DOI: 10.2298/CSIS110303056C

TRM-IoT: A Trust Management Model Based on Fuzzy Reputation for Internet of Things

Dong Chen[1], Guiran Chang[2], Dawei Sun[1], Jiajia Li[1], Jie Jia[1], and Xingwei Wang[1]

[1] College of Information Science and Engineering, Northeastern University, 110004 Shenyang, China
chend.2008@gmail.com
[2] Computing Center, Northeastern University, 110004 Shenyang, China
chang@neu.edu.cn

Abstract. Since a large scale Wireless Sensor Network (WSN) is to be completely integrated into Internet as a core part of Internet of Things (IoT) or Cyber Physical System (CPS), it is necessary to consider various security challenges that come with IoT/CPS, such as the detection of malicious attacks. Sensors or sensor embedded things may establish direct communication between each other using 6LoWPAN protocol. A trust and reputation model is recognized as an important approach to defend a large distributed sensor networks in IoT/CPS against malicious node attacks, since trust establishment mechanisms can stimulate collaboration among distributed computing and communication entities, facilitate the detection of untrustworthy entities, and assist decision-making process of various protocols. In this paper, based on in-depth understanding of trust establishment process and quantitative comparison among trust establishment methods, we present a trust and reputation model TRM-IoT to enforce the cooperation between things in a network of IoT/CPS based on their behaviors. The accuracy, robustness and lightness of the proposed model is validated through a wide set of simulations.

Keywords: Internet of Things, Cyber Physical System, Wireless Sensor Network, Trust, Reputation, Fuzzy Sets.

1. Introduction

Cyber-Physical Systems (CPS) are systems deployed in large geographical areas and generally consist of a massive number of distributed computing devices tightly coupled with their physical environment [1]. CPS and Internet of Things (IoT) have always been closely related, since both of them employ physical objects and events, including WSNs, RFID-based systems, mobile phones, etc. Cyber-Physical Internet [1], which can roughly be viewed as a

large-scale universal network that interconnects several heterogeneous CPS in order to ensure worldwide interoperability of cyber-physical devices. Therefore, we argue that the proposed fuzzy theory based trust and reputation model is not only suitable for CPS, but also suitable for IoT.

IoT and CPS cannot perceive physical information from physical world themselves. Intelligent things are usually labeled with RFID tags or equipped with sensors and sensors are widely regarded as the nerve endings of IoT/CPS [2] [3]. Sensors or sensor embedded things can usually form a wireless multi-hoc network-WSN employing ZigBee, Wi-Fi, Bluetooth and etc. In a future IoT/CPS, a large number of embedded, possibly mobile computing devices will be interconnected through WSNs, constituting various autonomous subsystems that provide intelligent services for end users. IoT/CPS can benefit from WSNs from the perspective that so far, sensors and RFID readers are the most efficient tools to obtain sensed data from the physical world, turning ubiquitous computing of IoT/CPS into a reality. Therefore, Internet connectivity in WSNs of the IoT/CPS is highly desirable, featuring sensing services at a global scale all over the world [4].

However, such networks present some new challenges when compared with traditional computer networks, namely in terms of smart node hardware constraints, very limited computing and energy resources. Unlike other networks using dedicated nodes to support basic functions like packet forwarding, routing, and network management, in WSNs of IoT/CPS, those functions are carried out by all available nodes. This significant difference is at the core of the increased sensitivity to node misbehavior. Due to the wireless nature of this kind of WSNs, it is also quite possible that a node could be captured by an adversary, which may lead to its non-cooperative behavior or misbehavior with the rest of the nodes in the network and even become a malicious node. Malicious nodes aim at damaging other nodes by causing network outage by partitioning.

In order to facilitate the detection of untrustworthy nodes, and assist decision-making process of various protocols in a WSN which is vital for carrying out specific tasks as it aids sensors establish collaborations, it is necessary to provide a trust and reputation mechanism for WSNs of IoT/CPS. One strategy to improve the security of WSNs is to develop trust mechanisms that allow a node to evaluate trustworthiness of other nodes [5] [6]. Such trust and reputation systems not only help in node behavior detection, but also improve network performance since honest nodes can avoid working with untrustworthy nodes [7].

The measurement and computation of trust and reputation to secure interactions between sensor nodes in IoT/CPS is crucial for the development of trust and reputation management mechanisms. The calculation and measurement of trust and reputation in a supervised ad-hoc environment involves complex aspects such as credible rating for opinions delivered by a node, the honesty of recommendations provided by a sensor node, or the assessment of past experiences with the node one wishes to interact with. The deployment of suitable algorithms and models imitating fuzzy logic can help to solve these problems. Therefore, the focus of this paper is to develop

a fuzzy theory based trust and reputation model for IoT/CPS environment. The proposed theoretical models are then applied to improve the performance of routing algorithms and detect node behaviors of WSNs in IoT/CPS.

The contribution of this paper can be categorized as follows. (1) Analysis of special features and unique trust challenges of IoT/CPS; (2) Concepts of trust and reputation and discussion of the relationship between trust and reputation in IoT/CPS; (3) A novel fuzzy theory based trust and reputation management model towards IoT/CPS; (4) Trust evaluation metrics, local trust relationship evaluation and global trust relationship evaluation; (5) A wide set of simulations, performance evaluations of the proposed fuzzy trust and reputation management model.

The remainder of the paper is organized as follows. We give an overview of related influential works in Section 2. In Section 3, a novel trust and reputation model for choosing trusted source nodes base on the fuzzy relationship theory in fuzzy mathematics TRM-IoT is proposed and further discussed in detail in WSNs of IoT/CPS. The simulation results in Section 4 show that TRM-IoT model can effectively prevent malicious and selfish nodes. TRM-IoT scheme can promote data forwarding and cooperation between nodes and improve the performance of the entire network, followed by the conclusion and future work of the paper in Section 5.

2. Related Works

Establishing security communication channels based on trust and reputation models among sensor nodes is an important consideration when designing a secure routing solution in IoT/CPS.

ATRM [8] is an agent-based trust and reputation management scheme for WSNs where trust and reputation management is carried out locally with minimal overhead in terms of extra messages and time delay. However, since mobile agents are designed to travel over the entire network and run on remote nodes, they must be launched by trusted entities. An agent-based trust model for WSN is presented in [9] using a watchdog scheme to observe the behavior of nodes and broadcast their trust ratings. Sensor nodes receive the trust ratings from the agent nodes, which are responsible for monitoring the former and computing and broadcasting those trust ratings. In [10], a reputation-based scheme called DRBTS is proposed to provide a method by which beacon nodes, *BN*, can monitor each other and provide information so that sensor nodes, *SN*, can choose who to trust, and based on a quorum voting approach. However, in order to trust a *BN*'s information, a sensor must get votes for its trustworthiness from at least half of their common neighbors. BTRM-WSN [11] is a bio-inspired trust and reputation model for WSN aimed to achieve to the most trustworthy path leading to the most reputable node in a WSN offering a certain service. Each node must maintain a pheromone trace for each of its neighbors. CONFIDANT [12] is proposed to extend

reactive routing protocols with a reputation-based system in order to isolate misbehaving nodes. Each node monitors the behaviors of its next hop neighbors. Trust relationships and routing decisions are based on experienced, observed, or reported routing and forwarding behavior of other nodes. SORI [13] scheme is proposed to encourage packet forwarding and discipline selfish behavior. The reputation of a node is quantified by objective measures, and the propagation of reputation is efficiently secured by a one-way-hash-chain-based authentication scheme. Watchdog and Pathrater mechanisms [14], are just two extensions to the DSR algorithm.

However, not all of the most known works take into account the strong restrictions about processing, storage or communication capabilities. Some of them rely on a watchdog mechanism with or without using a multi-agent system. IoT/CPS assumes that trillions of things which are used on a daily basis will eventually be connected to the Internet employing 6LoWPAN [15] protocol and provide intelligent service through cooperating with each other. Most things have the following significant characteristics [16] [17], limited power capability, wireless receivers and transmitters with limited range facing the use of multi-hop communication, mobility (things will move, possibly become disconnected) and violability (things may be switched on and off frequently). All the above issues raise the need for the development of a novel management model, different from those being in use today. Based on the research of characteristics of IoT/CPS and in-depth understanding of ATRM [8], ATSN [9], DRBTS [10], BTRM-WSN [11], CONFIDANT [12], SORI [13] and WP [14], we propose a novel trust and reputation model TRM-IoT to enforce the cooperation between things in a network of IoT/CPS based on their behaviors.

3. TRM-IoT: A Trust Model for IoT/CPS

The trust between sensor nodes cannot be set up simply by using the traditional trust mechanisms. In a human social community, trust between two individuals is developed based on the reputation evaluation of their actions over time. When faced with uncertainty, individuals will trust and rely on the actions and evaluations of others who have behaved well in the past.

Trust is one of the most fuzzy, dynamic and complex concepts in both social and business relationships. The difficulty in measuring trust and predicting trustworthiness in service-oriented network environments leads to many problems. These include issues such as how to measure the willingness and capability of individuals in the trust dynamics and how to assign a concrete level of trust to an individual. Wireless networks of IoT/CPS have several salient characteristics, such as dynamic topologies, bandwidth constraints, variable capacity links, energy constrained operation, and limited physical security. Due to these features, WSNs of IoT/CPS are particularly vulnerable to all kinds of attacks launched through malicious nodes. Unreliable wireless links are vulnerable to jamming and

eavesdropping. Constraints in bandwidth, computing power, and battery power in mobile devices may lead to their trade-offs between security and resource consumption. Dynamics make it hard to evaluate node behaviors, because routes in this kind of networks change frequently. Sensors or sensor embedded things are more likely to form a wireless multi-hoc network. Therefore, they cannot rely on central authorities and infrastructures for key management.

In this paper, we propose a generalized and unified mechanism to address the trust and reputation issue by developing a community of sensor nodes in the WSNs of IoT/CPS. Our motivation is to develop a similar behavior and fuzzy theory-based trust and reputation model for sensor nodes or sensor-embedded nodes, where each node develops a direct reputation for each other node by making direct observations and indirect reputation between individuals set up upon recommendations of other individuals about these other nodes in the neighborhood. The two kinds of reputations are used together to help a node evaluate the trustworthiness of other sensor nodes, detect the malicious nodes, and assist decision-making within the wireless network. The proposed scheme can be employed in any WSNs routing protocol to enforce cooperation among nodes and counter with non-cooperative nodes in IoT/CPS infrastructure.

The resource constraints of WSNs such as limited battery lifetime, memory space and computing capability in IoT/CPS make it easy to attack and fairly hard to protect. Therefore, it is fairly critical to detect the compromised nodes in order to avoid being misled by those compromised or malicious nodes. However, malicious nodes are so difficult to detect even a cryptography mechanism is applied, since most low-cost tiny sensor nodes are not tamper-resistant and easy to be cracked by the adversary. Therefore, in this paper we argue that behaviors-based trust and reputation mechanism can be used to resolve this problem efficiently. Based on this motivation, this paper proposes a novel behavior-based trust and reputation for IoT/CPS. The management model of trust and reputation is related to the creation, update and deletion of trust and reputation degree.

First, an effective lightweight authentication mechanism must exist to ensure all the identities are trustworthy [18] [19] [20]. That means the identity of each sensor node is unique and trustworthy, on the basis of cryptographic primitives [21] [22] [23]. In fact, we have proposed a novel lightweight pair-wise key management scheme towards IoT/CPS in a previous paper before this one. Second, the task evaluation component evaluates the performance of the nodes, including sensors nodes and sensor-embedded device nodes. The tasks here include data processing and routing. Third, evaluation combination component is in charge of the result combination of the old trust degree and the indirect information from the third node in order to form the new trust degree which is used in future task allocation and evaluation.

Throughout this paper we assume a scenario where a WSN of IoT/CPS is composed of hundreds of sensor nodes with relatively high sensor activity. Without loss of generality, we consider some sensor nodes requesting lightweight common services and some nodes providing these services. We

also assume that every sensor node in the WSN only knows its neighbors and nothing else about the whole topology of the WSN. Additionally, the topology is considered to be relatively highly dynamic, with many nodes joining or leaving the community. The contribution of the proposed model is aimed to help a sensor node requesting a specific service to find the most trustworthy route leading to another sensor node providing the corresponding service. An untrustworthy node in this paper can be considered either because it intentionally provides a fraudulent service or because it provides a wrong service due to hardware failures or performance deterioration.

In this paper, taking costly decisions depends on the expectations created according to past behavior of others. Usually, this kind of information is called reputation and it is one of the most significant factors to trust merchants and recommenders towards IoT/CPS.

3.1. Definitions of Trust and Reputation

Although we experience and rely on trust in everyday life, it is so challenging to define trust accurately. The literature on trust is also quite confusing, since it manifests itself in fairly different forms. In this paper, we adopt the following definitions for trust and reputation.

Definition 1. Trust is the subjective probability by which an individual, A, expects that another individual, B, performs a given action on which its welfare depends [24].

Definition 2. Reputation is what is generally said or believed about a thing's character or standing [25].

Reputation exists only in a community which is observing its members in one way or the other. Accordingly, reputation is the collected and processed information about one partner's former behavior as experienced by others.

Josanga [25] gives a survey of trust and reputation systems and points out that there is significant difference between trust and reputation. Trust is a subjective phenomenon which is based on various factors or evidences. In fact, firsthand experience always carries more weight than the secondhand trust recommendation or reputation. Since the nodes in the data collection layer of IoT/CPS usually are heterogeneous and mobile, trust establishment model can significantly stimulate collaboration among distributed computing and communication entities, facilitate the detection of untrustworthy entities, and assist decision-making process of various protocols.

Based on [24] and [25], we try to give the following more detailed trust and reputation definitions towards IoT/CPS.

Definition 3. In a wireless network of IoT/CPS, a node S's trust in another node P is the subjective expectation of node S receiving positive outcomes through the transactions with node P.

Definition 4. In IoT/CPS, a node S's reputation is the global perception of its trustworthiness in the wireless network. Furthermore, the trustworthiness can be evaluated from its past and current behaviors.

Trust in this paper describes the relying node's trust in a service or resource provider node and it is relevant when the relying party is a user seeking protection from malicious or unreliable service providers.

3.2. Relationship between Trust and Reputation

The term 'trust' and 'reputation' have strongly linked meanings. Especially in WSNs of IoT/CPS, trust is often defined as an abstract acquired attribute relative to some sensor nodes which is due to the amount of reputation held by such sensor nodes.

By making full use of observing good long-term behavior, reputation ratings can be improved; therefore, trust relationships will be easily established [5]. In real-life communities, trust is the consequence of the satisfaction of certain desired properties [26].

As discussed in [25], the concept of reputation is closely linked to that of trust; however, there is a clear and significant difference. A node *S* can trust in another node *P* because of its good reputation. Likewise, node *S* can also trust in node *P* in spite of its bad reputation. Reputation is usually inspired by the past behaviors observed. Trust reflects the relying party's subjective view of an entity's trustworthiness, whereas reputation is a score which can be seen by the whole community.

Note that, in this paper, trust is considered as a subjective probability value while reputation is regarded as an objective and acknowledged value in a specific community context.

3.3. Fuzzy Trust Model Description

An entity's trustworthiness is the quality indicator of the entity's services, which is used to predict the future behavior of the entity (stored in sensors or sensor-embedded things). Intuitively, if it is trustworthy enough, the entity will provide good services for future transactions. In most trust models, the domain of trustworthiness is assumed to be [0, 1].

Since the key issue in investigating fuzzy problems is to establish membership functions (membership degrees) by employing the fuzzy set theory, we have to create the mathematical model of fuzzy trust firstly [27].

Suppose that $SN = \{SN_1, SN_2, \cdots, SN_n\}$ is a problem domain of the fuzzy trust model. Note that, $SN_i (i = 1,2,\cdots,n)$ is a subset in the corresponding domain. Then we can get the following mapping,

$$\begin{cases} MappingFuction : SN \times SN \to [0,1], \\ (SN_i, SN_j) \to \psi(SN_i, SN_j) \in [0,1]. \end{cases} \quad (1)$$

where $\psi(SN_i, SN_j)$ represents the degree of trust relationship between SN_i and SN_j. $MappingFuction$ is a fuzzy relation mapping from $SN \times SN$ to $[0,1]$.

In the proposed scheme, a neighbor monitoring process is used to collect information of the package forwarding behaviors of the neighbors. Each sensor node in the network maintains a data forwarding transaction table as follows,

$$DFT_{i,j} =< Souce, Destination, RF_{i,j}, F_{i,j}, TTL > \quad (2)$$

where *Souce* is the trust and evaluation evaluating nodes, *Destination* is the evaluated destination nodes, $RF_{i,j}$ denotes the times of successful transactions which node SN_i has made with node SN_j, and $F_{i,j}$ denotes the positive transactions.

3.4. Trust Evaluation Metrics

Within the realm of IoT/CPS security, we interpret the concept of trust as a relation between entities stored in sensor nodes that participate in various protocols. Trust relations are based on evidence or reputation created by the previous interactions of entities within a protocol. Each node employs a neighbor monitoring process in order to collect information about the packet forwarding behaviors of the neighbor nodes. Furthermore, each node is capable of overhearing the transmissions of its neighbors in the promiscuous mode. Each node independently overhears its neighboring nodes packet forwarding activities. This overhearing is related to the proportion of correctly forwarded packets with respect to the total number of packets to be forwarded during a fixed time window. Then, each node in the network maintains a data forwarding information table. The table includes only the data forwarding transaction information by overhearing its neighboring nodes.

In the proposed model, we consider the following trust evaluation metrics for the establishment and validation of the proposed trust management model.

(1) End-to-end packet forwarding ratio (EPFR). EPFR is defined as the ratio between the numbers of packets received by the application layer of destination nodes to the numbers of packets sent by the application layer of the source node. The EPFR can be calculated by

$$EPFR = \frac{\sum_i^k RECV_i}{\sum_i^n SEND_i}, 0 \le k \le n. \quad (3)$$

where $RECV_i$ and $SEND_i$ denote the packages received and sent by the *i*-th destination node and the *i*-th source node, respectively. And *k* denotes the successful receiving times, while *n* denotes the total times of packages sending.

(2) AEC. The key criterion for the design of a WSN in IoT/CPS Infrastructure is the energy consumption. In order to research and analyze the energy consumption of our TRM-IoT model, we define the energy consumption metric as follows,

$$AEC = \frac{\sum_{i=1}^{n} consume_i}{\sum_{i=1}^{n} send_i + recv_i + \tau} \quad (4)$$

where $send_i$ and $recv_i$ denotes the energy consumption when the *i*–th sensor node sending and receiving messages, respectively. $consume_i$ denotes the total energy cost of consumption the trust and reputation values of the corresponding sensor node. And τ represents the other energy consuming which is used to maintain the normal running of the node itself.

(3) PDR. In fact, the package delivery ratio (PDR) is affected by the packet loss and packet retransmissions. Packet loss may occur for many reasons. In this paper we only focus on the behavior that an intermediate node intentionally drops the received data packets instead of forwarding them to the next hop node.

3.5. Reputation Evaluation

Node SN_i evaluates the reputation of node SN_j with which it tries to make transactions by rating each package forwarding process as either positive or negative, depending on whether SN_j has completely done the transaction correctly.

As discussed above, we use *Con* to describe the evaluation of the whole metrics in order to judge whether this transaction is successful. The *Con* can be computed by

$$Con = [EPFR, AEC, PDR] \cdot \begin{bmatrix} \alpha \\ \beta \\ \gamma \end{bmatrix} = \alpha \cdot EPFR + \beta \cdot AEC + \gamma \cdot PDR \quad (5)$$

where α, β, γ represent the corresponding aspect weights of the different resources. We also define a parameter $Sat_{Threshold}$ to describe the satisfaction degree. That means, if $Con < Sat_{Threshold}$, then it indicates that node SN_i get a negative reputation evaluation to node SN_j; if $Con \geq Sat_{Threshold}$, it indicates that node SN_i gets a positive reputation evaluation to node SN_j.

The reputation evaluation of all interactions from node SN_i to node SN_j is defined as follows,

$$\delta = \frac{F_{i,j}}{RF_{i,j}} \in [0,1]. \quad (6)$$

Reputation evaluation is the basis of trust management. In our trust model, the reputation is evaluated considering three metrics, EPFR, AEC and PDR. Compared with other reputation evaluation methods, we consider more factors which can more accurately evaluate the behaviors of nodes according to specific characteristics of IoT/CPS.

3.6. Local Trust Evaluation

From different points of view, trust can usually be categorized into different classes: direct trust and indirect trust. When we say node SN_j is trustworthy or untrustworthy for the node SN_i, it means that there must be a trust and reputation model between node SN_j and node SN_i. If a trust relationship statement is based on the reputation of direct observations on node SN_j, the corresponding model mentioned above is the direct trust model.

Since the direct trust relationship also has some significant fuzzy properties, we can describe the direct trust model employing the fuzzy theory. According to the data forwarding transaction table, fuzzy reputation membership based direct trust model can be defined as

$$T_{i,j}^{d} = \frac{\delta}{\delta + \alpha(1-\delta) + \frac{\lambda}{RF_{i,j}}} \quad (7)$$

where α denotes the weight of the past negative behavior that can be regulated to punish the malicious node action. λ represents the uncertainty trust for the weight value α.

Since the behavior of a node is not always constant but often changes in time and volatility, it is significant that the recent events are more credible than the historical events. Let $T_{i,j}^{d}(t-1)$ be the most recent trust evaluation and $T_{i,j}^{d}(\Delta t)$ be the past trust evaluation during a time interval Δt. We combine the recent events and historical events to update $T_{i,j}^{d}(t)$:

$$\begin{cases} T_{i,j}^{d}(t) = \omega_1 \cdot T_{i,j}^{d}(t-1) + \omega_2 \cdot T_{i,j}^{d}(\Delta t), \\ \omega_1 = 1 - \frac{1}{2} \cdot \zeta, \forall \zeta \in [0,1] \\ \omega_1 + \omega_2 = 1. \end{cases} \quad (8)$$

Therefore, the new trust of $T_{i,j}(t)$ is dependent on the three factors, $T_{i,j}^{d}(t-1)$, $T_{i,j}^{d}(\Delta t)$ and ζ. Then we can get the local trust updating equation,

$$T_{i,j}^{d}(t) = (1-\frac{1}{2}\cdot\zeta)\cdot T_{i,j}^{d}(t-1) + \frac{1}{2}\cdot\zeta\cdot T_{i,j}^{d}(\Delta t)\,. \qquad (9)$$

However, it is arbitrary and difficult to decide whether a mobile sensor node' behavior is good or bad only based on a few interactions. Therefore, we must have an interaction threshold value of interaction times $C_{threshold}$. Consequently, the fuzzy direct trust evaluation can be computed by

$$T_{i,j}^{d} = \begin{cases} \frac{1}{2}\times(1+\frac{\delta}{C_{threshold}}), RF_{i,j} < C_{threshold} \\ \frac{\delta}{\delta+\alpha(1-\delta)+\frac{\lambda}{RF_{i,j}}}, RF_{i,j} \geq C_{threshold} \end{cases} \qquad (10)$$

When node SN_i and node SN_j has no direct relationship and cannot establish direct communication channel to exchange data, node SN_i can evaluate the trust of node SN_j based on the recommendation trust of a third party node SN_k.

As is discussed in [28], the recommendation trust and reputation model can be divided into two categories, transitivity and consensus recommendation trust and reputation management models.

The fuzzy transitivity recommendation trust and reputation model defines a degree of recommending relationship between node SN_i and node SN_j. $RR_{i,j}$ denotes the number of request recommendations, and $HR_{i,j}$ represents the number of the positive recommendations. $CR_{threshold}$ is defined as threshold value of the recommendation times. Therefore, the membership function for fuzzy recommendation trust model is defined as:

$$T_{k,j}^{r} = \begin{cases} \frac{1}{2}\times(1+\frac{\eta}{CR_{threshold}}), RR_{i,j} < CR_{threshold} \\ \frac{\eta}{\eta+\alpha(1-\eta)+\frac{\lambda}{RR_{i,j}}}, RR_{i,j} \geq CR_{threshold} \end{cases} \qquad (11)$$

where $\eta = \frac{HR_{i,j}}{RR_{i,j}} \in [0,1]$.

The different sensor nodes may provide diverse recommendations on the same nodes. That means, different nodes may have the different or even opposite trust evaluations towards the same sensor node. Assume that node SN_k gives the recommendation trust evaluation of $T_{k,j}^{r}$ and node SN_t provides the recommendation trust evaluation of $T_{t,j}^{r}$ to node SN_j. Also there have two direct trust relationships between node SN_i and node SN_k, node SN_i and node SN_t, respectively.

Here we combine the two recommendation trust evaluation and the two direct trust evaluations to make a relatively objective assessment for node SN_j ,

$$T_{i,j}^{i} = (D(SN_i, SN_k) \wedge R(SN_k, SN_j)) \cup (D(SN_i, SN_t) \wedge R(SN_t, SN_j)), \forall SN_k, SN_t \in SN. \quad (12)$$

Therefore, in a similar way, the fuzzy membership function of *n*-level fuzzy consensus recommendation trust and reputation model can be defined as

$$T_{i,j}^{i} = \underbrace{(R \circ D) \cup (R \circ D) \cup \cdots (R \circ D)}_{n} \quad (13)$$

In conclusion, the fuzzy local trust relationship can be calculated through the combination based on direct and indirect trust evaluation by

$$\begin{cases} T_{i,j} = X \cdot T_{i,j}^{d} + Y \cdot \sum_{k} \left(T_{i,k}^{d} \cdot T_{k,j}^{r} \right), 1 < Y < X < 0 \\ X + Y = 1 \end{cases} \quad (14)$$

where *X*, *Y* denotes the weight of direct trust value and indirect trust value in the whole fuzzy local trust value, respectively. Note that, $1 < Y < X < 0$ means that compared with the indirect recommendations, our fuzzy local trust evaluation is more focused on the direct observations. Since nodes in IoT/CPS may dynamically join in the WSNs and quit the WSNs, it stands to reason that the long historical recommendations should have relatively small weights in the Equation (14).

3.7. Global Trust Evaluation

In fact, node SN_i may have not only the direct observation on the node SN_j , but also indirect experiences by asking its acquaintances. Therefore, there are two fuzzy trust models between node SN_i and node SN_j , fuzzy direct trust model and fuzzy indirect trust model.

Obviously, if a node wants to obtain more accurate trust value with another node, it must integrate more direct and indirect experiences. Note that, the direct trust may vary with time. In order to get the most accurate trust value, we must discover the most wide indirect trust set. In this paper, the fuzzy global trust relation is defined as a union of fuzzy direct trust relation, 1-level fuzzy indirect trust relationship, 2-levels indirect trust relationship, and *n*-levels fuzzy indirect trust relation ($n \to \infty$).

Let us consider an example of the fuzzy trust relationship evaluation between node SN_i and node SN_j in a community of (*n+16*) nodes, as shown in Fig.1. In the example the source node SN_i has five routes to the destination node SN_j . If we want to obtain the most accurate trust evaluation between them, all of the five routes must be contained and evaluated. Therefore, the fuzzy global trust relationship evaluation can be calculated by

$$T_{i,j} = D + R \circ D + R^2 \circ D + R^3 \circ D + R^n \circ D \\ = (SN + R + R^2 + R^3 + R^n) \circ D. \quad (\mathbf{15})$$

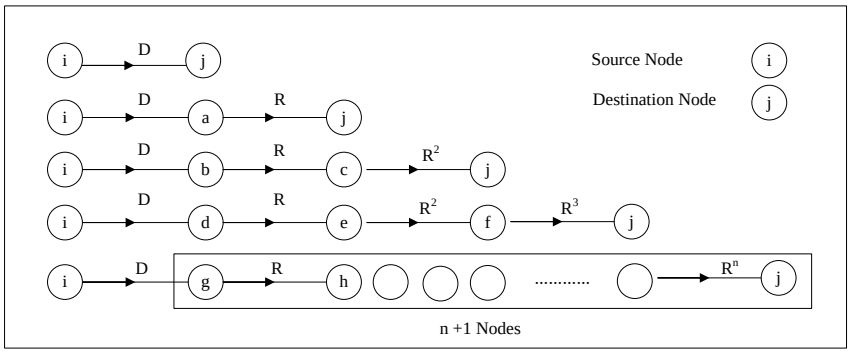

Fig. 1. Illustration of the fuzzy global trust relationship evaluation between node SN_i and node SN_j

Obviously, node SN_i can make the fuzzy global trust evaluation to node SN_j which is computed as,

$$T_{i,j} = \lim_{n \to \infty} \left[(SN \cup R \cup R^2 \cup \cdots \cup R^n) \circ D \right]. \quad (\mathbf{16})$$

WSNs of IoT/CPS have dynamic topologies, bandwidth constraints, variable capacity links, energy constrained operation, and limited physical security. Dynamics make it hard to evaluate behaviors, because routes in this kind of network change frequently. In this case, fuzzy global trust evaluation reflects the past interactions of the community with the corresponding node being evaluated. This evaluation is globally available to all member nodes of the community and updated each time a member node issues a new evaluation of a sensor node.

4. Simulation and Discussion

4.1. NS-3 Setup

In this paper, we perform our simulation on a NS-3 simulator [29]. Every plot is taken as an average of ten different runs. And each run is executed with source and destination pairs selected randomly from the WSN.

Since we rely on TCP acknowledgments and retransmission as indications of successful and failed package delivery events, respectively, we employ AODV protocol [30] as the communication protocol in our simulation. The

NS-3 setup parameters and model configuration parameters are listed in Table 1 and Table 2.

Table 1. NS-3 Setup Parameters.

Parameter	Value
Simulator	NS-3
MAC Layer	IEEE 802.11
Nodes Number	300
Node Placement	Random, uniform
Package Size	512 bytes
Maximum Connection	30
Transmission Range	250
Application Traffic	CBR

Table 2. Model Configuration Parameters.

Parameter	Value
ζ	0.7
α	0.75
λ	4.6
Δt	0.5
$C_{threshold}$	12
$CR_{threshold}$	12
Reply Delay	60ms

Note that, since the maximum connection number of a service node is no more than 30, $C_{threshold}$ and $CR_{threshold}$ have to be initialized as a value which is no more than $0.5\times(0+MAX\_Connections)=15$. Higher value of the two parameters will reduce the success rate of recommendations from neighbor nodes.

In this simulation experiment, we divide the sensor nodes into two types, good nodes and malicious nodes. Moreover, according to the behavior in route discovery, route maintenance and data forwarding, malicious nodes can be divided into two categories further. For the first type (Type 1): the malicious nodes do not perform the package forwarding function; for the second type (Type 2), the malicious nodes do not participate in the route discovery phase. Those malicious nodes are selected randomly in each run according to the setup percentage, as shown in Fig.2.

The trust and reputation relationship is initialized randomly at the very beginning of simulation. Therefore, after several rounds, we establish a similar behavior and fuzzy theory-based trust and reputation model for WSNs of IoT/CPS, where each node develops a direct reputation for each other node by making direct observations and indirect reputation between

individuals which are set up on recommendations of other individuals about these other nodes in the neighborhood.

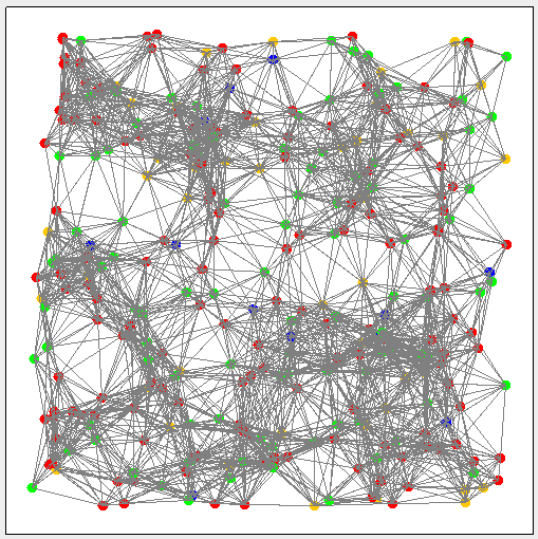

Fig. 2. The random distribution of malicious and misbehavior nodes in the simulations.

4.2. EPFR

End-to-end packet forwarding ratio (EPFR) is defined as the ratio between the number of packets received by the application layer of destination nodes to the number of packets sent by the application layer of the source node. As discussed in [28], this parameter significantly reflects the effect on the drop ratio, the path interruption repair, sending buffer overflow, interface queue overflow, the conflict MAC packet and end-to-end packet in the process of data packet. The lost packets cover all packet losses due to drops, route failures, congestion and wireless channel losses.

As shown in Fig. 1, some sensor nodes are set to be malicious nodes randomly. The percentage of malicious sensor nodes is increased and taken values from 10% to 60%, while other nodes of the network behave benevolently. The results indicate that some individual selfish nodes obviously result in the linear regression of EPFR.

Therefore, the secure mechanisms mainly focus on Type 1 to correctly perform the packet forwarding function. When 60% of the nodes follow Type 1 and Type 2, EPFR degrades by 53% and 82%, respectively. However, when the number of normal nodes becomes so smaller to a certain degree, such as 50%, the corresponding EPFR will decrease significantly.

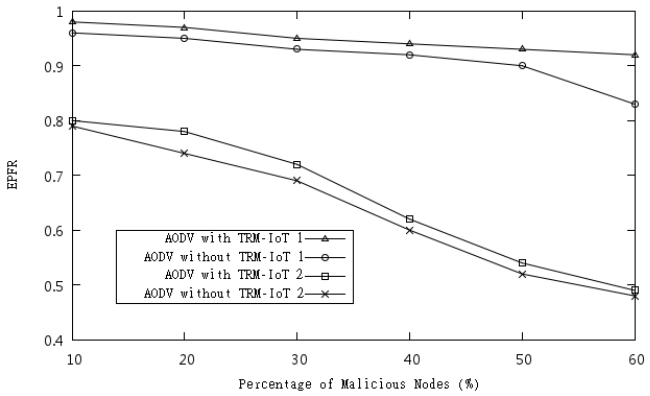

Fig. 3. The relationship between EPFR and different percentage of malicious nodes.

As shown in Fig. 3, EPFR can be degraded by malicious nodes. Through employing the proposed behavior-based trust and reputation model, the WSNs of IoT/CPS performance can be enhanced, since it enables the best loyal route selection process to avoid asking the less trustworthy nodes to forward messages.

By examination of EPFR, we can see improvements by BRM-IoT under attacks of type 1 and 2, compared to the original AODV protocol. Moreover, as the percentage of malicious nodes increases, Type 2 has a less obvious influence on EPFR than Type I.

4.3. AEC

As shown in Fig. 4, we make malicious nodes which change between 10% and 60% of the sensor nodes in the network, increasing 10% for each running of the experiment, while the other nodes of the network behave virtuously. Since any malicious node does not participate in the route discovery phase of the AODV protocol or it not be honestly execute data packets forwarding, AEC of malicious nodes is less than that of other normal nodes.

The experimental results show that even if individual malicious nodes of type 1 seriously affect the network performance, the trust and reputation mechanism, which prompts the times of nodes transmitting data packets, is the basic security need for the non-malicious routing in WSNs. TRM-IoT model effectively cubes the malicious nodes, and significantly reduces the energy consumption of good sensor nodes.

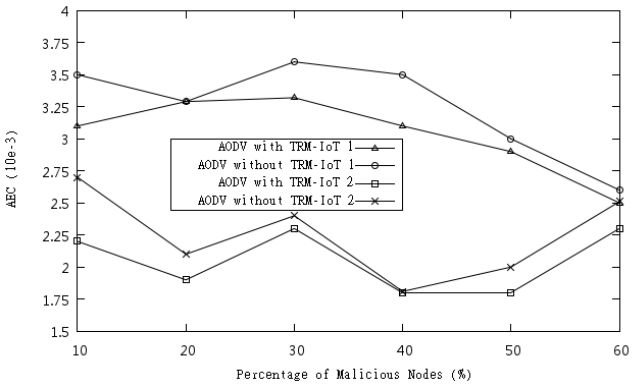

Fig.4. The relationship between AEC and different percentages of malicious nodes.

4.4. Package Delivery Ratio

Fig. 5 shows a comparison between the proposed trust and reputation scheme for IoT/CPS, TRM-IoT, and two existing trust models based on reputation mechanisms, namely DRBTS [10] and BRTM-WSN [11], in terms of PDR. In fact, package delivery ratio (PDR) is affected by packet loss and packet retransmissions. Packet loss may occur for many reasons. In this paper, we focus on the behavior that an intermediate node intentionally drops received data packets instead of forwarding them to the next hop node. From Fig. 5, we can see that the proposed trust and reputation model outperforms the other two schemes especially at higher loads on the network.

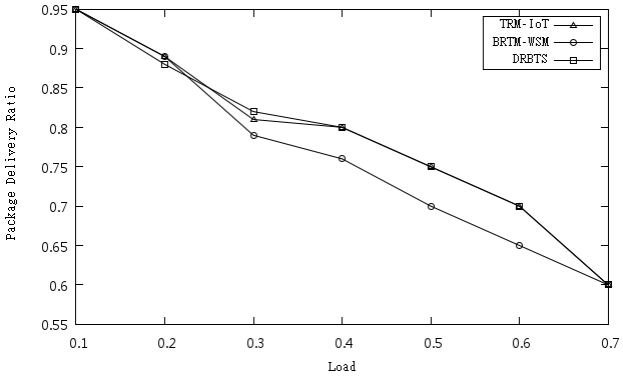

Fig. 5. The relationship between load and package delivery ratio.

4.5. Convergence Speed

Convergence speed (CS) is defined as the least number of cycles required making the number of the failed data forwarding transaction. That is, the greater of the CS, the more unfair represents that if a trust model works, the good nodes can be differentiated from the misbehavior nodes by their trust values after a few transaction cycles [31]. At the beginning, all sensor nodes have the same initial trust value, and the source sensor nodes randomly select a node for data packet forwarding. After a small numbers of transactions, the good nodes can get the higher trust value than the other bad malicious nodes.

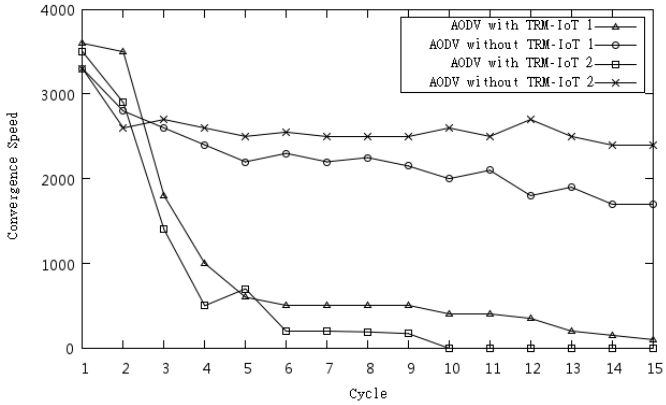

Fig. 6. The relationship between cycles and convergence speed.

The failure numbers of all data forwarding packets of the normal nodes reflect CS with the change of the simulation cycles. Since nodes always select the nodes with the higher trust values, the fewer cycles the faster the convergence of the model.

Fig. 6 describe TRM-IoT almost completely eliminates the failure of data packet forwarding after the first eight cycles in WSNs.

However, selfish nodes of Type 1 intentionally drop the received packets instead of forwarding them, and increase in the failure ratio of the normal packet forwarding increasing. The system is not the very good convergence, and has slow convergence speed in comparison with the selfish nodes of Type 2.

4.6. Detection Probability

Detection Probability (DP) indicates that whether a trust and reputation model can better handle incorrect recommendations from the third party. In Fig. 7, BRTM-WSN [11] model performs better than DRBTS [10] model. This is

because BRTM-WSN model can better handle incorrect recommendations from the third party.

Moreover, TRM-IoT model performs well than the other two existing models. This is mainly because TRM-IoT model considers the possible estimation error when evaluating the trust and reputation values. Therefore, compared with the two other existing models, our model, TRM-IoT, has better performance.

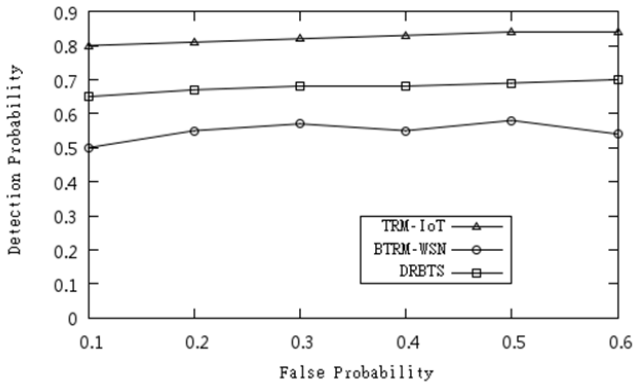

Fig. 7. The relationship between false probability and detection probability.

5. Conclusion and Future Works

Since WSNs are to be completely integrated into Internet or Next Generation Internet as a core part of IoT/CPS, it is necessary to consider various security challenges that come with IoT/CPS, such as the detection of malicious attacks.

A trust and reputation model is recognized as an important approach to defend a large distributed sensor networks in IoT/CPS against malicious node attacks, since trust establishment mechanisms can stimulate collaboration among distributed computing and communication entities, facilitate the detection of untrustworthy entities, and assist the decision-making process of various protocols.

Based on in-depth understanding of trust establishment process and quantitative comparison among trust establishment methods, this paper present a trust and reputation model TRM-IoT to enforce things cooperation in a WSN of IoT/CPS based on their behaviors. The potential benefits of employing fuzzy sets to manage trust and reputation relationships are analyzed according to the excellent NS-3 simulations.

Although the proposed model TRM-IoT has better performance compared with two other existing models, we have increasingly aware of the necessity

of eliminating the influence upon the evaluation results affected by malicious recommendation and defamation behaviors of the third party. The mechanism by which global trust is updated while local trust changes can be improved in order to be more efficient in future works.

Acknowledgement. This work is supported by the National Natural Science Foundation of China under Grant No. 60903159 and the Fundamental Research Funds for the Central Universities under Grant No. N100604012.

References

1. Wolf, W.: Cyber-Physical Systems. Computer, Vol. 42, No. 3, 88-89. (2009)
2. Zhu, Q., Wang, R. C., Chen Q., Liu Y., Qin W. J.: IOT Gateway: Bridging Wireless Sensor Networks into Internet of Things. In Proc. of 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, USA, CA，Los Alamitos, 347-352. (2010)
3. Khoo, B.: RFID- from Tracking to the Internet of Things: A Review of Developments. In Proc. of 2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing, Hangzhou, 533-538. (2010)
4. Joel, J. P. C. Rodrigues, Paulo, A. C. S. Neves.: A survey on IP-based wireless sensor network solutions. International Journal of Communication Systems, Vol. 23, Issue 8, 963-981. (2010)
5. Sun, Y. L., Yang, Y.: Trust establishment in distributed networks: Analysis and modeling. In Proc. of 2007 IEEE International Conference on Communications, ICC'07, United Kingdom, Glasgow, 1266-1273. (2007)
6. Sun, Y., Yu, W., Han, Z., Liu, K.: Trust modeling and evaluation in ad-hoc networks. In Proc. of Global Telecommunications Conference 2005 GLOBECOM'05, Vol. 3, 1862-1867. (2005)
7. Buttyan, L., Hubaux, J. P.: Stimulating cooperation in self-organizing mobile ad hoc networks. Mobile Networks and Applications, Vol. 8, No. 5, 579-592. (2003)
8. Boukercha, A., Xua, L., EL-Khatibb, K.: Trust-based security for wireless ad hoc and sensor networks. Computer Communications Vol. 30, Issues 11-12, 2413-2427. (2007)
9. Chen, H. G., Wu, H. F., Zhou, X. and Gao, C. S.: Agent-based Trust Model in Wireless Sensor Networks. In Proc. of the Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, 119-124. (2007)
10. Srinivasan, A., Teitelbaum, J. and Wu, J.: DRBTS: Distributed Reputation-based Beacon Trust System. In Proc. of 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC'06), 277-283. (2006)
11. Marmol, G., Perez, M.: Providing trust in wireless sensor networks using a bio-inspired technique. Telecommunication Systems, Vol. 46, Number 2, pp 163-180. (2010)
12. Buchegger, S., Boudec, J. Y. L.: Performance analysis of the confidant protocol. In Proc. of MobiHoc'02: Proceedings of the 3rd ACM international symposium on Mobile Ad-hoc networking & computing, ACM, New York, NY, USA, 226-236. (2002)

13. He Q., Wu D., Khosla P.: Sori: A secure and objective reputation-based incentive scheme for ad-hoc networks. In Proc. of 2004 Wireless Communications and Networking Conference, Vol. 2, 21-25, 825-830. (2004)
14. Zhong, S., Chen, J., Yang, Y.: Sprite: a simple, cheat-proof, credit-based system for mobile ad-hoc networks. In Proc. of INFOCOM 2003, Twenty- Second Annual Joint Conference of the IEEE Computer and Communications Societies, Vol. 3, 1987-1997. (2003)
15. Hui, J. W., Culler, D. E.: Extending IP to Low-Power Wireless Personal Area Networks. IEEE Internet Computing, Vol. 12, No. 4, 37-45. (2008)
16. Liekenbrock, D.: The Internet of Things State-of-the-Art and Perspectives for Future Research. Communications in Computer and Information Science, Vol. 32, No. 2, 10-15. (2009)
17. Luigi, A., Antonio, I., Giacomo, M.: The Internet of Things: A survey. Computer Networks, Vol. 54, No. 15, 2787-2805. (2010)
18. Eshenauer, L., Gligor, V. D.: A Key-Management Scheme for Distributed Sensor Network. In Proc. of 9th ACM Conf. Computer and Comm. Security (CCS'02), United states, Washington, DC, 41-47. (2002)
19. Liu, D., Ning, P., Rongfang, L. I.: Establishing Pairwise Keys in Distributed Sensor Networks. ACM Transactions on Information and System Security, Vol. 8, No. 1, 41-77. (2005)
20. Zhu, S., Seia S., Jajodia S.: LEAP+: Efficent Security Machanisms for Large-Scale Distributed Sensor Networks. ACM Transactions on Sensor Networks, Vol. 2, 500-528. (2006)
21. Liu, F., Cheng, X., Ma, L., Xing, K.: SBK: A Self-Configuring Framework for Bootstrapping Keys in Sensor Network. IEEE Transactions on Mobile Computing, Vol. 7, No. 7, 858-868. (2008)
22. Loree, P., Nygard, K., Du, X. J.: An Efficient Post-Deployment Key Establishment Scheme for Heterogeneous Sensor Networks. In Proc of 2009 Global Telecommunications Conference, GLOBECOM 2009, United states, HI, Honolulu, 1-6. (2009)
23. Sun, Y., Trappe, W., Liu, K. J. R.: A scalable multicast key management scheme for heterogeneous wireless networks. IEEE/ACM Transactions on Networking, Vol. 12, No. 4, 653-666. (2004)
24. Gambetta, T.: Can we trust trust? In: D. Gambetta (Ed.), Trust: making and Breaking Cooperative Relations, Basil Blackwell, Oxford, 213-238. (1990)
25. Josang, A., Ismail, R., Boyd, C.: A survey of trust and reputation systems for online service provision. Decis. Support Syst, Vol. 43, No. 2, 618-644. (2007)
26. Better Busines Bureau. [Online]. Available: http://www.bbb.org.
27. Azzedin, F., Ridha, A., Rizvi, A.: Fuzzy trust for peer-to-peer based systems. In Proc. of World Academy of Science, Engineering and Technology, Vol. 21, 123-127. (2007)
28. Luo, J. H., Liu, X., Fan, M. Y.: A trust model based on fuzzy recommendation for mobile ad-hoc networks. Computer Networks, Vol. 53, 2396-2407. (2009)
29. NS-3. [Online]. Available: http://www.nsnam.org/index.html.
30. Perkins, C., Belding-Royer, E., Das, S.: Ad hoc on-demand distance vector (AODV) routing, IETF RFC 3561, July 2003.
31. Griffiths, N., Chao, K. M., Younas, M.: Fuzzy trust for peer-to-peer systems. In Proc. of 26th IEEE International Conference on Distributed Computing Systems Workshop, Portugal, Lisboa, 73-73. (2006)

Dong Chen is a PhD candidate at the school of Information Science and Engineering, Northeastern University, Shenyang, China. He received his MSc in Computer Science from Northeastern University in 2010. His current researches interests include Internet of Things, Cyber Physical System.

Guiran Chang received his Ph.D. degree in electrical engineering from the University of Ten-nessee, Knoxville, Tennessee in 1991. He is currently a Professor at the computing center of Northeastern University, China. His current research interests include computer networks, Internet of Things and information security.

Dawei Sun is a PhD candidate at the school of Information Science and Engineering, North-eastern University, China. He received his MSc in Computer Science from Northeastern University in 2009. His current researches interests include cloud computing and virtualization technology.

Jiajia Li is a PhD candidate at the school of Information Science and Engineering, Northeastern University, China. He received his MSc in Computer Science from Northeastern University in 2010. His current researches interests include Spatial-Temporal Database and XML Database.

Jie Jia received her Ph.D degree in computer science from Northeastern University, China. She is currently an Associate Professor at the School of Information Science and Engineering, Northeastern University, China. Her research interests are mainly on RFID systems and Wireless Sensor Network.

Xingwei Wang received his Ph.D degree in computer science from Northeastern University, China in 1998. He is currently a Professor at the School of Information Science and Engineering, Northeastern University. His research interests are mainly on routing algorithms and protocols, mobility management in NGI.

Received: March 3, 2011; Accepted: April 22, 2011.