar to sensor layer, trust values are followed by some attributes. For example, $TN_X = \{HT, RT, Risk, Attack, capability\}$, represent the historical trust, recommended experience, risk, ability of anti-attack and the service capability respectively. Each attribute in the vector is judged by a fuzzy set $S_{TN}=\{s_{N1},s_{N2},\ldots,s_{Nm}\}$. Generally m is set to 6 in fuzzy theory standing for 6-level trust, from the lowest trust to the highest trust. For 5 attributes, evaluation matrix can be obtained $R=(r_{ij})_{5\times 6}$. The weighted vector for every attribute is $W_{TN}=(w_1,w_2,w_3,w_4,w_5)$, the trust vector for the single evaluated item is calculated as follows: $V_{TN}=\{ v_1, v_2, v_3, v_4, v_5, v_6 \}=(w_1,w_2,w_3,w_4,w_5)\circ(r_{ij})_{5\times 6}$.

Trust management for core layer is aimed at acquiring a set of optimal routes. $AN_{tar}\subset AN$, $IN_{tar}\subset IN$ denote the optimal routes of access network and Internet, $X_{op}=AN_{tar}\cap IN_{tar}$, $X_{op}\subset X_N$ is the self-organized result for TN.

3) Trust based on application layer TA

The objects in the application layer are application services, i.e. processing data, storage. We need to evaluate which the candidate methods of processing data (P2P, Grid, pervasive) are trusted, whether the candidate storage services (DHT, cloud storing) are trusted, etc.

For a single service, the process of evaluation is the same as that in sensor layer, while the control attributes are service efficiency, service risk, service history and others. For multiple services, a set of services could be combined from a single service.

$$X_{ser}=\{S_{t1}^{i}, i\in[1,n1]\}\bigcap\{S_{t2}^{i}, i\in[1,n2]\}\bigcap\ldots\bigcap\{S_{tm}^{i}, i\in[1,nm]\} \quad (1)$$

Where $X_{ser}\subset X_A$, $t1$, $t2$, …, tm denote the service content, $n1$, $n2$, …, nm denote the number of selected objects under the same service content based on trust values.

B. Decision-making based on trust

In this paper, we assume that information transmission is secure, the self-organized trust information will be transmitted to higher layer sequentially, and the final result is $T = \{TS, TN, TA\}$. Based on the service model, we propose two kinds of decision-making based on trust: access control policy based on trust and self-organized decision.

1) Access control policy based on trust

Not all the requested services can be responded, we should prevent the privacy information from leaking to un-trusted requesters in the decision-making. An access control policy based on trust is given: $R:\mapsto(f,s,T)$, f is security policy, s is security credential, T is trust value for users. The user has access to the IoT only if security credential satisfies security policy, namely the statement (f, s) is true. A service decision-making function can be defined according to user's trust value. Suppose that the overall trust

can be divided into p levels, which satisfy: $t_1<t_2<\ldots<t_p$ and $t_i \cap t_j=\emptyset$ $(i\neq j)$. Potential $p+1$ services can be provided, denote as $S=\{s_0, s_1,\ldots, s_p\}$, the access control policy based on user's trust value T is defined as follows.

$$S(T)=\begin{cases} s_p, & T>t_p \\ s_{p-1}, & t_{p-1}\le T<t_p \\ \vdots & \vdots \\ s_1, & t_1<T\le t_2 \\ s_0, & T\le t_1 \end{cases} \quad (2)$$

The access control policy can decide whether to provide service and what degree to provide service according to users' trust values when users demanding certain services. For example, S = {deny, partial, normal}, and T_P = {0.2, 0.5}. If T = 0.8, then he can acquire the normal service. It is vital to set proper trust thresholds to determine if the data or only a sample of it will be disclosed, or if the request will be rejected.

2) Self-organized decision-making based on trust

In order to provide various quality of service (Qos), there should be more than one set of self-organized objects selected in each layer. $TS=\{T_{S_1},T_{S_2},\ldots,T_{S_l}\}$, $TN=\{T_{N_1}, T_{N_2},\ldots,T_{N_l}\}$, $TA=\{T_{A_1},T_{A_2},\ldots,T_{A_l}\}$, where the elements of each vector in each layer denote different sets of objects providing different Qos in descending order. The best Qos means selecting the best combination of objects (T_{S_1}, T_{N_1}, T_{A_1}) to provide a service.

In the case of multiple policies, the trust mechanism of the IoT can provide l^3 solutions supposing existing l available sets of objects for each layer in theory. A particular triple (T_{S_t}, T_{N_t}, T_{A_t}), $t\in[1,l]$, is selected according to secure request and personalized policy. In order to achieve concrete decision-making value like formula (2), fuzzy set theory still be used to quantify these selected set of objects. Given a system variable X and a mapping relationship, $f(X): TS\mapsto\{f(T_{S_1}), f(T_{S_2}),\ldots, f(T_{S_l})\}$. A simple example is that the $f(X)$ is the sum of trust values for X. Then an evaluation vector $S_{TS}=\{S_1, S_2, \ldots, S_l\}$ corresponding to $\{f(T_{S_1}), f(T_{S_2}),\ldots, f(T_{S_l})\}$ is obtained with the self-defined $f(X)$. The evaluated vector is obtained $V_{TS}=\{V_{S_1}, V_{S_2},\ldots, V_{S_l}\}$ with the same weight W for each element in S_{TS}: $V_{TS}=W\times S_{TS}$. Another two vectors $V_{TN}=\{V_{N_1}, V_{N_2},\ldots, V_{N_l}\}$ and $V_{TA}=\{V_{A_1}, V_{A_2},\ldots, V_{A_l}\}$ of TN and TA can also be obtained in the same manner. Then new triple (V_{S_i}, V_{N_i}, V_{A_i}), $i\in[1,l]$ is combined randomly. Further, one of the overall trust value T_i of the whole IoT is calculated by the weighted sum of each element in (V_{S_i}, V_{N_i}, V_{A_i}), with the weight of (W_1, W_2, W_3) determined by different importance of each layer and the uses' preference. All the combined triples will form a vector $T=\{T_1, T_2,\ldots,T_{l3}\}$, each element stands for a triple (T_{S_t}, T_{N_t}, T_{A_t}) under the same context. The final decision-making based on trust is achieved by the concrete value in T and self-defined threshold.

V. DISCUSSIONS

The established trust management mechanism provides a general trust-based framework for the IoT. Moreover, it provides a significant reference for the development of trust models for IoT. Notice that a trust model is fundamentally different from a trust management, as it describes the trust establishment and computation techniques. Trust model is the specific realization of the trust management.

Notice that, no concrete trust models are discussed in this paper, as we attempt to establish a general framework, in which the mature trust models can be integrated. Especially, the extracting, calculating and the transmitting of the trust information, as well as the decision-making mechanism varied in different trust models. Anyway, the existed or the newly established trust model should be unified under the function of trust management that is providing a service of self-organizing a set of items based on their trust status to take an informed decision.

VI. CONCLUSIONS

This paper proposes a general research framework of trust mechanism for the Internet of Things. We use formal semantics-based method to realize the trust mechanism and decision-making based on trust, and the result is coherent and reasonable. It provides a significant reference for the development of trust models for IoT, as mature trust models can be integrated in the proposed general framework. Further research of trust model for IoT scene will be the future works.

ACKNOWLEDGEMENT

The work is supported by "National Natural Science Foundation of China (No. 61121061), (No. 61003285)."

REFERENCES

[1] Miorandi, D., Sicari, S., Pellegrini F. D., et al. "Internet of things: Vision, applications and research challenges", Ad Hoc Networks, 10(7), 2012, pp. 1497-1516.

[2] Bahtiyar, S., Caglayan, M.U., "Extracting trust information from security system of a service", Journal of Network and Computer Applications, Volume 35, Issue 1, 2012, pp. 480-490.

[3] Liu, Y., Wang K., "Trust control in Heterogeneous Networks for Internet of Things", ICCASM 2010, Volume: 1, pp. 632-636.

[4] Gu X., Qiu J., Wang J., "Research on Trust Model of Sensor Nodes in WSNs", Procedia Engineering, Volume 29, 2012, pp. 909-913.

[5] Shaikh, R. A., Jameel, H., d'Auriol, B. J., *et al*., "Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks", IEEE Transactions on Parallel and Distributed Systems, 2009, 20(11), pp. 1698-1712.

[6] Li X, Zhou F, Yang X. A multi-dimensional trust evaluation model for large-scale P2P computing [J]. Journal of Parallel and Distributed Computing, 2011, 71(6): 837-847.

[7] Sun, Y. L., Han, Z., Yu, W. *et.al*, "A trust evaluation framework in distributed network: Vulnerability analysis and defense against attacks", Proceedings of the IEEE Infocom 2006. Barcelona, Spain, 2006. pp. 1-13.

[8] Khoury, R., Karray, F., Yu, Sun, *et al*., "Semantic understanding of general linguistic items by means of fuzzy set theory", IEEE Transactions on fuzzy systems, 2007, Vol. 15, pp. 757-771.