Journal of Computational Information Systems 9: 8 (2013) 3109–3116
Available at http://www.Jofcis.com

WSN Trust Models Evaluation in the Context of the IoT [⋆]

Jingpei WANG [1,*], Bin SUN [1], Yu YANG [1,2], Xinxin NIU [1,2]

[1] *Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China*

[2] *National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing 100876, China*

Abstract

This paper evaluates several traditional trust models for WSN(Wireless Sensor Network)in the context of the IoT(Internet of Things). The evaluated parameters are extracted from a concrete context, which is establishing the trust relationship between remote nodes after the WSN being integrated into the IoT. As an extension, the Ad hoc trust model is also evaluated. The evaluation and the simulation results show that possible trust models are suited for IoT on condition that several restrictions are available. The evaluated method and results provide a reasonable reference for the establishment of trust model for IoT.

Keywords: IoT; Wireless Sensor Network; Security; Trust Models; Trust Model Evaluation

1 Introduction

The Internet of Things (IoT) is a huge organic network that connects a large number of heterogeneous items and networks to provide directional services for humanity [1]. From the angle of networks composition, the sensor network, the core network (include access networks and the Internet), and application network are the basic compositions of IoT. However, the interconnection of these composite networks will inevitably bring new security challenges, such as the credibility of the nodes, the secure interaction, and the data privacy protection. Trust management provides a potential solution for the above security issues [2].

The core issue of Trust Management is establishing reliable trust models. However, there are rare researches on the trust models for IoT. Hu et al. proposed a reputation-based data fusion model [3], which aimed at solving the problems of the security of data sources and the fusion of trust data. However, their model only considered the trust issue of the WSN. In fact, most researches of the trust management proposed mainly focused on the composite networks of the IoT, such as WSN trust model [4-6], the trust mechanism for the IP network [7], and trust model

[⋆] Project supported by the National Nature Science Foundation of China (No. 61121061),(No. 61003285).

[*] Corresponding author.
Email address: dq2003136230@yahoo.com.cn (Jingpei WANG).

April 15, 2013

for the application network [8]. As sensor networks are the most basic components of IoT, it is a shortcut to probe into the trust models for IoT based on the mature trust solutions for WSN, which can maintain the relevant characteristics of the WSN as well as reduce the difficulty of the trust modeling for IoT directly.

This paper evaluates several typical WSN trust models and the related model. The evaluated parameters are extracted from a concrete security scene that how to create and update the trust relationship between the remote nodes in heterogeneous cross-domain networks (e.g. one node in WSN, and the other in P2P network) when the WSN is integrated into the IoT. The evaluated results are intended to provide a reference for the establishment of the trust model for the Internet of Things. The rest of the paper is organized as follows. Section 2 proposes a concrete security scene. We evaluate and compare typical trust models in Section 3. The analysis and simulation results are given in Section 4, followed by the conclusion in Section 5.

2 A Concrete Scene

The role of WSN in the IoT is that of a virtual skin, it becomes aware of surroundings and shares this information with other items in order to take informed decisions. When integrating into the IoT, the WSN will encounter new security challenges, such as the credibility of the WSN nodes, the secure interaction between the WSN node and the host node, and the privacy protection of the confidential data. Trust mechanism, as a method for portraying the uncertainty of the behavior of the network nodes at the semantic level, provides a viable solution for the above-mentioned security issues. In order to analyze the requirement of the trust mechanism in the process of integration, we consider a concrete scenario: the establishment and renewal of a trust relationship between two remote nodes that come from two different network domains in the Internet of Things. Suppose there is a cyberspace $X = \{X_1, X_2, \cdots, X_n\}$, $X_i (i \in n, n \geq 2)$ denote a set of networks, node $A \in X_1$, $B \in X_n$ (i.e. A is in WSN, B is in application network), and $X_1 \bigcap X_n = \varnothing$. The initial trust value $T(A, B) = 0$. Node A establishes trust relationship with B through a trust function $TR(A, B)$, where $TR(A, B) = \{Path(A, B), Value(A, B), Context, Requirement\}$. $Path(A, B) = \{P_1, \cdots, P_n\}$ represents the paths set from node A to B, $P_i (i \in [1, n])$ denotes the transitive node. Node A need to span multiple intermediate nodes or networks to build trust with node B. $Value(A, B)$ denotes the established trust value, $Context$ is the concrete context defining a set of assumptions, which are outlined as follows.

• **Hypothesis 1:** There exist heterogeneous cross-domain networks. Multiple heterogeneous networks exist between the strange nodes in different networks. Trust needs to be transferred across heterogeneous domains.

• **Hypothesis 2:** The network structure of WSN is static. In this article, we assume that sensor networks used are static, which is a group of sensor nodes scattered in a certain area (e.g. a building) using IEEE 802.15.4 transceivers and constantly connected to the Internet.

• **Hypothesis 3:** The behaviors of the remote nodes are equivalent. Sensor node and Internet host node are treated equally and any one of them can be used as the service node or client node. The establishment of the trust relationship is bidirectional.

Requirement defines a set attributes and requirements for building the trust relationship:

• *Transitivity*. When establishing a link between cross-domain nodes, the transmission of the trust is necessary. Trust, as the concept at the semantic level, can be transferred seamlessly among different domains. The trust model should meet the requirements of transitivity, which judged by the transfer efficiency, either the shortest time or the optimal path.

- *Robustness.* This feature describes the self-healing mechanism of a trusted network when encountering attacks. A good trust model should could find fault timely, update the trust relationship, and shield or punish malicious nodes to maintain network stability. Clearly, the more robust is the trust model, the better.

- *Overhead.* This property will mainly refer to sensor nodes, as most sensor nodes will be energy-constrained. The overhead directly influences the lifecycle of the sensor nodes. Therefore, the overhead in the IoT context must be as low as possible.

- *Scalability.* This property describes the relationship between the amount of information stored in a single node and the number of connected nodes. A trust model is scalable if the information required to contact any potential peer does not impose any storage on the device. Again, it is desirable to have a high scalability for the IoT.

The establishment and renewal of the trust relationship are the most basic problems of the trust management, the four attributes above-mentioned can be used as metrics to judge whether a certain trust model meets the requirement of the IoT. In this paper, we use these metrics as evaluated parameters to analyze the performance and applicability of different WSN trust models in the defined security scene.

3 The Evaluation of Typical WSN Trust Models

As our article focuses on the establishment and renewal of the trust mechanism, we will investigate current trust models based on the dimension, the method, and the network granularity of trust establishment. Trust is a multi-dimensional concept. Trust and reputation, identity-based trust and behavior-based trust are the two kinds of classification. A hybrid trust and reputation model for sensor networks (HRMSN)[4] combining above two classifications will be analyzed detailed. The probability theory is the most popular method for establishing trust, and related WSN trust model (BNWSN)[5] will be analyzed in detail. As to network granularity, sub-domain based and domain-based trust mechanism are considered to be more reasonable, especially cluster-based WSN trust models (GTMS)[6] are widely used. We will evaluate these three typical WSN trust models. In addition, we will also evaluate one of the Ad Hoc trust models [7]. The reason for selecting the Ad Hoc model is that the WSN is similar to the Ad Hoc network, we consider the WSN as a typical application of the Ad Hoc network.

3.1 Typical WSN trust models and related model

(1) HRMSN model: The HRMSN[4] overcomes the inflexibility of a single identity-based trust model and huge energy consumption of a single behavior-based reputation model. In their model, when a node i need to establish a trust relationship with a strange node j, the node i will search for a credible certification center x to certify the target node j. If the certification is approved, the node i will collect trust evidences of the node j, including the direct trust relationship and recommendation trust. When sufficient evidences are collected, the trust values can be calculated:$T_{ij} = t(R_{ix}, T_{xj})$, $x \in N$, where $t(\cdot)$ is a self-defined function, R_{ix} denotes the reputation of i relative to the certification node x, T_{xj} is the trust value of x to j, and N is the

set of recommended nodes. When the accumulative identity-based evidences are not enough, this trust model will seek more behavior-based trust. The recommendation from trusted monitoring nodes as well as third-party nodes will be collected to calculate and renew the trust relationship. The collected evidences and the renewed reputation will be stored to detect malicious behavior when necessary. Some monitoring nodes as well as malicious nodes may be forbidden to interact by the revocation of their trust certificates if being found abnormal.

(2) BNWSN model: Trust modeling based on probability theory is the most typical method. Bayesian theory based trust model(BNWSN)[5] is paid more attention to because of simple inference. The Bayesian fusion algorithm is introduced to combine both data and communication trust to infer the overall trust. Communication Trust (CT) means the trust value based on cooperation in routing messages between two nodes in the network, and it is defined as the expected value of the Beta reputation system. Data Trust (DT) is based on the performance of sensed data of the sensors. DT is the distribution function value of the Gaussian distribution. Using the Bayesian theorem, the probability of the total trust can be presented in (1).

$$P(T|T_c, T_d) = P(T|T_d) * P(T|T_c). \tag{1}$$

Where T_c and T_d denote the values of CT and the DT respectively, T is the overall trust value, $P(T|T_c, T_d)$ is the probability of the total trust. The proposed algorithm is simple and generic as it allows more trust components to be plugged into the model to infer the total trust for different scenarios.

(3) GTMS model: A typical three-layered structure for WSN is depicted as: the base station - the cluster head - sensor nodes. Based on this network granularity, the GTMS was proposed [6]. GTMS works with two topologies. One is the intra-group topology where distributed trust management is used. The other is intergroup topology where centralized trust management is employed. The trust model works in three levels: the node level,the cluster-head level and the BS level. At the sensor node level, the trust is calculated in (2).

$$T = [100(\frac{S}{S+U})(1 - \frac{1}{S+1})] = [\frac{100S^2}{(S+U)(S+1)}]. \tag{2}$$

Where S and U are the number of successful trading and failed trading in a certain-length time window Δt, T is defined as an integer, and $T \in [0, 100]$. Based on the trust values, a node assigns one of the three possible states: 1) trusted, 2) un-trusted, or 3) uncertain to other member nodes. The half of the mean of all the trusted values and the 1/3 of the mean of all the un-trusted values is set to the medial boundaries of three states. At the level of the cluster head and the base station, the trust values between the objects are calculated similar to equation (2), while the calculative target of trust is the trust state. Simple trust status can flag the node behavior, reduce the computational load, and provide a range of identification for anti-attack analysis.

(4) Ad Hoc model: This article further analyzes an Ad Hoc Trust Model[7].The trust is defined as describing the uncertainty that the agent will perform an action in the subject point of view. In particular, one entity trusts the other entity to perform an *action*. The first entity is called the *subject*, the second entity is called the *agent*. They introduced the notation $\{subject : agent, actions\}$ to describe a trust relationship. As entropy is a natural measure for uncertainty. This model defined an entropy-based trust calculation, in which $H(p) = -plog_2(p) - (1-p)log_2(1-p)$ is the entropy function, and $p = P\{subject : agent, actions\}$ denotes the probability of uncertainty. And the trust value $T = 1 - H(p)$ if $0.5 \leq p \leq 1$, while

$T = H(p) - 1$ if $0 \leq p \leq 0.5$. The proposed model considered the recommendation trust in detail, and obtained several deductions. One distinct feature of this model is that the trust values of multiple paths are obtained through multi-layer and multi-level calculation, and someone can choose an optimal credible route to implement the communication and interaction.

3.2 Trust model evaluation

In this section, we will compare and evaluate above four trust model using the evaluated parameters described in Section 2.

Transitivity. The evaluated standard of transitivity includes: trust can be transferred across different heterogeneous domain, and the higher the transfer efficiency, the better. HRMSN model has bad transitivity, as it searches for trusted nodes to build the transport chain every time, however, in the defined strange IoT scene, the certification centers may not always existed. Sometimes, we need to flood to collect trust information, thus transfer efficiency will decline. BNWSN, Ad Hoc, and GTMS models measure trust with probability variable, entropy, and the function of the number of the transactions respectively. These items are transparent to the network structure, and can be seamlessly transferred across heterogeneous domains. BNWSN model is simple and flexible, fusion center can guide the transmission of information of CT or DT, thus it has relatively high transfer efficiency. In Ad Hoc model, users can choose the highest global trust routing from the multi-level multi-path trust chains to pass the trust information accurately. The transfer efficiency is improved. The GTMS model can organizes nodes in a layered group-based centralized manner to pass trust information to the target node efficiently. The shortest path will lead to the highest efficiency.

Robustness. The more robust is the trust model when encountering with attack, the better. HRMSN model can partially shield from the malicious nodes with several trusted CA, and it sets a monitoring network by exploiting the pre-deployment knowledge of the network topology to note and control the malicious behavior. BNWSN has the high efficiency in detecting the attacks, but it is difficult to achieve good robustness merely with probabilistic algorithms. In GTMS model, the cluster head node can choose a trusted group to interact through the base station. In addition, it can detect and prevent the attacks from malicious, selfish, wrong nodes, for the detailed description, please refer to [6]. The Ad hoc model can realize the self-organization of trusted route by selecting the most reliable paths, and it can shield the malicious node's routing, so the robustness is high.

Overhead. Lower complexity of computation and communication will lead to better overhead. HRMSN model has a good performance in the overhead, as the trust evidences are collected always through trusted nodes or trusted recommended nodes, it can reduce communication overhead utmost. Moreover, it allocates resources by understanding the heterogeneity of the network, and higher energy node may be assigned to heavier computation, which will scatter the consumption of sensor nodes. The calculation for BNWSN model is simple and the intermediate nodes are responsible for routing for other nodes except for computing trust information. Trust is available to the requester through the stable routing of several fuse nodes. Therefore, the overhead is stable. The overhead of GTMS model is controllable. Satisfactory overhead can be achieved in the case that both the number of groups and the number of nodes in each group are not very large. The Ad Hoc model receives the most expensive overhead, because it needs to calculate multi-level and multi-layered trust chain to decide the optimal paths, and all the nodes between two unfamiliar nodes need dynamic computing and communications.

Scalability. In terms of scalability, the ideal situation is that stored information is stable or even less as the increase of the connected nodes. In fact, none of the above-mentioned models performs well in scalability. BNWSN model has no efficient storage mechanism. The amount of trust information that must be stored inside a node grows linearly (that is $O(n)$)with the number of potential linked nodes. In fact, storage round $O(n)$ or above is considered to be large. The Ad Hoc model requires a large storage for multi-level and multi-path trust values between two nodes. Moreover, because of the mobility of the nodes, continuous detection of routing is required. As a result, a larger amount of storage will be consumed. GTMS is a centralized trust model. Each cluster head node needs to store all the trust information of a set of nodes, such as the node within the cluster, neighboring cluster head nodes, and base station nodes. However, the amount of stored information can be controlled according to group size and group number. For the HRMSN model, it is hard to find credible recommended nodes and monitoring nodes as the network size increases, especially for the connection of distanced nodes in different domain, the stored information will increase sharply, and the scalability is deteriorating.

4 The Evaluated Results and Simulation Analysis

4.1 Analysis and simulation results

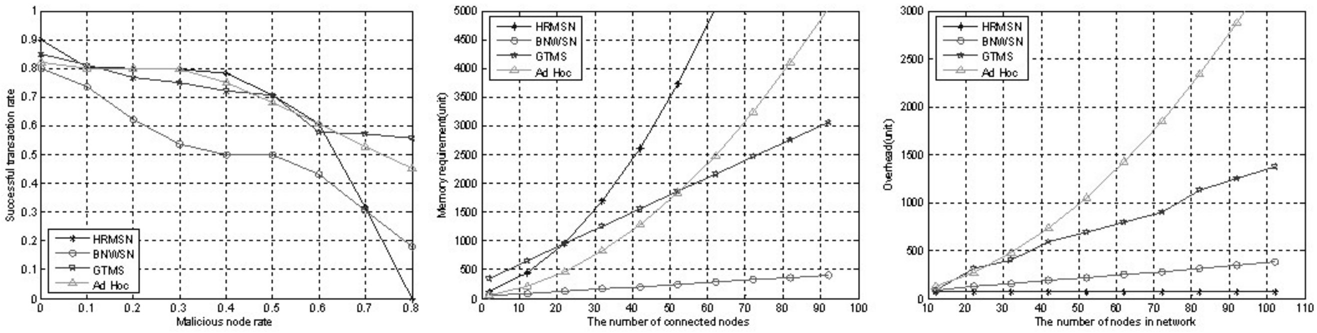
The previous section has evaluated four kinds of trust model. The evaluated results are presented in Table 1. We use high (good), medium, low (bad) to measure the performance of the investigated trust models, according to the definition of the evaluated parameters and the analysis results. On the other hand, we also perform a simulation for the evaluated parameters, and the results are shown in Fig.1.

Table 1: The performance of the investigated trust models in the evaluated parameters

	Transitivity	*Robustness*	*Overhead*	*Scalability*
HRMSN	bad	high	lowest	bad
BNWSN	medium	low	low	medium
GTMS	good	high	medium	bad
Ad Hoc	medium	high	high	bad

We choose 150 nodes, 50 nodes for each of the three structural networks (WSN, core network, and P2P network, the same as below), random link. We calculate the number of hops that the source node A reaches the furthest destination node B to evaluate the transitivity, supposing that the time for every hop is fixed. The less hops means the higher efficiency. The requested numbers of hops are 84, 71, 48, 70 for the four evaluated trust models. The GTMS gets access to the target node directly through three-level group-based nodes, which make the highest efficiency.

Fig.1(a) describes the robustness of the investigated trust models. We select malicious nodes randomly from the 150 nodes but with the consistent proportion for the three kinds of networks. The malicious nodes implement a DOS attack in WSN, and perform malicious feedback attack in the core network and P2P network continuously. The ability of robustness is measured by the



(a) The robustness of the investigated trust models (b) The scalability of the investigated trust models (c) The overhead of the investigated trust models

Fig. 1: Simulation results

relation of the successful transaction rate and malicious nodes rate after 100 times of transactions. BNWSN model has the lowest robustness; HRMSN shield some malicious nodes from interaction, but when the malicious nodes rate are high(0.6), the successful transaction rate declines sharply as some monitoring nodes and malicious nodes are forbidden to interact by the revocation of their trust certificates. GTMS and Ad Hoc model both are immune to attack, as the successful transaction rate maintains enough high when the malicious nodes rate is increasing. Fig.1(b) describes the scalability of the various models. The x-axis denotes the number of nodes connected to the source node, and y-axis denotes the memory requirement, the basic unit is 1 *unit*(just a proportional coordinate). The curve for HRMSN depicts the change of storage for the monitoring node, and the memory requirement is $O(n_2)$. Ad Hoc model also has a large amount of stored information. GTMS can adjust the scalability by adjusting the size of the group and the number of nodes within each group, both of which are set to 10 in the simulation. The storage requirement for BNWSN model is $O(n)$, relatively small. Fig.1(c) describes the overhead. The initial number of nodes is 12, and 10 nodes are increased every time. The overhead is measured by the amount of energy consumption, of which the basic unit is 1 *unit*. The Ad Hoc model receives the highest overhead(up to $O(n_2)$)while HRMSN receives the lowest. The overhead of GTMS is relatively high in the middle-size networks, which nodes may divide into ten groups roughly in our simulation. The overhead of BNWSN is about $O(n)$, and HRMSN round $O(1)$. It can be seen from Fig.1 that the simulation results are consistent with the analysis in Section 3.2.

4.2 Summary

From the evaluated results, we can see that all the investigated trust models have their merits and demerits, no trust models existed satisfy all the above parameters. However, we can determine the usability of the trust models on condition that several restrictions are available in IoT.

HRMSN model is suited for structured Internet of Things where the certification center is available (e.g. in intelligent transportation applications, road service units and the base stations are reliable and can be used as management nodes). Two remote nodes distributed in the distant domain can establish and update the trust relationship through a series of trusted CA and recommended nodes in this scenario. The transitivity, robustness and the scalability can be improved with the help of reliable nodes.

Trust model like BNWSN has certain universality. If the trust relationship is relatively stable in a structured or distributed IoT application (e.g. in healthcare system, when the doctor-patient relationship is relatively stable), the BNWSN could be a viable solution. In this environment, a node is able to self-organize a credible route to avoid attacks, and can connect sufficient extra-territorial nodes through the fusion nodes with excellent storage capacity to improve scalability.

Trust model based on network granularity such as GTMS is suitable for the situation that both the number of the groups and the number of nodes within each group are within a controllable scale (e.g. in a intelligent building, when the floors and the number of facilities on each floor are limited in a proper range). Proper scale will induce controllable overhead, and scalability will be improved. Theoretically, the proper scale of groups can be obtained, so as to the number of nodes within each group.

Distributed Ad hoc model, because of its expensive overhead, is only suitable for the powerful nodes to self-organized networking and establish trust. Other distributed trust models, if meet the requests of good transitivity, better stability, lower overhead and better extensional mechanism, can also be used in the Internet of Things.

5 Conclusion and Future Work

This paper evaluates the performance of a variety of WSN and related trust models in the context of the Internet of Things. We use simulation results to verify the correctness of the evaluated analysis. We also determine the possible applications of the investigated trust models in the specific scenarios of the Internet of Things. The summary provides a reasonable reference for the establishment of trust model for IoT. Notice that, if we develop a more reasonable, effective, and universal trust model as a standard model, the comparison results in Table 1 and Fig.2 will be further improved, which indicates the future works.

References

[1] Zhu H. A Framework to Enable Communication in Heterogeneous Environment for the Internet of Things [J], Journal of Computational Information Systems, 2012, 8(18): 7791-7798.

[2] Lopez J, Roman R, Agudo I, et al.. Trust management systems for wireless sensor networks: Best practices [J], Computer Communications, 2010, 33(9): 1086-1093.

[3] Hu X, Wei Q, Tang H. Model and simulation of creditability-based data aggregation for the Internet of Things [J]. Chinese Journal of Scientific Instrument, 2010, 31(11): 2636-2640.

[4] Aivaloglou E, Gritzalis S. Hybrid trust and reputation management for sensor networks [J], Wireless Networks, 2010, 16(5): 1493-1510.

[5] Momani M, Challa S, Alhmouz R. Bayesian Fusion Algorithm for Inferring Trust in Wireless Sensor Networks[J], Journal of Networks, 2010, 5(7): 815-822.

[6] Shaikh R. A, et al. Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks [J], IEEE Transactions on Parallel and Distributed Systems, 2009, 20(11): 1698-1712.

[7] Sun Y. L, et al. Information theoretic framework of trust modeling and evaluation for ad hoc networks [J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 305-319.

[8] Li X, Gui X. Research on adaptive prediction model of dynamic trust relationship in open distributed systems [J], Journal of Computational Information Systems, 2008, 4(6): 2483-2489.