An Energy-aware Trust Derivation Scheme with Game Theoretic Approach in Wireless Sensor Networks for IoT Applications

Junqi Duan, Deyun Gao, *Member, IEEE*, Dong Yang, Chuan Heng Foh, *Senior Member, IEEE*, and Hsiao-Hwa Chen, *Fellow, IEEE*

***Abstract*—Trust evaluation plays an important role in securing wireless sensor networks (WSNs) which is one of the most popular network technologies for the Internet of Things (IoT). The efficiency of the trust evaluation process is largely governed by the trust derivation as it dominates the overhead in the process, and performance of WSNs is particularly sensitive to overhead due to the limited bandwidth and power. This paper proposes an energy-aware trust derivation scheme using game theoretic approach, which manages overhead while maintaining adequate security of WSNs. A risk strategy model is first presented to stimulate WSN nodes' cooperation. Then, a game theoretic approach is applied to the trust derivation process to reduce the overhead of the process. We show with the help of simulations that our trust derivation scheme can achieve both intended security and high efficiency suitable for WSN-based IoT networks.**

***Index Terms*—Internet of Things; game theory; trust evaluation; energy-awareness; security; wireless sensor network**

I. Introduction

With the recent advancements in sensor technology, wireless communications and embedded system, we witness a rapid growth in the number of sensing capable devices connected to the Internet. The needs for mobility and convenience access also promote the use of wireless for the Internet connection. These recent developments have made wireless sensor network (WSN) one of the most important network technologies in Internet of Things (IoT).

A practical WSN for IoT must be capable of rapid deployment and self-organization to perceive the physical world at anywhere and anytime. This has created research challenges and triggered significant research attentions in recent years [1] [2] [3]. With the research efforts and contributions, WSNs have become an attractive platform for many applications [5] [6]. Despite the advancements in WSN development, there are still a number of issues that remain unsolved in WSNs.

Security is one of the main challenges for the practical implementation of IoT [1], especially for a WSN-based IoT. Traditionally, functions that drive WSNs, such as medium access control (MAC) and routing protocols, always assume that the operating environment is trustworthy [7]. However, this assumption is not realistic in many cases. WSNs are often deployed in remote environments which is susceptible to attacks and difficult to protect physically. Deployed sensor nodes may be tampered without detection, or hostile nodes may be introduced covertly into a WSN to compromise the security of the WSN. Furthermore, the sensor nodes that belong to different manufacturers or service providers may not completely cooperate with each other. For example, they may be configured for resource conservation which operate in a selfish manner. All of these can lead to performance degradation or malfunctioning of WSNs.

Cryptographic primitives represent a practical method to deal with the security issues in many research areas [8] [9] [10]. Unfortunately, their application to WSN-based IoT has been limited. The specific reasons can be summarized as follows: Firstly, most cryptographic algorithms, especially the asymmetric encryption processes, require high computational capabilities and power consumption [11] [12]. However, the low-cost sensor nodes usually are limited in memory size, energy capacity, and computational capabilities. Secondly, many practical encryption and authentication processes require fixed infrastructures or centralized administrations to operate [13] [14], which are often not present in WSNs. Finally, the sensor nodes deployed in an unattended area may be compromised by adversaries through physical means. Once the keys are leaked, all the security mechanisms immediately become ineffective. In other words, cryptographic mechanisms are vulnerable to attacks launch internally.

Due to the low complexity computation and high resistance to the internal attacks, trust evaluation is an effective solution to the above issues in the public key infrastructure (PKI) [15] [16]. Consequently, trust plays an important role in security mechanisms for WSNs. Although there are different definitions for trust in the previous works, the trust of nodes is normally composed of *direct trust* and *indirect trust*. The direct trust is based on direct observations of each node that participates in data communications, and the indirect trust is obtained from recommendations of other nodes. Besides, the trust evaluation process can also be divided into two parts: *trust derivation* and *trust computation* [17]. The former refers to the process of collecting trust information, while the latter represents the process of calculating the synthesis trust value based on the observed direct trust and collected indirect trust.

Although many trust models have been proposed in recent

Junqi Duan (e-mail: duanjunqi@bjtu.edu.cn), Deyun Gao (e-mail: gaody@bjtu.edu.cn), and Dong Yang (e-mail: dyang@bjtu.edu.cn) are with the National Engineering Laboratory for Next Generation Internet Interconnection Devices, School of Electronic and Information Engineering, Beijing Jiaotong University, China. Chuan Heng Foh (e-mail: c.foh@surrey.ac.uk) is with the Centre for Communication Systems Research, Department of Electronic Engineering, University of Surrey, UK. Hsiao-Hwa Chen (e-mail: hshwchen@ieee.org) is with the Department of Engineering Science, National Cheng Kung University, Taiwan.

The paper was submitted on October 23, 2013 and revised on March 26, 2014.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2014.2314132, IEEE Internet of Things Journal

years [18] [19] [20], most of them only focus on trust computation. Since the accuracy of trust computation relies on the amount of received recommendations, the trust derivation process that defines how recommendations are disseminated plays an important role. Given the bandwidth and power limitation in WSNs, the impact of recommendation dissemination on the overall performance of WSNs is relatively high. Therefore, designing an efficient trust derivation scheme is part of a critical issue in the development of WSN-based IoT networks.

In this paper, we propose an energy-aware trust derivation scheme for WSNs which aims to minimize the energy consumption and latency of the network under the premise of security assurance. Firstly, we provide a method of risk strategy analysis to stimulate the nodes' cooperation. By utilizing this method, we derive the optimal number of recommendations. Secondly, TDDG (trust derivation dilemma game) is introduced into the trust derivation process to reduce the overhead of the network. Based on the mixed strategy Nash equilibrium, the optimal ratio of gain to cost and the probability of the selected strategy are discussed. Finally, by conducting extensive simulations, we show that our approach can not only maintain the desirable security of the network, but also significantly reduce the energy consumption and latency of the network compared with traditional mechanisms.

The rest of this paper is organized as follows. We first discuss some relevant previous works in Section II. Section III describes our system model. Then, a risk strategy model is proposed in Section IV, followed by the introduction of our game theoretic approach in trust derivation in Section V. The simulation results and performance evaluation are presented in Section VI. Finally, Section VII draws some important conclusions and discusses potential future works.

II. Related Works

With the growing attention in the field of security for WSNs and IoT, there has been an increased effort in the research on trust evaluation in recent years [21] [22] [23] [33]. In order to improve the accuracy and precision of trust computation, most trust models focused on the trust computational process by adopting mathematical analysis and modeling tools, such as D-S theory and beta probability distribution model [21]. However, as the algorithms of trust computation do not generally contribute much to the overall operational overhead, these models will not have much impact on energy consumption. By contrast, the trust derivation process in which data interactions influence significantly to the energy consumption and latency of trust evaluation [24]. This paper makes contribution to the trust derivation process.

In trust evaluation systems, a source node or an evaluating node that launches the trust derivation process should obtain all trust data from others for trust computation. Trust data may be obtained directly or indirectly. A source node may make direct observation on its neighbors to determine the trust data easily by, say intrusion detection mechanisms such as watchdog and pathrater [25]. Determination of other nodes outside of its direct communication adds complexity and uncertainly to the process. Recommendation has been a common approach to achieve indirect trust. Due to the need for interactions among nodes, and more interactions generally lead to higher recommendation accuracy but more WSN resource consumption, there is a tradeoff between the efficient of WSNs and the accuracy of recommendations.

In order to minimize the management overhead of the network, an unweighted node evaluation scheme NEAT [18] is proposed to assist the central node (the initiating node of trust assessment) with evaluating its neighboring nodes' trust. When the central node wishes to evaluate a neighboring node's trust, it will query its assistants about this neighboring node. The assistants will then provide the queried node's trust values in their individual communities to the central node. However, limited by the characteristics of intrusion detection mechanisms, most abnormal behaviors lunched by malicious nodes can only measured by their neighbors. In order to reduce the overhead, the assistants are often limited to the neighbors of the central node, and they are unable to guarantee the credibility and validity of recommendations.

Focusing on trust dissemination process, Oliviero *et al.* propose a process that incorporates update of trust values into routing [26]. In the proposal, trust information is encapsulated in an route request packet which could exploit the reserved field. Together with the routing information, the route request packet is then broadcast to all neighbors. Once the packet is received, the neighbors look for the presence of the mentioned reputation option by checking the reserved field. If the node presented in the reputation option does not belong to the neighbors of the receiving node, it disregards the reputation information and leaves it unmodified in the forwarded route packet. Otherwise, it exploits the reputation value in order to update the computed reputation value with its local observation. This new value is then inserted in the route request packet, and broadcast to all neighbors. The main problem of this approach is its insecurity. Any intermediate node that receives the route request packet in route discovery process can tamper the trust value, which can significantly affect the credibility of trust values.

In [27], a trust-aware routing protocol (TARP) is proposed. Two steps are used to find a trusted neighbor node. The first step is called the "One Hop Check" and will only be initiated by the source node that has some data to send. The source node will send a Neighbor Request to all its neighbors asking them for their trust attributes. Once it receives the trust attributes, the source node will choose the most trusted node. In step two, the source node will make a credit check on the pre-selection node by communicating directly with its neighbors. For this purpose, the source node will use a different channel and a temporarily higher energy than the one used in step one. The source node will send a far neighbor request to nodes. In this case, more neighbor nodes of pre-selection node will receive the request and response with a far neighbor reply. However, to implement this approach, frequency-hopping and synchronization technologies are needed. These complex MAC scheduling mechanisms may limit the applications making it unattractive to WSNs.

Reputation broadcast is another common method for receiving recommendations from neighbors [28]. The source or the evaluating node broadcast the trust request that carries the identification of the evaluated node. If a receiving node is a neighbor of the evaluated node, it will reply the corresponding trust information. Otherwise, it only forwards the trust request packets. Since flooding is involved in the process, this approach may produce a high overhead and energy consumption due to the flooding process.

Game theory offers tools to model strategic interaction among rational entities [29] [30]. It is also useful for WSNs to analyze the sensor nodes' cooperation behaviors. Zheng *et al.* quantitatively analyzing the efficiency of establishing trust for improving node cooperation by studying a graphical game [7]. However, they do not consider the security requirements of the network. Kamhoua *et al.* present the interconnection between cooperation, trust and security in the network [31]. But they do not provide methods to reduce the overhead of the network which is produced by the security mechanisms. Furthermore, these schemes only utilize the computed trust value for dealing with other issues, none of them focus on the trust evaluation process itself. To our best knowledge, no specific study of trust derivation for WSNs by adopting game theoretic approach has been investigated.

III. System Model

A. Network Model

In this paper, we consider a WSN consisting of a few sink nodes and a number of sensor nodes that are randomly distributed in a designated area. Each sensor node is in charge of both detecting events and forwarding packets. All the sensor nodes are resource-constrained and have the same limited radio coverage. Consequently, end-to-end communication in a WSN is normally achieved via multi-hop relaying where a communication path is established in a distributed manner. Table I lists the main notations that are used in the following sections.

B. Security Model

With the open and remote deployment environment, WSNs are generally vulnerable to various attacks, such as blackhole attack, wormhole attack, and sybil attack [34]. In this paper, we assume that all the sensor nodes are compromisable. Compared with them, the sink node can be recognized as a highly trusted party in most cases with more sophisticated hardware.

The attacks launched by malicious nodes can be divided into two types: passive and active. In passive attacks, malicious nodes may passively gather sensitive information or behave selfishly in collaborative operations, such as routing, in order to affect the proper operation of WSNs. In active attacks, malicious nodes may actively request for sensitive information, influence the behavior of surrounding nodes [22], or directly affect the normal operation of WSNs using attacks such as Denial of Service (DoS).

C. Trust Model

Trust model essentially performs trust derivation, computation and application [36]. In this paper, we adopt watchdog [25] as the foundation of detection mechanisms. Each sensor node is responsible for monitoring the behavior of its neighbors within its radio range. The detection results are utilized for the evidence of trust computation. The trust T of an arbitrary node includes direct trust T_D and indirect trust T_I. Finally, the results of trust computation can be used as a measure of security for various aspects of communications and networking: securing routing, access control, as well as key management. The discussion of trust computation methods is out of the scope of this paper. A detailed study of the trust computation model can be found in our previous work [35].

IV. The analysis of security requirements for TDDG

WSNs are usually deployed in an environment without central infrastructures and vulnerable to attack. In this paper, we assume that arbitrary sensor node is compromisable and may not cooperate with other nodes. As mentioned above, the distributed detection technologies and trust evaluation methods are proposed to ensure the security of the network in this case. The main goal of this paper is to reduce energy

TABLE I
NOTATIONS FOR TDDG.

Symbol	Meaning
R_j	Quantifies the reputation of node j
$f_g(e_j)$	Energy saving for node j
γ	A parameter specifying the ratio of reputation loss to energy saving
R_{th}	Reputation tolerable threshold
V	The set collecting all nodes in network
l	Round number
$\Delta T_D(i,j)$	The overall direct trust value of node j for node i
$\Delta T_I(M,j)$	The overall indirect trust value of node j for node i
$P_j(a)$	Positive or well behaved activities
$N_j(a)$	Negative or misbehaved activities
ΔT_j	Changes of trust value
ΔE_j	The amount of energy saving
k	The optimal number of recommendations
N	The number of participating nodes
G	The Utility
p	The probability of sending trust reply
$f_s(e)$	The cost to an arbitrary node to send trust reply

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2014.2314132, IEEE Internet of Things Journal

consumption and latency for trust evaluation while maintaining adequate security. Before introducing TDDG, we first analyze the security policies and measure the demand for network security.

Fig. 1 illustrates the trust derivation for an arbitrary node. In the diagram, node i is the evaluating node and node j is the evaluated node. In order to secure the network, we employ a risk strategy model to stimulate the nodes for proper security behaviors. We begin by defining the following network risk condition:

$$R_j - \gamma f_g(e_j) \geq R_{th}, \quad j \in V, \tag{1}$$

where R_j quantifies the reputation of node j after some evaluation. The function $f_g(e_j)$ is the energy saving for node j if it does not comply with a collection of proper behaviors, e_j. One example that a node may gain energy with misbehavior is a selfish behavior where the node does not forward data packets as it should according to the protocol specification. Such improper behavior poses risk to the proper operation of the network, and it should be prevented. The coefficient γ is a parameter specifying the ratio of reputation loss to energy saving. Thus the left hand side of (1) determines the overall reputation of node j after its potential misbehavior. We set a tolerable threshold R_{th} such that if the overall reputation remains above R_{th}, the proper network function involving node j can be maintained. Quantities R_j and R_{th} are normalized to give values between 0 and 1. Let V be the set collecting all nodes in the network, then (1) represents the minimum condition for the entire network to function properly.

From the node's prospective, if it attempts any improper behavior, it will be penalized by lowered reputation rating. At the point when its reputation rating is not sufficiently high, any attempt of improper behavior to conserve energy will violate the condition set in (1) with consequences of being evicted from the network. Thus the condition also stimulates the proper behavior of nodes.

In our model, risk and reputation are evaluated periodically. The instantaneous reputation of node j, which is also the overall trust value at round l, is defined as the difference between the positive and negative trust assessments combined from direct and indirect observations. It can be expressed as:

$$R_j = \Delta T_j^{(l)} = f_t\left(\Delta T_D(i,j)^{(l)}, \Delta T_I(M_j,j)^{(l)}\right), \tag{2}$$

where $\Delta T_D(i,j)^{(l)}$ and $\Delta T_I(M,j)^{(l)}$ represent the overall direct trust value and indirect trust value of node j for node i at l-th around respectively. The quantity M_j is the set of nodes providing recommendations of node j for node i. The function $f_t(\cdot)$ defines how direct and indirect trust values are consolidated.

We shall first focus on direct trust determination framework. Let A be a set containing all defined network activities. To determine the behavior of node j, its neighbor node i observes the activities of node j and records the likelihood of presence of any observed activity. Positive or well behaved activities are recorded in $P_j(a)$ while negative or misbehaved activities are recorded in $N_j(a)$, where $a \in A$, with a value of 1 (or 0) indicating a strong evidence of the presence (or absence) of an activity a. Moreover, the importance of each predefined activity is also predetermined and specified as weight functions in $P_W(a)$ and $N_W(a)$, where

$$\sum_{a\in A} P_W(a) = \sum_{a\in A} N_W(a) = 1. \tag{3}$$

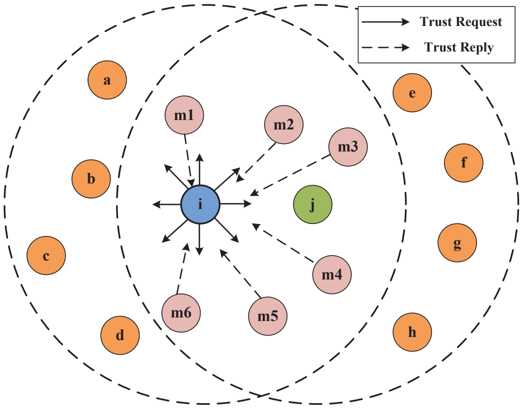


Fig. 1. The process of trust derivation

Based on the trust values in the previous round (i.e. $T_D(i,j)^{(l-1)}$ and the recent assessed behaviors of node j (i.e. $P_j(a)^{(l)}$ and $N_j(a)^{(l)}$), the overall direct trust value can be derived. The computation can be formulated in the following general form:

$$\begin{aligned}\Delta T_D(i,j)^{(l)} = &\sum_{a\in A} f_d(T_D(i,j)^{(l-1)}, P_j(a)^{(l)})P_W(a)\\ &-\sum_{a\in A} f_d(T_D(i,j)^{(l-1)}, N_j(a)^{(l)})N_W(a),\end{aligned} \tag{4}$$

where $f_d(\cdot)$ is the function that defines the combination of the previous trust value and the current assessment of a behavior. The difference between weighed average positive and negative trust assessments gives the overall trust value on node j.

We apply the similar process for indirect trust computation. Indirect trust computation requires neighbors of node j, which are x where $x \in M_j$ to obtain the indirect trust values. Likewise, the overall indirect trust computation can be formulated as follow:

$$\begin{aligned}&\Delta T_I(M_j,j)^{(l)}\\ &\quad = \textstyle\sum_{a\in A}\left[f_r\left(T_I(m_1,j)^{(l-1)}, T_I(m_2,j)^{(l-1)}, ...,\right.\right.\\ &\qquad \left.\left. T_I(m_n,j)^{(l-1)}, P_j(a)^{(l)}\right) P_W(a)\right]\\ &\quad - \textstyle\sum_{a\in A}\left[f_r\left(T_I(m_1,j)^{(l-1)}, T_I(m_2,j)^{(l-1)}, ...,\right.\right.\\ &\qquad \left.\left. T_I(m_n,j)^{(l-1)}, N_j(a)^{(l)}\right) N_W(a)\right],\end{aligned} \tag{5}$$

where $m_1, m_2, ..., m_n \in M_j$, and the function $f_r(\cdot)$ defines the combination of the previous indirect trust value and the current assessment of a behavior.

We note that $f_t(\cdot)$, $f_d(\cdot)$ and $f_r(\cdot)$ are three arbitrary functions that define how the trust values are computed in the process. We refer readers to [35] for a possible design of these functions.

Without loss of generality, we set energy cost to be directly proportional to the overall trust value, ΔT_j. In other words, the energy saving of an improper behavior is linear to the reduction in the trust value. To capture the fact that each individual negative behavior may result in different energy saving, proper mapping between energy costs and activities can be given in the weight functions $P_W(a)$ and $N_W(a)$, if desirable. With the above relationship between trust reduction and energy saving, we have

$$\frac{\Delta T_j}{T_{max}} = \frac{\Delta E_j}{E_{max}}, \tag{6}$$

where $T_{max} = 1$ by definition, E_{max} is the total energy consumption of an arbitrary node during the predefined cycle, and ΔE_j is the amount of energy saving. With the above, the quantity of $f_g(e_j)$ can be simply represented by ΔE_j. Notating $f_g(e_j)$ using ΔE_j, with the last result in the above, we rewrite (1) as:

$$f_t\left(\Delta T_D(i,j), \Delta T_I(M_j,j)\right) \geq R_{th} + \gamma \Delta T_j E_{max}. \tag{7}$$

As the selection of R_{th} is based on the network security requirements, which varies for different practical applications, the characteristic parameters of formula (7) mainly depends on the left part of the inequality $f_t(\cdot)$. The specifications of $f_t(\cdot)$ is shown in our previous work [35], and its performance is closely associated with the number of recommendations. Since the indirect trust value is computed by the combination of all received recommendations in the trust computation model, acquiring adequate number of recommendations is important to make reliable judgement on trustworthiness of a node. Ideally, we hope to collect all recommendations. However, this involves in communication overheads which consume relatively high energy. It is thus practical to determine the appropriate number recommendations needed to ensure the security of the networks. We find the optimal number of recommendations, k, from indirect trust such that the network risk condition specified in (1) can be satisfied, that is

$$k \quad = \min\left\{ \parallel \Omega(\Delta T_I(M_j,j)) \parallel \right\}, \tag{8}$$

where $\Omega(\cdot)$ gives a collection of sets, each of which contains node j's neighbors such that the condition (1) can be satisfied. In other words, $\Omega(\cdot)$ carries all possible combinations of neighbor selections for recommendations that satisfy the condition (1). The function $\min\{\cdot\}$ returns the smallest number from the input set. In the following, we shall present our proposed trust derivation scheme namely TDDG that utilizes this optimal energy consumption of the network.

V. Trust Derivation Dilemma Game (TDDG)

A. Trust derivation procedure

In this section, we describe the trust derivation procedure of our proposed TDDG. As reviewed in Section II, a robust trust derivation procedure relies on adequate collection of trust information from the network for computation. To ensure adequate collection of trust information for all users, flooding is often used to broadcast such information to all other nodes in the network. However, flooding in an uncontrolled manner consumes a large amount of energy and incurs lengthy latency. This drawback can be overcome by introducing a certain control mechanism in flooding. The common method is the use of hop limitation. We shall include this method in our proposed TDDG. Using the diagram given in Fig. 1, the following describes a hop limited trust derivation procedure.

Step 1. A source node i initializes the trust derivation process and broadcasts a trust request packet whose target is node j. To reduce the overhead of the flooding mechanism, we set a hop limit value. This value should be decremented by one every time the trust request packet is rebroadcast if it is not zero.

Step 2. Any node that receives the trust request packet first checks if it has already received the same request. If it has, the packet is immediately discarded. Otherwise, the packet is rebroadcast if the hop limit is larger than zero.

Step 3. The node receiving the trust request packet should now check whether the evaluated node j is its neighbor. If node j is its neighbor, the node may unicast a trust reply to the source node i through the reverse route. The decision of whether to reply depends on a dilemma game which will be introduced in the next section.

Step 4. After obtaining the recommendations, the source node i compute the trust value by combining the direct trust with the indirect trust. Finally, the evaluating node i can determine whether the evaluated node j should be trusted according to the computed results. The algorithm of trust computation is outside the scope of this paper. We assume that an adequate trust evaluation algorithm is implemented.

In this paper, we only choose the recommendations provided by the neighbor nodes of the evaluated node. Because most malicious behaviors can be detected by the neighbors and this mechanism can obviously reduce the overhead of the network. As shown in Fig. 1, only node m_1 to node m_6 will reply the trust request. The neighbor list can be updated by the existing neighbor discovery process such as the interactions of periodical hello packets.

While the implementation of hop limit in flooding may reduce the communication involvement trust information collection, the effect may be limited, especially in a dense network often considered in IoT. To deal with a dense network, it is thus necessary to also constrain the trust replies from the local neighbors. As this constraint directly affect the quality of trust information collection, a careful design is needed to ensure the trust information replied from a set of selected neighbors can maintain the desirable security requirement. In the following, we introduce a game theoretic approach to deal with this issue.

B. Dilemma game in trust derivation

As described in the previous section, a selective trust reply from neighbors helps achieve a secure and yet energy-efficient trust derivation mechanism. Setting the appropriate number of nodes for trust replies is important as a smaller number challenges the security while a higher number introduces unnecessary overheads. In Section IV, we have established the optimal number of recommendations k by considering the requirements of security. This setting may be immediately used in an ideal environment where all nodes behave cooperatively. However, this assumption may not be always practical. Here, we introduce a game theoretic approach to deal with the potential selfishness in the process.

Algorithm 1 Trust derivation with TDDG.

```
Process Initialization
if Node $i$ Ready then
    Broadcast Trust Request ($HopLimit = h_{th}$)
end if
if Trust Request Received then
    if Receive Duplicate Request then
        Discard Trust Request
        return
    else
        if $HopLimit > 0$ then
            $HopLimit$=$HopLimit - 1$
            Rebroadcast Trust Request
        end if
        if Node $j \in NeighborSet$ then
            Send Trust Reply With Probability $p$
            Discard Trust Request
            return
        else
            Discard Trust Request
            return
        end if
    end if
end if
END Process
```

Since the pioneering work [37] of Axelrod on the evolutionary prisoner's dilemma games, this approach has become a fruitful tool in the area of political and behavior sciences, biology and economics [39] [40]. In the prisoner's dilemma game, each of two players has to decide simultaneously whether it wishes to cooperate with the other or to defect [38]. The final purpose of this game is to find the optimal strategy profile that leads to the highest total (average) payoff.

Here we consider a trust derivation dilemma game (TDDG) with N nodes, where N is the number of the specified evaluated node's neighbors except the evaluating node. Each participating node has two strategies, Reply or Not Reply. Reply denotes that the nodes reply to the evaluating node when receiving trust request. Not Reply means that the nodes disregard the trust request when receiving it. The network is secure if and only if the number of recommendations is greater than k. We notice that there may be a special condition that nodes receiving trust request simply disregard it considering their remaining energy. This issue can be dealt with a more effective neighbor discovery and maintenance mechanism. In other words, we can enforce announcement of remaining battery power during some message exchange such that neighboring nodes can update this information. Consequently, the N participating nodes in TDDG do not include those with low remaining energy.

When $N \leq k$, the network may not be secure even all the neighbors of the evaluated node reply the trust request. In this case, we enforce that all the neighbors must reply to the evaluating node in order to reduce the security risk of the network. When $N > k$, every participating node makes a decision whether to reply the trust request. The decision making process is elaborated in the following.

TABLE II
PAYOFF MATRIX FOR TRUST DERIVATION DILEMMA GAME ($k = 1$).

TDDG ($k = 1$)		Other Nodes ($N-1$)	
		No Other Reply	At Least One Reply ($1 \leq \alpha \leq N-1$)
Node i	No Reply	$0, 0$	$G, G - \alpha f_s(e)$
	Reply	$G - f_s(e), G$	$G - f_s(e), G - \alpha f_s(e)$

Considering the security attributes of the network, we define a utility G under the condition that the number of participating nodes that reply to the evaluating node is greater than k. To simplify the analysis, we assume that the cost to an arbitrary node to send trust reply is $f_s(e)$. We also make a reasonable assumption that the gain from security exceeds the optimal cost to send trust reply. Therefore we have $G > kf_s(e) > 0$.

There are two cases in the TDDG. In the first case, $k = 1$, where the requirements of security can be satisfied if any node sent trust reply. The strategic form can be depicted in Table II. The row player (node i) can be an arbitrary participating node that receives the trust request, while the column player stands for the other $N-1$ neighbor nodes. A node prefers to keep silence to save energy if it thinks that at least another node will send trust reply. As an arbitrary node chooses its own strategy, all the sensor nodes are independent in this game. We assume that an arbitrary node i sends trust reply with probability p, or remains silence with probability $1-p$. Then for N nodes, at least one node reply the trust request with a probability of $1-(1-p)^N$. As a result, the mixed strategy Nash equilibrium can be computed by

$$G\big(1-(1-p)^{N-1}\big) = G - f_s(e). \tag{9}$$

Consequently, the probability of sending trust reply can be represented as

$$p = 1 - \Big(\frac{f_s(e)}{G}\Big)^{\frac{1}{N-1}}. \tag{10}$$

Setting $q = 1-p$, the following expressions can be obtained by taking the logarithm of both sides of (10), or

$$\ln\big(G/f_s(e)\big) = (1-N)\ln q. \tag{11}$$

For the second case where $k > 1$, the strategic form of TDDG can be depicted in Table III. In the game, a node will prefer to reply the trust request if and only if it believes that $k-1$ other nodes will send trust reply. Otherwise, it prefers to keep silence to conserve energy. The probability of k nodes choosing "reply" strategy can be denoted as $C_N^k p^k (1-p)^{N-k}$. Consequently, the mixed strategy Nash equilibrium can be

TABLE III
PAYOFF MATRIX FOR TRUST DERIVATION DILEMMA GAME ($k > 1$).

TDDG ($k > 1$)		Other Nodes ($N-1$)		
		α Nodes Reply ($0 \leq \alpha < k-1$)	$k-1$ Nodes Reply	β Nodes Reply ($k-1 < \beta \leq N-1$)
Node i	No Reply	$0, -\alpha f_s(e)$	$0, -(k-1)f_s(e)$	$G, G-\beta f_s(e)$
	Reply	$-f_s(e), -\alpha f_s(e)$	$G-f_s(e), G-(k-1)f_s(e)$	$G-f_s(e), G-\beta f_s(e)$

computed by

$$\begin{aligned} & G\sum_{\beta=k}^{N-1} C_{N-1}^{\beta}p^{\beta}(1-p)^{N-\beta-1} \\ & = -f_s(e)\sum_{\alpha=0}^{k-2} C_{N-1}^{\alpha}p^{\alpha}(1-p)^{N-\alpha-1} \\ & + (G-f_s(e))\Big\{C_{N-1}^{k-1}p^{k-1}(1-p)^{N-k} \\ & + \sum_{\beta=k}^{N-1} C_{N-1}^{\beta}p^{\beta}(1-p)^{N-\beta-1}\Big\}. \end{aligned} \tag{12}$$

From the equation above, we can obtain the following expressions:

$$C_{N-1}^{k-1}p^{k-1}(1-p)^{N-k} = \frac{f_s(e)}{G}. \tag{13}$$

If we denote $U(p) = C_{N-1}^{k-1}p^{k-1}(1-p)^{N-k}$, the derivative of $U(p)$ can be written as

$$\frac{\partial U(p)}{\partial p} = C_{N-1}^{k-1}p^{k-2}(1-p)^{N-k-1}(k-1+p-np). \tag{14}$$

By setting the derivative to zero, we observe that $U(p)$ is an increasing (resp. decreasing) function when p is smaller than (resp. greater than) $\frac{k-1}{N-1}$. On the other hand, the right side of (13) is a decreasing function with the variable G. As we know, greater values of G give the participating nodes incentives to send trust reply compared with the cost. Consequently, we have $\frac{k-1}{N-1} \leq p < 1$, and $G \geq f_s(e)/C_{N-1}^{k-1}(\frac{k-1}{N-1})^{k-1}(\frac{N-k}{N-1})^{N-k}$.

As a result, all the participating nodes will send trust reply with probability p, which should also consider the tradeoff between energy efficiency and security (Algorithm 1 shows the pseudocode of the improved trust derivation process). From (10) and (13), we can find that the probability p depends on the selection of $G/f_s(e)$. The optimal selection of $G/f_s(e)$ and its effect on network performance will be studied shortly in Section VI.

C. The analysis of attacks on trust derivation

The preceding discussion does not consider the effect of misbehaved nodes on our trust derivation scheme. Although trust management systems can deal with most of the conventional attacks in WSNs and help improve the security of the network, there still exists some potential risks [42]. For example, due to the cost and resources constraints, the intrusion detection system that is the foundation of trust-based schemes cannot guarantee 100% accuracy of detecting. Consequently, it is possible that some malicious or misbehaved nodes are incorrectly included in the trusted set of nodes that provide recommendations at some point. In this case, the misbehaved nodes may launch passive or active attacks on trust derivation and impair the performance of TDDG. This paper mainly focuses on the methods which can reduce or even eliminate the effects of the misbehaved nodes. Some of the most common attacks to a trust management system for WSNs [23] and their solutions are listed as follows:

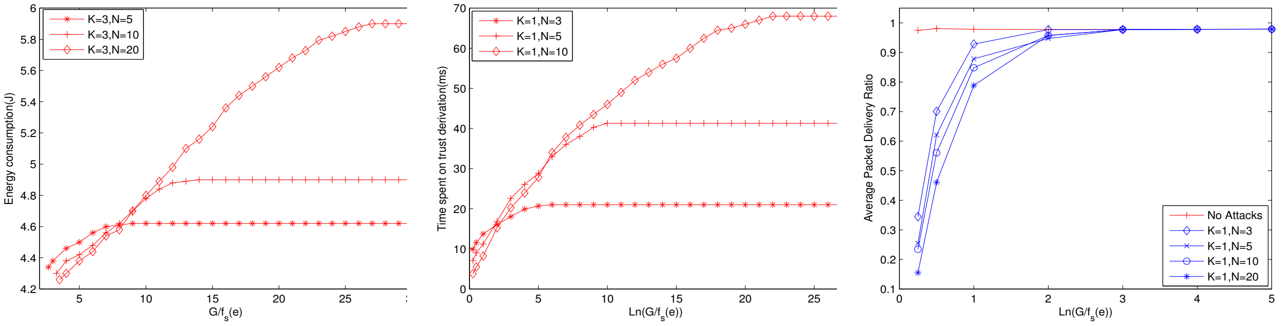
- Bad mouthing attack: The misbehaved nodes provide false recommendations and propagate negative reputation information about well behaved nodes, which might affect the accuracy of the trust evaluation. To solve this problem, an inconsistency check scheme [43] can be used in trust derivation process to detect misbehaved nodes and filter out false recommendations.
- DoS attack: A DoS attacker can disrupt legitimate communication of other nodes by flooding the network with redundant recommendations. This kind of attacks can be solved by limiting the data generation rate of the source node or adopting the DoS-resistant network architecture such as NetFence [44].
- Selfish attack: A selfish node may not follow the policies in TDDG. When receiving the trust request, it will simply drop the request and not send trust reply by preserving its resources. In this case, we should increase the value of $G/f_s(e)$ to ensure the security of the network. The effect of misbehaved nodes on our trust derivation scheme is also presented in Section VI.

VI. SIMULATION RESULTS AND PERFORMANCE EVALUATION

We evaluate our proposed game theoretic approach for trust derivation using the NS-2 simulator [32]. To validate the security of the network, we assume that arbitrary routing node will behave selfishly (that is, not forwarding data packets) if and only if the number of recommendations is less than k when it is evaluated by other nodes. Furthermore, we adopt a trust computation mechanism to compute the trust of nodes, which is proposed in [35]. All the simulations have run more than 50 times and the simulation parameters used in our experiments are summarized in Table IV.

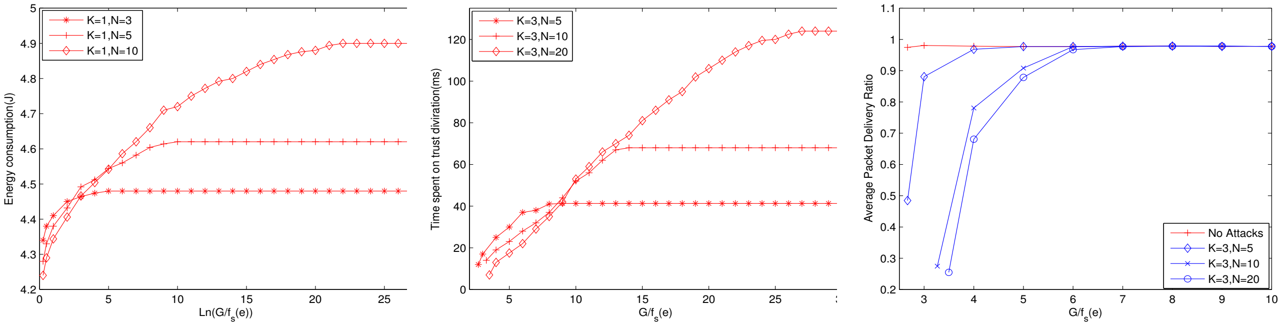
The simulations can be divided into three parts. First, we take account of the optimal selection of $G/f_s(e)$ and analyze its effect on network performance. Then, we further discuss the security of our scheme when the misbehaved nodes are present in the trusted set of nodes in TDDG. Finally, we compare the performance of our TDDG with other mechanisms in trust derivation schemes.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2014.2314132, IEEE Internet of Things Journal



(a) The energy consumption (b) The time spent on trust derivation (c) The packet delivery ratio

Fig. 2. The effect of $\ln(G/f_s(e))$ on network performance (k=1).



(a) The energy consumption (b) The time spent on trust derivation (c) The packet delivery ratio

Fig. 3. The effect of $G/f_s(e)$ on network performance (k=3).

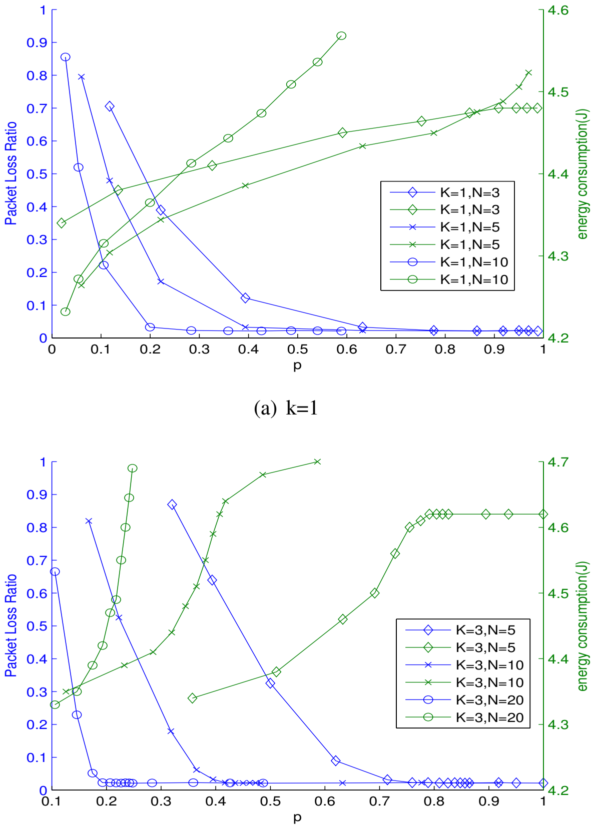
TABLE IV
SIMULATION PARAMETERS.

Parameters	Values
Monitoring Area	$500m \times 500m$
Number of nodes	100
Communication Range	100m
Packet Interval	5s
Simulation Time	500s
Length of Data Packet	100 bytes
Transmit Energy	0.01w
Receive/Listen Energy	0.01w
Idle Energy	0.003w
Routing Protocol	AODVjr [41]
Mac Layer Protocol	IEEE 802.15.4
E_{max}	1000J
R_{th}	0.01
γ	5000
ΔE	0.01J
$P(a)$	0.01
$N(a)$	-0.10

A. The selection of $G/f_s(e)$

The ratio of G to $f_s(e)$ is critical in our trust derivation process. We list common values of $G/f_s(e)$ to analyze their effect on the performance of the network. We first consider the case when $k = 1$. As shown in Fig. 2(a), regardless of the number of participating nodes, energy consumption increases as the value $\ln(G/f_s(e))$ increases. This is because the high ratio of G to $f_s(e)$ gives the participating nodes incentives to reply the trust request. As the value $\ln(G/f_s(e))$ increases, the energy consumption increases until when $\ln(G/f_s(e))$ exceeds the threshold. At that point, all participating nodes send their trust replies and the energy consumption saturates. In Fig. 2(b), we observe similar behavior for the duration of trust derivation process. This is because when more nodes decide to send trust reply over the wireless common channel, more time is involved in the process. Excessive replies may also lead to transmission congestion.

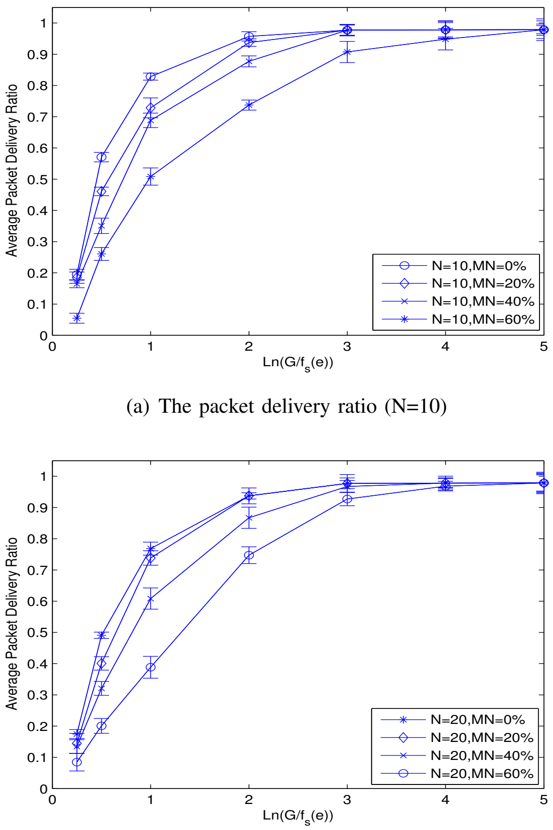
From the above results, we conclude that the ratio $\ln(G/f_s(e))$ should be kept small for lower energy consumption and shorter latency. However, if the ratio is not set adequately large, in an event of selfish users who refuse to send trust replies, fewer than intended replies will be returned which may reduce the quality of the recommendation. Consequently, there is a need to analyze the effect of $\ln(G/f_s(e))$ on the security of the network. Our focus here is to ensure collection of an adequate number of trust replies so that trust computation is accurate. In Fig. 2(c), we present the packet delivery ratio



(a) k=1

(b) k=3

Fig. 4. Packet loss ratio and energy consumption versus the probability of sending trust reply.



(a) The packet delivery ratio (N=10)

(b) The packet delivery ratio (N=20)

Fig. 5. The effect of misbehaved nodes (k=1).

which indicates the success reception of the intended trust replies. As can be seen, when $\ln(G/f_s(e)) \geq 2$, the average packet delivery ratio reaches over 95% even with presence of selfish attacks. Consequently, when $k = 1$, we consider $\ln(G/f_s(e)) = 2$ as an appropriate value in this paper.

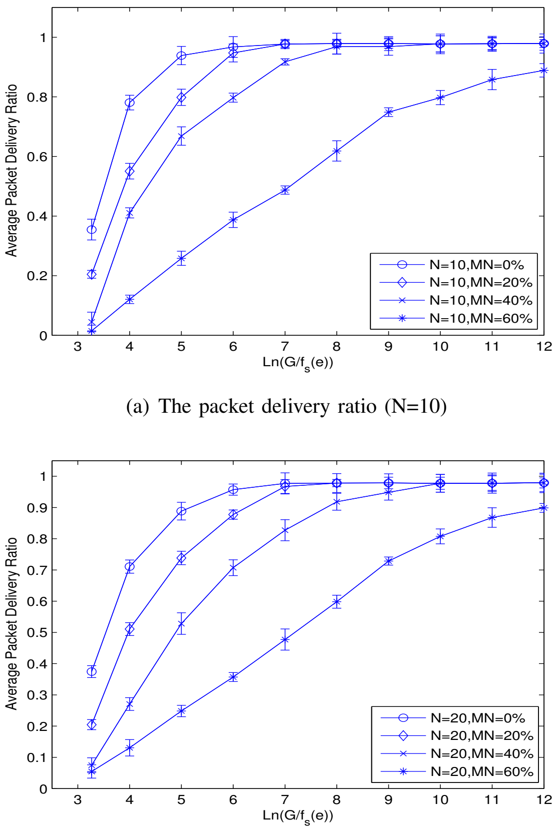
We notice similar behaviors for the case when $k > 1$, and we use a typical example $k = 3$ for illustration. As can be seen in Figs. 3(b), 3(b) and 3(c), the ratio of $G/f_s(e)$ should be kept small, but adequately large enough to achieve a high packet delivery ratio so that the quality of trust computation is maintain. For this example, we shall recommend $G/f_s(e) = 6$ as a recommended setting for optimal operation. Recommended settings for other k values can be determined in the similar manner.

In Fig. 4, we show the effect of p on packet loss ratio and energy consumption for optimal operation. We see that as p increases, packet loss ratio decreases and energy consumption increases. The tradeoff between energy efficiency and security is clearly shown. When low energy consumption is achieved, high packet loss ratio is resulted which reduces the quality of outcome produced by the trust computation, and vice versa. At the optimal operation point, taking $k = 1, N = 3$ as an example, p is approximately 0.6 based on (10). From the figure, we see that at around $p = 0.6$, packet loss rate is kept under the desirable value and energy consumption is not excessive. Similar observation can be concluded for other settings.

B. The effect of misbehaved nodes

As an error probability of detection may exist in the intrusion detection system, it is possible that some misbehaved nodes are wrongly included in the trusted set of nodes that provide recommendations at some point. In the simulation experiments, we include some misbehaved nodes (MN) that launch various attacks such as bad mouthing attack, selfish attack, etc.

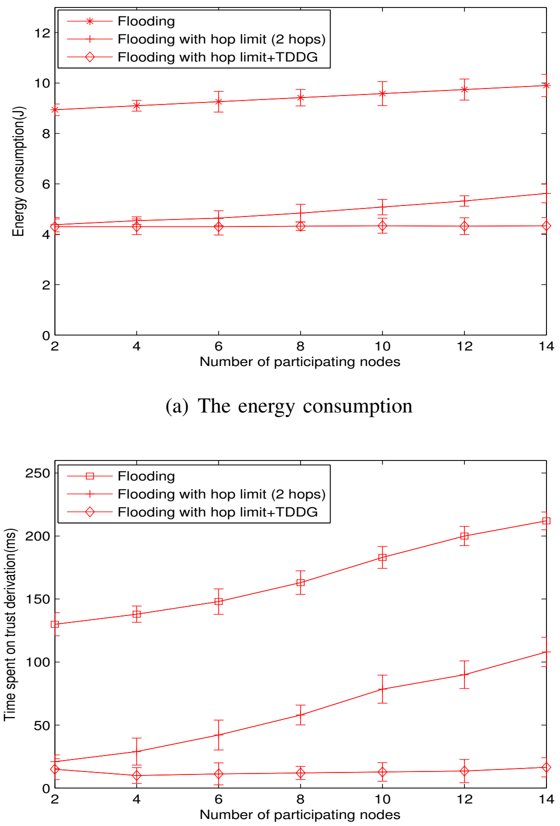
Although the attacks launched by misbehaved nodes can be solved by corresponding methods described in Section V, the optimal setting of $G/f_s(e)$ for satisfying the security of the network is obviously different. As shown in Fig. 5 ($k = 1$), when there is no misbehaved node in the set of participating nodes, $\ln(G/f_s(e)) \geq 2$ can satisfy the security of the network (the average packet delivery ratio reaches over 95%). However, this threshold increases as the proportion of misbehaved nodes rises (when $MN = 20\%$, $\ln(G/f_s(e)) \geq 2$; when $MN = 40\%$, $\ln(G/f_s(e)) \geq 3$; when $MN = 60\%$, $\ln(G/f_s(e)) \geq 4$). To obtain the requisite number of recommendations, a higher value of $G/f_s(e)$ is required in this case. Because the actual number of participating nodes is less than the theoretical value as the misbehaved nodes do not follow the policies in TDDG.



(a) The packet delivery ratio (N=10)

(b) The packet delivery ratio (N=20)

Fig. 6. The effect of misbehaved nodes (k=3).



(a) The energy consumption

(b) The time spent on trust derivation

Fig. 7. The performance of the network (k=1).

Similarly, when $k = 3$, the selection of the ratio $G/f_s(e)$ should also be readjusted as considering the effect of misbehaved nodes (when $MN = 20\%$, $G/f_s(e) \geq 7$; when $MN = 40\%$, $G/f_s(e) \geq 10$; when $MN = 60\%$, $G/f_s(e) > 12$), which is illustrated in Fig. 6. Consequently, compared with the case without misbehaved nodes, we should select a relatively high value of $G/f_s(e)$ to ensure the network security in practical application environments.

C. Performance evaluation

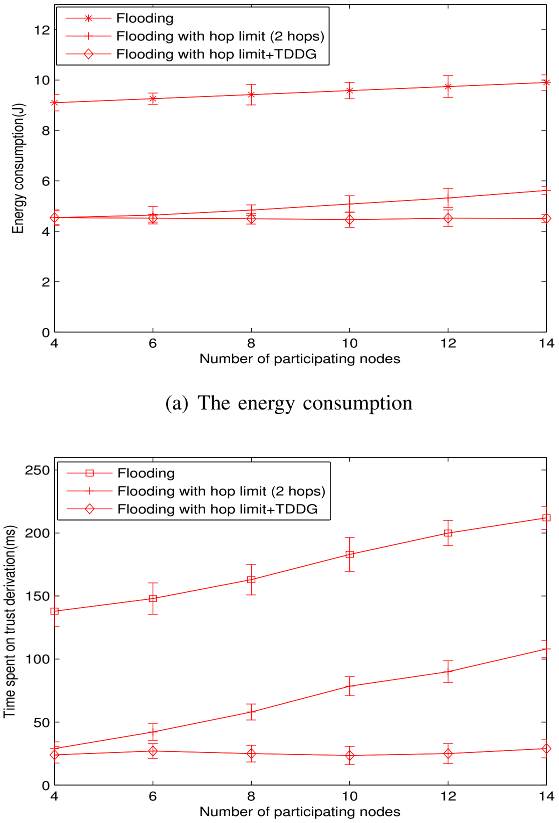
Compared with the conventional trust derivation scheme such as flooding mechanism, our game theoretic approach provides facility to balance performance and quality of recommendation. We previously discussed the selection of the ratio $G/f_s(e)$, we shall now focus on the performance using the recommended ratio setting.

Energy consumption is an important factor we should consider when designing schemes for WSNs. It is more so in IoT as applications in IoT often demand high network density. In the simulation, we shall focus on the energy consumption of the trust derivation process. In Figs. 7(a) and 8(a), we compare the energy consumption of several methods including flooding. We can see that the energy consumption of flooding is much higher than the other two schemes due to its large number of broadcast and rebroadcast packets. Imposing hop limit in flooding or using our TDDG approach significantly reduces the energy consumption of the network. Comparing the two improved schemes, when the number of participating nodes is small, these two schemes produce similar energy consumption. However, the energy consumption produced by the former will grow with the increasing number of participating nodes. In contrast, the energy consumption produced by TDDG approach remains stable throughout. With say 14 participating nodes for $k = 1$, our TDDG approach saves 23.6% of energy consumption than flooding with 2-hop limit. More saving can be expected for denser networks.

Figs. 7(b) and 8(b) represent the different time spent to complete the trust derivation process between TDDG and other mechanisms. It is clear that latency performance exhibits similar behaviors as those in energy consumption, with more obvious advantages over other schemes. For example, compared with the flooding with 2-hop limit, our game theoretic approach can save 73.2% of time when the number of participating nodes is 14 for $k = 3$.

VII. Conclusions and Future Works

In this paper, we first proposed a risk strategy model to determine the optimal number of recommendations k that can satisfy the security requirements of a network. Based on the optimal number of recommendations, we introduced the trust derivation dilemma game into the trust derivation process. The



(a) The energy consumption

(b) The time spent on trust derivation

Fig. 8. The performance of the network (k=3).

probability of the selected strategy was calculated based on the mixed strategy Nash equilibrium of the game. Compared with the traditional trust derivation methods, the simulation results showed that our game theoretic approach can improve the performance of the network under the premise of security assurance, especially in a dense networks.

In the future, we plan to design trust derivation schemes by reducing the overhead produced by trust request, which can further improve the performance of the network.

ACKNOWLEDGEMENTS

This work was supported in part by National Natural Science Foundation of China (NSFC) (Grants No. 61272504 and 61201204), Beijing Nature Science Foundation (Grant No. 4122057), Research Fund for the Doctoral Program of Higher Education of China under grant No. 20130009110010, National S&T Major Program (Grant No. 2012ZX03005003), Fundamental Research Funds for the Central Universities (Grants No. 2012YJS016, 2014JBM006 and 2012JBM011), and Taiwan National Science Council (Grant No. NSC102-2221-E-006-008-MY3).

REFERENCES

[1] R. Roman, P. Najera, and J. Lopez, Securing the internet of things, Computer, vol. 44, no. 9, pp. 51-58, 2011.

[2] P. Kasirajan, C. Larsen, and S. Jagannathan, A new data aggregation scheme via adaptive compression for wireless sensor networks, ACM Transactions on Sensor Networks (TOSN), vol. 9, no. 1, pp. 1-5, 2012.

[3] X. Li, J. Yang, A. Nayak, and I. Stojmenovic, Localized geographic routing to a mobile sink with guaranteed delivery in sensor networks, IEEE Journal on Selected Areas in Communications, vol. 30, no. 9, pp. 1719-1729, 2012.

[4] V. Kapnadak, M. Senel, and E. Coyle, Distributed iterative quantization for interference characterization in wireless networks, Digital Signal Processing, vol. 22, no. 1, pp. 96-105, 2012.

[5] T. Newman, S. Hasan, and D. DePoy, Designing and deploying a building-wide cognitive radio network testbed, IEEE Communications Magazine, vol. 48, no. 9, pp. 106-112, 2010.

[6] R. Zhang, J. Shi, Y. Zhang, and J. Sun, Secure cooperative data storage and query processing in unattended tiered sensor networks, IEEE Journal on Selected Areas in Communications, vol. 30, no. 2, pp. 433-441, 2012.

[7] S. Zheng, T. Jiang, and J. Baras, Exploiting trust relations for Nash equilibrium efficiency in ad hoc networks, in Proceedings of the 2011 IEEE international conference on communications (ICC). IEEE, 2011, pp. 1-5.

[8] H. Dai and H. Xu, Key predistribution approach in wireless sensor networks using lu matrix, IEEE Sensors Journal, vol. 10, no. 8, pp. 1399-1409, 2010.

[9] L. Abusalah, A. Khokhar, and M. Guizani, A survey of secure mobile ad hoc routing protocols, IEEE Communications Surveys & Tutorials, vol. 10, no. 4, pp. 78-93, 2008.

[10] S. Zhong and F. Wu, A collusion-resistant routing scheme for noncooperative wireless ad hoc networks, IEEE/ACM Transactions on Networking, vol. 18, no. 2, pp. 582-595, 2010.

[11] J. Cordasco and S. Wetzel, Cryptographic versus trust-based methods for MANET routing security, Electronic Notes in Theoretical Computer Science, vol. 197, no. 2, pp. 131-140, 2008.

[12] S. Yu, K. Ren, and W. Lou, Fdac: Toward fine-grained distributed data access control in wireless sensor networks, in Proceedings of the 2009 IEEE INFOCOM. IEEE, 2009, pp. 963-971.

[13] M. Das, Two-factor user authentication in wireless sensor networks, IEEE Transactions on Wireless Communications, vol. 8, no. 3, pp. 1086-1090, 2009.

[14] P. Ning, A. Liu, and W. Du, Mitigating DoS attacks against broadcast authentication in wireless sensor networks, ACM Transactions on Sensor Networks (TOSN), vol. 4, no. 1, p. 1-35, 2008.

[15] G. Theodorakopoulos and J. Baras, On trust models and trust evaluation metrics for ad hoc networks, IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 318-328, 2006.

[16] C. Zhang, X. Zhu, Y. Song, and Y. Fang, A formal study of trust-based routing in wireless ad hoc networks, in Proceedings of the 2010 IEEE INFOCOM. IEEE, 2010, pp. 1-9.

[17] H. Xia, Z. Jia, X. Li, L. Ju, and E. Sha, Trust prediction and trust-based source routing in mobile ad hoc networks, Ad Hoc Networks, 2012.

[18] Y. Ren and A. Boukerche, Performance analysis of trust-based node evaluation schemes in wireless and mobile ad hoc networks, in Proceedings of the 2009 IEEE international conference on Communications (ICC). IEEE, 2009, pp. 5535-5539.

[19] M. Mahmoud and X. Shen, Trust-based and energy-aware incentive routing protocol for multi-hop wireless networks, in Proceedings of the 2011 IEEE International Conference on Communications (ICC). IEEE, 2011, pp. 1-5.

[20] Y. Ren and A. Boukerche, Modeling and managing the trust for wireless and mobile ad hoc networks, in Proceedings of the 2011 IEEE International Conference on Communications (ICC). IEEE, 2008, pp. 2129-2133.

[21] R. Feng, X. Xu, X. Zhou, and J. Wan, A trust evaluation algorithm for wireless sensor networks Based on Node Behaviors and D-S Evidence Theory, SENSORS, vol. 11, no. 2, pp. 1345-1360, 2011.

[22] M. Denko, T. Sun, I. Woungang, J. Rodrigues, and H.-C. Chao, A trust management scheme for enhancing security in pervasive wireless networks, in Proceedings of the 2009 IEEE Global Telecommunications Conference (GLOBECOM). IEEE, 30 2009-dec. 4 2009, pp. 1-6.

[23] J. Lopez, R. Roman, I. Agudo, and C. Fernandez-Gago, Trust management systems for wireless sensor networks: Best practices, Computer Communications, vol. 33, no. 9, pp. 1086-1093, 2010.

[24] G. Pottie and W. Kaiser, Wireless integrated network sensors, Communications of the ACM, vol. 43, no. 5, pp. 51-58, 2000.

[25] S. Marti, T. Giuli, K. Lai, M. Baker et al., Mitigating routing misbehavior in mobile ad hoc networks, in Proceedings of the 6th Annual International Conference on Mobile Computing and Networking. ACM, 2000, pp. 255-265.

[26] F. Oliviero and S. Romano, A reputation-based metric for secure routing in wireless mesh networks, in Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM). IEEE, 2008, pp. 1-5.

[27] L. Abusalah, A. Khokhar, and M. Guizani, Trust aware routing in mobile ad hoc networks, in Proceedings of the 2006 IEEE Global Telecommunications Conference (GLOBECOM). IEEE, 2006, pp. 1-5.

[28] S. Zakhary and M. Radenkovic, Reputation-based security protocol for manets in highly mobile disconnection-prone environments, in Proceedings of the 2010 Seventh International Conference on Wireless On-demand Network Systems and Services. IEEE, 2010, pp. 161-167.

[29] K. Komathy and P. Narayanasamy, Trust-based evolutionary game model assisting AODV routing against selfishness, Journal of Network and Computer Applications, vol. 31, no. 4, pp. 446-471, 2008.

[30] M. Naserian and K. Tepe, Game theoretic approach in routing protocol for wireless ad hoc networks, Ad Hoc Networks, vol. 7, no. 3, pp. 569-578, 2009.

[31] C. Kamhoua, N. Pissinou, and K. Makki, Game theoretic modeling and evolution of trust in autonomous multi-hop networks: Application to network security and privacy, in Proceedings of the 2011 IEEE International Conference on Communications (ICC). IEEE, 2011, pp. 1-6.

[32] K. Fall and K. Varadhan, The ns Manual, The VINT project, vol. 1, 2002.

[33] J. Luo, X. Ni, and J. Yong, A trust degree based access control in grid environments, Information Sciences, vol. 179, no. 15, pp. 2618-2628, 2009.

[34] Y. Yu, K. Li, W. Zhou, and P. Li, Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures, Journal of Network and Computer Applications, vol. 35, no. 3, pp. 867-880, 2012.

[35] J. Duan, D. Gao, C. H. Foh, and H. Zhang, TC-BAC: A trust and centrality degree based access control model in wireless sensor networks, Ad Hoc Networks, 2013, 10.1016/j.adhoc.2013.05.005.

[36] A. A. Pirzada, C. Mcdonald, and A. Datta, Performance comparison of trust-based reactive routing protocols, IEEE Transactions on Mobile Computing, vol. 5, no. 6, pp. 695-710, 2006.

[37] R. Axelrod, The evolution of strategies in the iterated prisoner's dilemma, in Proceedings of the Genetic Algorithms and Simulated Annealing. 1987, pp. 32-41.

[38] G. Szabó and C. Tőke, Evolutionary prisoner's dilemma game on a square lattice, Physical Review E, vol. 58, no. 1, pp. 69-74, 1998.

[39] G. Szabó J. Vukov and A. Szolnoki, Phase diagrams for an evolutionary prisoner's dilemma game on two-dimensional lattices, IEEE Transactions on Mobile Computing, vol. 72, no. 4, pp. 047107, 2005.

[40] H. Ishibuchi, H. Ohyanagi, and Y. Nojima, Evolution of strategies with different representation schemes in a spatial iterated prisoner's dilemma Game, IEEE Transactions on Computational Intelligence and AI in Games, vol. 3, no. 1, pp. 67-82, 2011.

[41] I. D. Chakeres and L. Klein-Berndt, AODVjr, AODV simplified, ACM SIGMOBILE Mobile Computing and Communications Review, vol. 6, no. 3, pp. 100-101, 2002.

[42] Y. Sun, Z. Han, and K.J.R Liu, Defense of trust management vulnerabilities in distributed networks, IEEE Communications Magazine, vol. 46, no. 2, pp. 112-119, 2008.

[43] H. Deng, G. Jin, K. Sun, R. Xu, M. Lyell, and J.A. Luke, Trust-aware in network aggregation for wireless sensor networks, in Proceedings of the IEEE Global Telecommunications Conference 2009 (GLOBECOM). IEEE, 2009, pp. 1-8.

[44] X. Liu, X. Yang, and Y. Xia, NetFence: preventing internet denial of service from inside out, ACM SIGCOMM Computer Communication Review, vol. 40, no. 4, pp. 255-266, 2010.

Junqi Duan received his B.S. degree in the School of Electronics and Information Engineering from Beijing Jiaotong University of China. He is a Ph.D. student in the National Engineering Laboratory for Next Generation Internet Interconnection Devices at Beijing Jiaotong University. His current research interests include security issues of wireless sensor networks and protocol design of wireless sensor networks.

Deyun Gao (M'06) received B.Eng. and M.Eng. degrees in electrical engineering and a Ph.D. degree in computer science from Tianjin University, China, in 1994, 1999, and 2002, respectively.

He spent one year as a research associate with the Department of Electrical and Electronic Engineering, Hong Kong University of Science and Technology, Kowloon. He then spent three years as a research fellow in the School of Computer Engineering, Nanyang Technological University, Singapore. From 2007, he was on the faculty of Beijing Jiaotong University as an associate professor of School of Electronics and Information Engineering, and was promoted to a full professor in 2012. His research interests are in the area of wireless sensor networks, vehicular networking, and next-generation Internet.

Dong Yang received his B.S. degree from Central South University, Hunan, China, in 2003 and Ph.D. degrees in communications and information science from Beijing Jiaotong University, Beijing, China, 2009. From March 2009 to June 2010, he was a Post-Doctoral Research Associate with Jönköping University, Jönköping, Sweden. He is an associate professor of the School of Electronic and Information Engineering, Beijing Jiaotong University. His research interests are network technologies, including routing, Internet architecture, and wireless sensor networks.

Chuan Heng Foh (S'00-M'03-SM'09) received his M.Sc. degree from Monash University, Australia in 1999 and Ph.D. degree from the University of Melbourne, Australia in 2002. After his PhD, he spent 6 months as a Lecturer at Monash University in Australia. In December 2002, he joined Nanyang Technological University, Singapore as an Assistant Professor until 2012. He is now a Senior Lecturer at the University of Surrey. His research interests include protocol design and performance analysis of various computer networks including wireless local area and mesh networks, mobile ad hoc and sensor networks, 5G networks, and data center networks. He has authored or coauthored over 100 refereed papers in international journals and conferences. He actively participates in IEEE conference and workshop organization, including the International Workshop on Cloud Computing Systems, Networks, and Applications (CCSNA) where he is a steering member. He is an Associate Editor for IEEE Access and International Journal of Communications Systems, and a guest editor for various International Journals. He is currently also the chair of the Special Interest Group on Green Data Center and Cloud Computing under IEEE Technical Committee on Green Communications and Computing (TCGCC). He is a senior member of IEEE.

Hsiao-Hwa Chen (S'89-M'91-SM'00-F'10) is currently a Distinguished Professor in the Department of Engineering Science, National Cheng Kung University, Taiwan. He obtained his BSc and MSc degrees from Zhejiang University, China, and a PhD degree from the University of Oulu, Finland, in 1982, 1985 and 1991, respectively. He has authored or co-authored over 400 technical papers in major international journals and conferences, six books and more than ten book chapters in the areas of communications. He served as the general chair, TPC chair and symposium chair for many international conferences. He served or is serving as an Editor or/and Guest Editor for numerous technical journals. He is the founding Editor-in-Chief of Wileys Security and Communication Networks Journal (www.interscience.wiley.com/journal/security). He is the recipient of the best paper award in IEEE WCNC 2008 and a recipient of IEEE Radio Communications Committee Outstanding Service Award in 2008. Currently, he is also serving as the Editor-in-Chief for IEEE Wireless Communications. He is a Fellow of IEEE, a Fellow of IET, and an elected Member at Large of IEEE ComSoc.