Toward Energy-Efficient Trust System Through Watchdog Optimization for WSNs

Peng Zhou, Siwei Jiang, Athirai Irissappane, Jie Zhang, Jianying Zhou, and Joseph Chee Ming Teo

***Abstract*— Watchdog technique is a fundamental building block to many trust systems that are designed for securing wireless sensor networks (WSNs). Unfortunately, this kind of technique consumes much energy and hence largely limits the lifespan of WSN. Although the state-of-the-art studies have realized the importance of trust systems' efficiency in WSNs and proposed several preliminary solutions, they have overlooked to optimize the watchdog technique, which is perhaps among the top energy-consuming units. In this paper, we reveal the inefficient use of watchdog technique in existing trust systems, and thereby propose a suite of optimization methods to minimize the energy cost of watchdog usage, while keeping the system's security in a sufficient level. Our contributions consist of theoretical analyses and practical algorithms, which can efficiently and effectively schedule the watchdog tasks depending on the sensor nodes' locations and the target nodes' trustworthiness. We have evaluated our algorithms through experiments on top of a WSNET simulation platform and an in-door WSN testbed in our collaborative lab. The results have successfully confirmed that our watchdog optimization techniques can save at least 39.44% energy without sacrificing much security (<0.06 in terms of trust accuracy and robustness), even in some cases enhance the protection against certain attacks.**

***Index Terms*— Wireless sensor network security, trust system, energy-efficiency, watchdog technique.**

I. Introduction

As a critical complement to traditional security mechanisms (e.g., cryptographic methods [1], authentication [2] and access control logics [3] etc.), trust systems are widely applied to protect wireless sensor networks (WSNs for short) from being attacked by "legitimate" sensor nodes (i.e., the nodes are either compromised or selfish or on fault) [4]–[12]. Those nodes can bypass traditional security protections using their "legitimate" identities, but can be possibly captured by trust systems due to their poor reputation or past misbehavior [13]. That is, trust is built upon sensor nodes' reputation and past behaviors, and can be used to model these nodes' honesty and internal states. Although many trust systems [14] enable trust recommendations to extend the trust from neighborhood (i.e., direct trust) to a global network view (i.e., indirect trust), the direct experience of past behaviors is still the basis for securing those recommendations. In another word, sensor nodes' past behaviors constitute the basic foundation for building WSN's trust systems (WSNTSs for short).

However, collecting enough past behaviors through business traffic to build a reliable trust system for WSN is not a trivial task. First, the powerful base station (when WSN has a flat topology [15]) and cluster heads (when a hierarchical topology [16]), both of which are likely to have business requirements to interact with the whole network (or the entire cluster), may not locate in the communication range (i.e., neighborhood) of all sensor nodes (i.e., some nodes are remote), hence missing the opportunity to have direct experiences of those remote nodes. Second, some sensor nodes may not have business requirements to interact with their neighbour nodes, or their business interactions occur at a very low frequency. Those lazy nodes' past behaviors are hard to be collected using business traffic. Third, since trust is context aware [17], [18], the experience of one kind of behaviors cannot be used to build up trust for another kind. For example, a node behaving well to forward routing packets in the past does not mean the sensing data reported from this node is trustworthy (i.e., past multi-hop routing behaviors cannot derive the trust for data sensing). As a result, WSN may lack a wide variety of business traffic to build up all kinds of trust. To tackle those challenges and facilitate past behavior collection, most of existing WSNTSs have adopted a so-called watchdog technique [19]. Using this technique, sensor nodes can operate as proactive monitors and launch trust-dedicated tasks in a pre-defined frequency to directly interact with their neighborhood nodes. They thus can get the first-hand experiences of these nodes' behaviors, even if no business tasks happen. For example, a node can actively query other nodes' sensing data in some time interval [6] (despite it does not actually require those data for business purpose),

Manuscript received August 10, 2014; revised November 23, 2014; accepted December 22, 2014. Date of publication January 6, 2015; date of current version February 9, 2015. The work of J. Zhang was supported by the A*STAR/I2R-SERC, Public Sector Research Funding (PSF) Singapore (M4070212:020). The associate editor coordinating the review of this manuscript and approving it for publication was Prof. T. Charles Clancy.

P. Zhou is with the Shanghai Key Laboratory of Power Station Automation Technology, School of Mechatronic Engineering and Automation, Shanghai University, Shanghai 200072, China, and also with the School of Computer Engineering, Nanyang Technological University, Singapore 639798 (e-mail: pzhou@shu.edu.cn).

S. Jiang is with the Singapore Institute of Manufacturing Technology, Singapore 638075 (e-mail: jiangsw@simtech.a-star.edu.sg).

A. Irissappane and J. Zhang are with the School of Computer Engineering, Nanyang Technological University, Singapore 639798 (e-mail: athirai001@e.ntu.edu.sg; zhangj@ntu.edu.sg).

J. Zhou and J. C. M. Teo are with the Institute for Infocomm Research, Singapore 138632 (e-mail: jyzhou@i2r.a-star.edu.sg; cmteo@i2r.a-star.edu.sg).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2015.2389145

or continuously overhear its neighborhood's routing communications through the promiscuous mode [4], [20].

Although the watchdog technique has been proved as a very effective approach to build up WSNTS's foundations, it introduces a large amount of additional energy consumptions which conflict the energy efficient design principle of WSN. More precisely, sensor nodes are usually equipped with limited battery, and work in an unattended mode for a long period of time to adapt various harsh environments such as the deep desert and ocean abyss. Rechargement or replacement of those nodes' power is very difficult and expensive. Due to those challenges, energy saving plays a very important role in the design of modern WSNs [21]. However, to our best knowledge, no existing WSNTSs give appropriate solutions to save the energy consumed by the watchdog technique (i.e., the trust-energy conflict induced by watchdog usage has not been addressed before). In particular, some WSNTSs do not discuss how to schedule watchdogs in their proposals [20], [22], while some others implicitly suggest to let sensor nodes launch neighbour-flooding watchdog tasks to monitor all their neighbors and do not study which frequency is appropriate for their monitoring [4], [6], [23]. This kind of neighbour-flooding methods could make running watchdogs redundant and will waste a lot of energy without inducing much additional security benefits. As a result, to simultaneously save energy and collect sufficient past behaviors for trust evaluation, an intelligent watchdog scheduler is highly required.

In this paper, we will fill in this gap by optimizing watchdog techniques for WSNTSs to balance energy efficiency and security (in terms of trust accuracy and robustness). Our ultimate goal is to reduce the energy cost induced by watchdog tasks as much as possible, while keeping trust accuracy and robustness in a sufficient level. To touch this goal, we optimize watchdog techniques in two levels. First, we optimize watchdog locations by considering the fact: although sensor nodes which are located more closely may consume less energy to monitor each other due to shorter communication distance [24], these nodes are more likely of being compromised together and launch collaborative attacks [25]. We therefore explore the optimal watchdog location (given a target node) to minimize the overall risk (in terms of both energy consumption and security). Second, we optimize watchdog frequency and reduce its redundancy. In particular, compared with the sensor nodes whose behaviors are more uncertain, the nodes with more determined trustworthiness (i.e., trustworthy or untrustworthy) may require less watchdog tasks (i.e., lower watchdog frequency) to further investigate. We thus seek appropriate watchdog frequency depending on target nodes' trustworthiness.

To sum up, we make three major contributions in this paper.

1) We conduct a novel study to reveal trust-energy conflict induced by the inefficient use of watchdog techniques in existing WSNTSs. This conflict has not been comprehensively addressed by prior research in the literature.
2) We optimize watchdog techniques in two levels, both of which consist of a theoretical analysis to show potential optimal results and a practical algorithm to efficiently and effectively schedule watchdog tasks.
3) We evaluate our optimization techniques using extensive experiments in a WSNET simulation platform [26] and an in-door testbed in our collaborative lab. The experimental results have successfully confirmed the effectiveness of our design.

The remainder of this paper is structured as follows. We first review the literature in Section II. We then give a high level overview of WSN and WSNTS models in Section III. We present our watchdog optimization algorithms in Section IV, and evaluate these algorithms in Section V. After discussing some limitations and potential future works in Section VI, we conclude this paper in Section VII.

II. Background and Related Work

In this section, we revisit state-of-the-art WSNTSs in the literature, especially the systems designed for efficient trust management in WSNs.

Basically, trust systems are designed and deployed in WSNs for a general security purpose (to identify and isolate "legitimate" sensor nodes which are either compromised by attackers, or selfish to refuse assisting others, or on fault due to misconfigurations and bugs), and can protect particular WSN functionalities. In the literature, WSNTS is usually applied to avoid unreliable and corrupted sensing data [6], or secure multi-hop routing [4], [8], [27], [28], or protect both of them [7], [9]–[11], [23]. Many of those WSNTSs [4], [6], [10], [11], [23] claim that they adopt a watchdog or watchdog-like technique for trust behavior collection, and hence get a very good performance in guarding data sensing and multi-hop routing. They have this achievement since they can collect enough past behaviors for trust evaluation through watchdogs. For example, [6] employs the watchdog technique to actively collect sensing data from neighbor nodes, and applies an outlier detection algorithm to detect invalid data reported by compromised or faulty nodes. [4] lets a sensor node work as a watchdog to overhear the past routing behaviors in its neighborhood, hence identifying misbehaving sensor nodes and preventing those nodes from being used for future routing.

Although WSNTSs can largely enhance WSNs' functionality and security, the energy overhead induced by the construction of such systems cannot be neglected. More seriously, although WSNs are usually expected to work in an unattended mode for a long period of time (e.g., two or three years without battery recharge), they are usually equipped with restricted resource and battery. For this reason, WSNs' long life expectation could be dramatically limited if the cost induced by trust management is heavy. In state-of-the-art research, several WSNTSs have realized the significance of the efficiency problem and proposed some preliminary solutions in their design. In particular, [10] proposed a storage-efficient trust model by applying a geographic hash table to identify trust managers (may save energy due to low storage usage), while [28] implemented an energywatcher to help sensor nodes estimate their neighbor nodes' energy cost for each packet forwarding and thus enable the selection of the most efficient node as their next hop in the route. Moreover, a clustering technology is widely used by the literature [7], [27] to make WSNs and WSNTSs energy-efficient. By electing a number of cluster heads to manage sensor nodes (cluster members) on behalf of the base station, energy consumption can be reduced due to shorter communication distance. Based on the clustered topology, [11] further reduced energy by cancelling feedback (i.e., trust recommendation) between cluster members and/or between cluster heads, and thereby proposed a more lightweight WSNTS.

Despite those preliminary efforts, none has taken watchdog technique, perhaps the largest energy consumption unit in WSNTS, into consideration. We thereby conduct an innovative study in this paper to optimize watchdog scheduling. Our research is very different compared to the literature and opens a new door to energy-efficient WSNTS design. First, unlike [10] which is mainly designed to save storage rather than energy, our research takes energy saving as a central topic and optimizes watchdog technique for the first time. Second, although [28] proposes an energy-efficient secure routing algorithm to choose efficient and trustworthy next-hop node in a route, it cannot reduce the energy used to build up WSNTS, which is the major problem we should solve in this paper. Third, unlike the clustering techniques [7], [27] which save energy by reorganizing WSN's topology to a hierarchical architecture, our research saves energy by means of reducing redundant trust foundations in WSNTS. And even better, our solution can also be applied to clustered WSNs to further reduce energy cost. Last but the most relevant, [11] designs an energy-efficient WSNTS by reducing unnecessary communications of trust recommendations (a.k.a. second-hand experiences). Unlike that, our research goes a step forward to save energy by reducing unnecessary watchdog tasks (a.k.a. first-hand experiences). As discussed by [14], the first-hand experience is more expensive (in terms of energy consumption) than the second-hand one. We therefore obtain a more advanced opportunity to save energy than [11].

III. Model Overview

In this section, we formalize WSN and WSNTS using four high level models. More precisely, we first present a system model to describe WSN in Section III-A. We then model WSN's energy consumption law in Section III-B. Afterwards, we reason about WSNTS on top of a threat model in Section III-C and a trust model in Section III-D, respectively. For the ease of reference, we summarize important notations used by this paper in Table I.

TABLE I
Important Notations

Notation	Definition
$G = (V, E)$	An undirected graph used to model a WSN
v_i	$v_i \in V$ represents a sensor node in WSN
r_i	v_i's communication range
d_{ij}	The spatial distance between v_i and v_j
e_{ij}	$e_{ij} \in E$ exists iff $d_{ij} \leq r_i$ & $d_{ij} \leq r_j$
B_j	The set of v_j's neighborhood nodes
W_j	The set of v_j's watchdog nodes
ϵ	The free space constant measured in J/bit/m^2
t	A discrete time slot, the minimal time unit in this paper
N	A time window consists of a sequence of discrete time slots
w_{ij}^t	The watchdog task v_i performs to monitor v_j at time slot t
L	The bits of information transmitted by a watchdog task
A	The set of sensor nodes under attackers' control in WSN
α	A parameter to control the probability of collaborative attackers
T_{ij}	v_j's trustworthiness from v_i's point of view
Λ_{ij}	The accuracy of T_{ij} (trust accuracy)
Υ_j	The average accuracy of T_{ij}s for $\forall v_i \in W_j$ (trust robustness)
I_{ij}^t	The event representing whether v_j's behavior is expected by v_i at t
$\mathbf{Q}_{ij}$	The distribution of I_{ij}^ts for $t \in N$
I_j^t	the event to represent v_j's true internal behavior at t
$\mathbf{P}_j$	The distribution of I_j^ts for $t \in N$
f_{ij}	Watchdog frequency v_i uses to monitor v_j
f_j	A sensor node v_j's internal behavior frequency
fa_j	A sensor node v_j's attacking/faulty behavior frequency
fn_j	A sensor node v_j's normal behavior frequency
π_i	Used by DBP algorithm to determine the size of W_i
μ	Used by HWFA(E) algorithm to keep watchdog redundancy

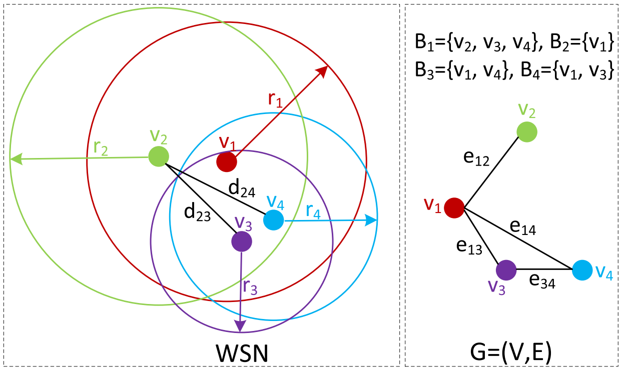


Fig. 1. An example of WSN and the system model G.

A. System Model

We model a WSN as an undirected graph $G = (V, E)$, where $\upsilon_i \in V$ represents a sensor node in WSN and $e_{ij} \in E$ means that the nodes υ_i and υ_j are within each other's communication range (i.e., neighborhood). We design our methods by considering a flat WSN topology, although our solutions work within the scope of neighborhood and thus also adapt to other topologies such as the clustering WSN. Let d_{ij} be the spatial distance between υ_i and υ_j, and let r_i be the communication range of υ_i. We consider that $e_{ij} \in E$ exists iff $d_{ij} \leq r_i$ and $d_{ij} \leq r_j$. We therefore define $B_i \subseteq V$ as the set of υ_i's neighborhood nodes. We have $B_i = \{\upsilon_j | e_{ij} \in E\} = \{\upsilon_j | d_{ij} \leq r_i \text{ \& } d_{ij} \leq r_j\}$. Figure 1 gives an example of our WSN system model. As can be seen, although υ_3 and υ_4 are within υ_2's communication range (i.e., $d_{23} \leq r_2$ and $d_{24} \leq r_2$), e_{23} and e_{24} do not exist (i.e., $\upsilon_3, \upsilon_4 \notin B_2$) because $d_{23} > r_3$ and $d_{24} > r_4$.

To formalize a watchdog task on top of G, we first separate time space into a sequence of consecutive time slots with equal size. We then define w_{ij}^t as a watchdog task the node υ_i performs to monitor its neighbor node υ_j at time slot t. A watchdog task w_{ij}^t consists of a bidirectional communication between the watchdog node υ_i and the target node υ_j. That is, υ_i should send a request packet to υ_j and then wait for υ_j's response. By this requirement, υ_i can take watchdog task w_{ij}^t to monitor υ_j iff $d_{ij} \leq r_i$ and $d_{ij} \leq r_j$ (i.e., e_{ij} exists in G). In another word, the node υ_i can work as a watchdog to monitor only $\forall v_j \in B_i$, and vice versa, only $\forall v_j \in B_i$ can perform watchdog tasks to monitor v_i.

B. Energy Consumption Model

To estimate energy consumed by each watchdog task w_{ij}^t, we follow a typical free space wireless radio model, which is widely adopted by the literature (e.g., LEACH [24]). In this model, a sensor node's transmitter unit consists of a transmit electronics device and a power amplifier, both of which will consume energy when transmitting signals. In contrast, a node's receiver unit only consumes energy due to the receive electronics device. We follow prior research like [24] and [29] to assume that a proper power controller has been deployed to adjust transmit power amplifier according to the transmission distance. Let ε^{elec} be the energy consumed by a sensor node's transmit electronics (or receive electronics) when sending (or receiving) 1 bit information (measured in J/bit). Let ϵ be free space constant measured in J/bit/m^2. We then can calculate the energy consumption when v_i transmits 1 bit information to its neighbor node v_j ($d_{ij} \leq r_i$) as:

$$\varepsilon_{ij}^{TX} = \varepsilon^{elec} + \epsilon \cdot d_{ij}^2. \tag{1}$$

Meanwhile, the energy consumed by v_i for receiving 1 bit information from neighbor node v_j can be computed as:

$$\varepsilon_{ij}^{RX} = \varepsilon^{elec}. \tag{2}$$

As described in Section III-A, to accomplish a watchdog task w_{ij}^t, the watchdog node v_i should first send query to target node then receive target node's reply, while the target node v_j should first receive the query from the watchdog node then send back the reply. As a result, if a watchdog task w_{ij}^t requires L bits information for either query or response, the energy consumed by the watchdog node v_i for this task is:

$$\varepsilon_i(w_{ij}^t) = L \cdot (\varepsilon_{ij}^{TX} + \varepsilon_{ij}^{RX}) = 2 \cdot L \cdot \varepsilon^{elec} + \epsilon \cdot L \cdot d_{ij}^2. \tag{3}$$

The target node v_j's energy consumption for this watchdog task w_{ij}^t is (note that $d_{ij} = d_{ji}$):

$$\varepsilon_j(w_{ij}^t) = L \cdot (\varepsilon_{ji}^{RX} + \varepsilon_{ji}^{TX}) = 2 \cdot L \cdot \varepsilon^{elec} + \epsilon \cdot L \cdot d_{ji}^2. \tag{4}$$

C. Threat Model

In our design, we assume some sensor nodes could be compromised or selfish or on fault. By exploiting those "legitimate" nodes, we consider two kinds of attacking behaviors. One is for disrupting WSN's normal functionalities such as routing and data sensing, and the other is for attacking WSNTS itself. In particular, we consider the attacking capabilities as follows:

1) Attacking From "Legitimate" Sensor Nodes: We consider the attackers who are capable of compromising some vulnerable sensor nodes or deploying malicious or faulty nodes to WSN. Attackers can exploit these nodes' "legitimate" identities to break traditional security protections, and hence can launch offensives to the remainder of WSN. Further, we consider the attacking model cooperative, where the nodes that are closer to an attacker's node are more likely of being controlled by the attacker as well [25]. We let $A \subseteq V$ be the set of the "legitimate" sensor nodes under attackers' control. Then, given an attacker's node v_j, the probability that another node v_i is also under attacker's control is inversely proportional to d_{ij}:

$$Pr[v_i \in A | v_j \in A] \propto \frac{1}{\alpha \cdot d_{ij}}. \tag{5}$$

However, $\frac{1}{\alpha \cdot d_{ij}}$ cannot be used as a probability function directly, because $\frac{1}{\alpha \cdot d_{ij}}$ belongs to $[0, +\infty]$ but a possible probability function should be falling into $[0, 1]$. To tackle this issue, we need to give a feasible probability definition that satisfies $Pr[v_i \in A | v_j \in A] \in [0, 1]$ and $Pr[v_i \in A | v_j \in A] \propto \frac{1}{\alpha \cdot d_{ij}}$ simultaneously. To meet this requirement, we define the probability function as $Pr[v_i \in A | v_j \in A] = \frac{1}{\alpha \cdot d_{ij} + 1}$ in this paper. This probability function is feasible and meaningful. In particular, WSN attackers usually exploit wireless signal to intrude sensor nodes. A longer distance leads to a weaker attacking signal, which represents a weaker attacking capability [25]. As a result, Eq. (5) can naturally reflect such wireless attacking scenario. More precisely, $d_{ij} = 0$ can lead $Pr[v_j \in A | v_i \in A] = 1$ since it indicates that v_i and v_j are the same node or different nodes located at the same position. While, with d_{ij} increasing, $Pr[v_j \in A | v_i \in A]$ will decrease due to the weakening signal and can eventually reach 0 when d_{ij} approximates $+\infty$. A larger α indicates a higher decreasing speed of $Pr[v_i \in A | v_j \in A]$ when d_{ij} increases.

2) Attacking WSN: By exploiting the "legitimate" sensor nodes, attackers could perform insider attacks to disrupt WSN's normal functionalities, such as damaging the quality of multihop routing by selectively dropping routing packets or misleading WSN's data aggregation by reporting crafted sensing data. Those attacks can avoid traditional security mechanism.

3) Attacking WSNTS: Moreover, we consider attackers smart enough and are aware of the existence of WSNTS. Those attackers attempt to evade WSNTS's detection by launching some advanced attacks. In particular, we consider four types of WSNTS attacks in this paper (all of them have been widely considered in the literature [14], [18]). The first is an *on-off attack*, where attacker's node may behave well for a long time to get enough reputation then do malicious behaviors suddenly. The second is a *discrimination attack* where attacker's node will behave differently to different sensor nodes (watchdogs). The third is a *bad-mouthing attack*, where attacker's node will perform watchdog tasks and report an honest node as a malicious one. The last is a *sybil attack* where attackers can control a large number of sensor nodes to mislead WSNTS.

D. Trust Model

In this paper, we model the trust of a sensor node as this node's expected behavior distribution over time. The behavior could be data sensing or routing behavior etc. This trust model can allow our analysis to be focused on WSNTS's foundation, and will not be affected by higher level's trust update and aggregation processes. On top of this model, we introduce three concepts. One is *trustworthiness* that can be used to estimate a sensor node's behavior. The other two are *trust accuracy* and *trust robustness*, which can be used to measure how accurate the target nodes' trustworthiness can be recovered in the presence of WSN attacks and WSNTS attacks respectively. Unlike the trustworthiness that the trust systems need to calculate at run time, the trust accuracy and trust robustness are two performance indices that we can use to evaluate and compare different trust systems' security levels. Trust systems do not need to compute the trust accuracy and robustness at run time.

1) Trustworthiness: From some watchdog node v_i's point of view, we define a sensor node v_j's trustworthiness in the context of a particular behavior (e.g., data sensing or routing etc.) as the percentage of v_j's behaviors that meet v_i's expectation among all the v_j's behaviors watched by v_i in a time window N. We denote this trustworthiness as T_{ij}. We then define I_{ij}^t as the event to represent whether v_j's behavior is expected by v_i at time slot t. I_{ij}^t returns 1 if v_j's behavior follows v_i's expectation and returns 0 otherwise. Watchdog node's expectation is context aware. For data sensing, watchdog nodes believe their own sensing function works fine and expect to see the similar sensing value reported by the target nodes. But for routing task, watchdog nodes expect target nodes can successfully help forward packets. We calculate T_{ij} as:

$$T_{ij} = \frac{\sum_{t \in N \vee w_{ij}^t \neq \varnothing} I_{ij}^t}{\sum_{t \in N \vee w_{ij}^t \neq \varnothing} 1}, \tag{6}$$

where, $w_{ij}^t \neq \varnothing$ means the watchdog node v_i actually performs watchdog task to monitor v_j at time slot t.

2) Trust Accuracy and Trust Robustness: We let I_j^t be the event to describe a sensor node v_j's internal behavior and draw it according to a binary distribution function $\mathbf{P}_j$. $I_j^t = 1$ if v_j behaves well at time slot t while $I_j^t = 0$ if v_j performs attacks against WSN at t (e.g., reporting corrupted sensing data or refusing packet forwarding etc.). Watchdog node v_i can sample $\mathbf{P}_j$ to discrete events I_{ij}^ts. We then model the accuracy of T_{ij} (i.e., **trust accuracy**) using the Kullback-Leibler divergence [30] between the probability distribution of I_j^ts (i.e., $\mathbf{P}_j$) and the distribution of I_{ij}^ts (denoted as $\mathbf{Q}_{ij}$). KL divergence is a well known measure of the information loss when using one information source (i.e., probability distribution) to approximate another, and hence being a good choice to measure trust accuracy. Let I be the random variable of distribution $\mathbf{P}_j$ and $\mathbf{Q}_{ij}$. We then can follow [30] to calculate KL divergence as:

$$D_{KL}(\mathbf{P}_j || \mathbf{Q}_{ij}) = \sum_I ln(\frac{\mathbf{P}_j(I)}{\mathbf{Q}_{ij}(I)})\mathbf{P}_j(I). \tag{7}$$

We use Λ_{ij} to denote trust accuracy and measure it as:

$$\Lambda_{ij} = \frac{1}{D_{KL}(\mathbf{P}_j || \mathbf{Q}_{ij}) + 1}. \tag{8}$$

As can be seen, $\Lambda_{ij} \in [0, 1]$ and a larger Λ_{ij} indicates more accurate of the trustworthiness T_{ij}. If the watchdog node v_i can correctly observe v_j's behaviors for all the time slots t within time window N, v_i will get the same $\mathbf{Q}_{ij}$ as $\mathbf{P}_j$ (which leads to $\Lambda_{ij} = 1$) and be able to accurately (without losing any information) rebuild v_j's internal behaviors. We use trust accuracy to express WSNTS's effectiveness against WSN attacks, as it can well reflect watchdog's capability of rebuilding target node's internal behaviors.

By considering WSNTS attacks, a target node v_j's behaviors observed by different watchdog nodes are likely different. For example, some malicious target nodes may behave differently to different watchdog nodes (discrimination attack), and some malicious watchdog nodes may report false observations to others (bad-mouthing attack). To address this issue and enable our analysis to cover WSNTS attacks, we introduce a new concept, **trust robustness**, to measure WSNTS's effectiveness against WSNTS attacks. We define trust robustness as mean value of trust accuracy provided by a group of cooperative watchdog nodes. This definition can naturally bound the average effectiveness of watchdog nodes in the presence of the WSNTS attacking model. We let Υ_j be the trust robustness of target node v_j and can calculate it as:

$$\Upsilon_j = \frac{\sum_{v_i \in W_j} \Lambda_{ij}}{||W_j||}, \tag{9}$$

where, $W_j \subseteq B_j$ is a set of cooperative watchdog nodes which will monitor v_j together, and $|| * ||$ is the size of set $*$. Since $\forall v_i \in W_j, \Lambda_{ij} \in [0, 1]$, we also have $\Upsilon_j \in [0, 1]$. As can be seen in Eq. 9, the higher trust robustness means more watchdog nodes can accurately rebuild target node's internal behaviors in the presence of malicious and discriminated neighbor nodes, hence demonstrating better capability against WSNTS attacks.

IV. Watchdog Optimization Techniques

In this section, we first formalize the watchdog optimization problem in Section IV-A. We then seek theoretical and practical solutions to this problem by dividing it into two sub problems, which consist of a location optimization problem in Section IV-B and a frequency optimization problem in Section IV-C.

A. Optimization Goal

Generally, we have two ultimate goals when optimizing watchdog techniques: one is to minimize the energy cost of the whole WSN and the other is to maximize security (in terms of trust accuracy and trust robustness). We can write our optimization goals as follows.

$$Minimize \sum_{v_j \in V} \sum_{v_i \in W_j} \sum_{t \in N \wedge w_{ij}^t \neq \varnothing} (\varepsilon_i(w_{ij}^t) + \varepsilon_j(w_{ij}^t)), \tag{10}$$

$$Maximize \sum_{v_j \in V, W_j = \{v_i\}} \Lambda_{ij} \ or \ Maximize \sum_{v_j \in V} \Upsilon_j, \tag{11}$$

where, Eq. (10) is for minimizing energy consumption throughout the whole WSN. The former part of Eq. (11) is for maximizing trust accuracy in face of WSN attacks while the latter one is for maximizing trust robustness in presence of WSNTS attacks. To solve the above optimization problem, our target is to find appropriate W_j for each $\upsilon_j \in V$ and the number of $w_{ij}^t \neq \varnothing, \upsilon_i \in W_j$ for each $t \in N$. We thereby divide the complete problem into two sub problems: (1) how to select nodes from each target node's neighborhood to perform watchdog tasks (i.e., finding W_j for $\forall \upsilon_j \in V$), and (2) how to schedule watchdog tasks among those selected watchdog nodes given a target node (i.e., determining how many $w_{ij}^t \neq \varnothing$ for $\upsilon_i \in W_j$ and $t \in N$). In the following two subsections IV-B and IV-C, we present theoretical analyses and practical algorithms for these two sub problems. Our practical algorithms can touch energy-efficient WSNTS design goal without costing (much) security (as shown in our extensive WSNET simulation and in-door WSN testbed experiments in Section V).

B. Watchdog Location Optimization

1) Theoretical Analysis: We cannot find the optimal $W_j, \forall \upsilon_j \in V$ by directly solving the optimization problem described in Eq. (10) and (11), because they are ill-posed and do not have solution in closed form. To conquer this challenge, we find optimal watchdog positions instead (find optimal d_{ij} given $\forall \upsilon_j \in V$). The selection of neighbour nodes $\upsilon_i \in B_j$ which are located closer to the optimal d_{ij} is more likely able to form the optimal W_j. To transform the original optimization problem of finding optimal W_j to the problem of finding optimal d_{ij}, the intuitive evidence is that: although the $\upsilon_i \in B_j$ with a shorter d_{ij} will consume less energy to perform watchdog tasks to monitor υ_j (see Eq. (3) and Eq. (4)) and hence ensure the energy minimization goal in Eq. (10), such υ_i is more likely of being controlled by attackers if υ_j is an attacker's node (see Eq. (5)). The use of attackers' node as watchdogs will impede the security maximization goal in Eq. (11), since those nodes can report false watchdog results to drop trust robustness. We therefore find the optimal watchdog location d_{ij} given a target node υ_j by considering an overall risk, which considers both energy and security (in terms of $Pr[\upsilon_i \in A | \upsilon_j \in A] \propto \frac{1}{\alpha \cdot d_{ij}}$):

$$F(d_{ij}) = 2L\epsilon d_{ij}^2 + \frac{1}{\alpha d_{ij}}, \tag{12}$$

where, $2L\epsilon d_{ij}^2$ is the distance relevant part of energy consumption function $\varepsilon_i(w_{ij}^t) + \varepsilon_j(w_{ij}^t) = 4L\varepsilon_i^{elec} + 2L\epsilon d_{ij}^2$. We directly merge $2L\epsilon d_{ij}^2$ and $\frac{1}{\alpha d_{ij}}$ into $F(d_{ij})$ using an additive function, because they share the same domain range (i.e., they both vary from 0 to ∞ when $d_{ij} \in [0, \infty]$). $F(d_{ij})$ can measure the overall risk of energy consumption and security in a balanced manner. We give the minimal risk $F(d_{ij})$ and its corresponding optimal d_{ij} in Theorem 1.

Theorem 1: The overall risk $F(d_{ij})$ can achieve its theoretically minimal value when $d_{ij} = (4L\epsilon\alpha)^{-\frac{1}{3}}$.

Proof: It is known that, if a function has an extreme value and the function's second derivative is larger than 0, this extreme value is the function's minimal value. Such minimal value can be obtained when letting the function's first derivative be equal to 0. For $F(d_{ij})$, we have its second derivative:

$$\frac{\partial^2 F}{\partial d_{ij}^2} = 4 \cdot L \cdot \epsilon + 2 \cdot \frac{1}{\alpha \cdot d_{ij}^3} > 0.$$

We thus find $F(d_{ij})$'s minimal value by letting its first derivative equal to 0:

$$\frac{\partial F}{\partial d_{ij}} = 4 \cdot L \cdot \epsilon \cdot d_{ij} - \frac{1}{\alpha \cdot d_{ij}^2} = 0.$$

We solve above equation by considering d_{ij} as variant and get result $d_{ij} = (4L\epsilon\alpha)^{-\frac{1}{3}}$. Theorem 1 has been proved. □

If we form W_j by selecting the υ_i with minimal $F(d_{ij})$, it approximately equals to optimize Eq. (10) and Eq. (11) under a constraint $d_{ij} = (4L\epsilon\alpha)^{-\frac{1}{3}}$ for $\upsilon_i \in W_j$. This constraint makes our optimization goal well-posed and solvable. It is worth noting that, if $(4L\epsilon\alpha)^{-\frac{1}{3}} > r_j$, we can choose $d_{ij} = r_j$ as the optimal distance.

2) Practical Algorithm (DBP Algorithm): Although Theorem 1 gives the optimal watchdog location in theory, it is still challenging to apply this theoretical solution to practical WSN. The reason is that, for almost sensor nodes, we cannot assume there necessarily exist some neighbour nodes located at the optimal watchdog location. In common, almost $\upsilon_j \in V$ may have their neighbors $\forall \upsilon_i \in B_j$, $d_{ij} \neq (4L\epsilon\alpha)^{-\frac{1}{3}}$. To address this issue, an intuitive solution is to choose the node nearest to the theoretically optimal location as watchdog. However, this intuitive algorithm is vulnerable to discrimination attacks. That is, since the intuitive algorithm fixes the watchdog node to υ_j's nearest neighbour, $\upsilon_j \in A$ can simply behave well to υ_j's nearest node but launch WSN attacks (e.g., dropping routing packets or reporting dishonest sensing data) to the rest of υ_j's neighborhood.

To tackle discrimination attack while still consult the optimal location to form W_j, we propose a new *distance-based probabilistic* algorithm (*DBP* algorithm for short). This algorithm can find a set of watchdog nodes by considering those nodes' locations in a probabilistic manner. Given a target node υ_j, DBP algorithm selects $\pi_j \cdot ||B_j||$ nodes from υ_j's neighbourhood B_j to form watchdog node set W_j (i.e., $||W_j|| = \pi_j \cdot ||B_j||$), and the selection probability of $\forall \upsilon_i \in B_j$ satisfies $Pr[\upsilon_i \in W_j] \propto \frac{1}{|d_{ij} - (4L\epsilon\alpha)^{-\frac{1}{3}}|}$, where $|| * ||$ is the size of set $*$, $| * |$ returns the absolute value of $*$ and $\pi_j \in (0, 1]$. We prove why we choose $Pr[\upsilon_i \in W_j] \propto \frac{1}{|d_{ij} - (4L\epsilon\alpha)^{-\frac{1}{3}}|}$:

Proof: In the DBP algorithm, the watchdog node selection probability $Pr[\upsilon_i \in W_j]$ should be larger in case the neighbor node is closer to the optimal position $(4L\epsilon\alpha)^{-\frac{1}{3}}$ given a target node $\upsilon_j \in V$. Obviously, in a polar coordinates, the target node υ_j's optimal position can form a circle in which the υ_j is the center and $(4L\epsilon\alpha)^{-\frac{1}{3}}$ is the radius. The nodes have the distance $(4L\epsilon\alpha)^{-\frac{1}{3}}$ to υ_j at any angle are always optimal. As d_{ij} is the distance between the target node υ_j and another node υ_i in a certain angle, $|d_{ij} - (4L\epsilon\alpha)^{-\frac{1}{3}}|$ can express the distance between υ_i and the target node υ_j's optimal position. Therefore, $Pr[\upsilon_i \in W_j] \propto \frac{1}{|d_{ij} - (4L\epsilon\alpha)^{-\frac{1}{3}}|}$ can well

Algorithm 1 Distance-Based Probabilistic (DBP) Algorithm

```
Input: $\pi_j$, $B_j$, $d_{ij}$ for $\forall \upsilon_i \in B_j$, $L$, $\epsilon$, $\alpha$
Output: $W_j$
$W_j \leftarrow \varnothing$
while $||W_j|| < \pi_j \cdot ||B_j||$ do
    $x \leftarrow random(0, \sum_{k \in B_j} \frac{1}{|d_{kj} - (4L\epsilon\alpha)^{-\frac{1}{3}}|})$
    if $\sum_{k=1}^{i} \frac{1}{|d_{kj} - (4L\epsilon\alpha)^{-\frac{1}{3}}|} \leq x < \sum_{k=1}^{i+1} \frac{1}{|d_{kj} - (4L\epsilon\alpha)^{-\frac{1}{3}}|}$ then
        $W_j \leftarrow W_j \vee \upsilon_i$
    end if
end while
```

represent that the nodes near the optimal position have a higher probability to be selected. □

DBP algorithm can resist discrimination attack due to the probabilistic selection manner and the maintenance of some watchdog node redundancy determined by π_j. Algorithm 1 describes the pseudo code of our DBP algorithm runs in each sensor node $\upsilon_j \in V$. There, the function $random(0, \sum_{k \in B_j} \frac{1}{|d_{kj} - (4L\epsilon\alpha)^{-\frac{1}{3}}|})$ returns a random float value belonging to $[0, \sum_{k \in B_j} \frac{1}{|d_{kj} - (4L\epsilon\alpha)^{-\frac{1}{3}}|}]$.

C. Watchdog Frequency Optimization

1) Theoretical Analysis: When watchdog nodes have been determined, the next optimization point is to find the minimal number of required watchdog tasks to save energy but keep security in a sufficient level. We define the number of watchdog tasks a watchdog node υ_i performs to monitor a target node υ_j within a time window N as watchdog frequency f_{ij}. We have $f_{ij} = \sum_{t \in N \wedge w_{ij}^t \neq \varnothing} 1$. Also, we define a node υ_j's behavior frequency and attacking frequency within the time window N as f_j and fa_j respectively. We then have $f_j = \sum_{t \in N} 1$ and $fa_j = \sum_{t \in N}(1 - I_j^t)$. In fact, the behavior frequency is determined by how the sensor nodes sense the environment. Taking the temperature sensing as an example, the behavior frequency is the number of times a sensor node measures the temperature within a pre-defined time window N. This frequency can be set up when the WSN is configured and deployed. On the other hand, the attacking frequency is determined by how the adversaries modify the sensing data to a false value. It must be smaller than the behavior frequency, because the adversaries can at most tamper all the data sensed by a compromised node.

We can model watchdog tasks as a sampling process, where watchdog nodes attempt to reconstruct the target node's internal behaviors based on their watched samples. We thus give the theoretical solution to the minimized watchdog frequency which can maximize Eq. (11) in Theorem 2.

Theorem 2: Given a watchdog node υ_i, to ensure perfect reconstruction of target node υ_j's internal behaviors and thus maximize Eq. (11), the minimal watchdog frequency (for minimizing Eq. (10)) is $f_{ij} = f_j$.

Proof: According to the Nyquist-Shannon sampling theorem [31], to have perfect fidelity for reconstructing a target signal, the sample-rate (i.e., sampling frequency) should be larger than two times of the target signal's frequency. In our problem, the target signal is for target node's internal behaviors, which contain binary values to represent normal behavior and attacking behavior. We have the attacking behavior frequency as fa_j and the normal behavior frequency as fn_j. As a result, to ensure perfect reconstruction of attacking behavior, the minimal sampling frequency f_{ij} (i.e., watchdog frequency) is $f_{ij} = 2 \cdot fa_j$. Similarly, to ensure perfect reconstruction of normal behavior, the minimal f_{ij} is $f_{ij} = 2 \cdot fn_j$. Since we have $f_j = fa_j + fn_j$ and f_j for $\forall \upsilon_j \in V$ is a known parameter which can be set up during WSN configuration, we can precisely recover attacking behavior if the normal one has been perfectly reconstructed, and vice versa. Therefore, the minimal f_{ij} that can perfectly reconstruct both normal and attacking behaviors is $f_{ij} = 2 \cdot \min(fn_j, fa_j)$. Moreover, since $\min(fn_j, fa_j) \leq \frac{f_j}{2}$, we have the minimal frequency $f_{ij} = 2 \cdot \frac{f_j}{2} = f_j$ which can perfectly reconstruct both normal and attacking behaviors regardless how fn_j and fa_j vary. Theorem 2 has been proved. □

Although Theorem 2 states the best watchdog frequency in theory, this result cannot ensure the perfect reconstruction in practical WSNs due to the unreliable and noisy transmission nature. For example, when performing watchdog tasks to monitor routing behavior, the watchdog nodes may waste some watchdog tasks if they miss the target node's forwarding packets due to noises. We will consider this issue in our practical algorithm design.

2) Practical Algorithm (HWFA(E) Algorithm): Despite the theoretically minimal value given by Theorem 2, we can further reduce watchdog frequency in practical WSNs by considering target node's trustworthiness. This practical reduction is based on an intuitive observation: if trustworthiness T_{ij} approximates 1 (i.e., the most trustworthy) or 0 (i.e., the most untrustworthy), the watchdog node υ_i can use a smaller watchdog frequency to monitor target node υ_j since υ_j's behaviors are more deterministic. But if trustworthiness $T_{ij} = 0.5$, υ_j's behaviors are particularly uncertain and υ_i should spend more watchdog tasks to monitor it.

We therefore propose a *heuristic watchdog frequency adjustment* algorithm (*HWFA* algorithm for short) to adaptively adjust watchdog frequency by referencing trustworthiness. HWFA algorithm runs in two phases. The first is an initial phase where watchdog node υ_i performs $f_{ij} = f_j$ (the theoretical result given by Theorem 2) watchdog tasks to establish an initial trustworthiness $T_{ij} = \frac{f_j - fa_j}{f_j}$ for target node υ_j. Then enter the second phase where υ_i performs $f_{ij} = (1 - \frac{|T_{ij} - 0.5|}{0.5}(1 - \mu)) \cdot f_j$ watchdog tasks and updates T_{ij} using Eq. (6). The second phase will be repeated till the end. We use $1 - \frac{|T_{ij} - 0.5|}{0.5}(1 - \mu)$ here to update f_{ij} because $(1 - \frac{|T_{ij} - 0.5|}{0.5})$ can well transform trustworthiness to behavior uncertainty, and $\mu \in (0, 1]$ is a value for maintaining some watchdog task redundancy to resist the unreliable and noisy transmission nature (see the last paragraph in Section IV-C1). Moreover, μ is also effective in thwarting on-off attacks where the adversary could behave normally for a long time to cause $T_{ij} = 1$ and launch attacks suddenly, because it can avoid the f_{ij} from being

Algorithm 2 Heuristic Watchdog Frequency Adjustment (HWFA) Algorithm

```
Input: $\mu$, $f_j$, $N$
Output: N/A
1: $f_{ij} \leftarrow f_j$
2: while watchdog tasks are not stopped do
3:     $v_i$ performs $f_{ij}$ watchdog tasks to monitor $v_j$ in the next time window $N$
4:     $v_i$ updates $v_j$'s trustworthiness $T_{ij}$
5:     $f_{ij} \leftarrow (1 - \frac{|T_{ij}-0.5|}{0.5}(1-\mu)) \cdot f_j$
6: end while
```

reduced to 0 when $T_{ij} = 1$ or $T_{ij} = 0$. A larger μ leads to a better capability against noisy transmission nature and on-off attacks, but may consume more energy. We prove why $f_{ij} = (1 - \frac{|T_{ij}-0.5|}{0.5}(1-\mu)) \cdot f_j$ can achieve our design goals as follows.

Proof: In the HWFA algorithm, we have two design goals: one is that the watchdog frequency f_{ij} should increase when T_{ij} grows up from 0 to 0.5 but decrease when T_{ij} climbs from 0.5 to 1, and the other is that the smallest f_{ij} should not be 0. The first design goal is to ensure that the watchdog frequency is high if the target node is uncertain but low if the target is determined. The second design goal is to guarantee that the watchdog node never disables the monitoring to the target node at any time. To fulfill the first design goal, we can use $f_{ij} = (1 - \frac{|T_{ij}-0.5|}{0.5}) \cdot f_j$ which ensures that f_{ij} can grow up when $T_{ij} < 0.5$ increases but decrease when $T_{ij} > 0.5$ increases. However, this calculation cannot meet the second design goal, as $f_{ij} = 0$ when $T_{ij} = 0$ or $T_{ij} = 1$. To tackle this issue, we need to multiply a factor $(1 - \mu)$ with $\frac{|T_{ij}-0.5|}{0.5}$ and hence convert the function to $f_{ij} = (1 - \frac{|T_{ij}-0.5|}{0.5}(1-\mu)) \cdot f_j$. By this way, f_{ij} can still increase when $T_{ij} < 0.5$ increases and decrease when $T_{ij} > 0.5$ increases, but f_{ij} will never drop to 0 when $T_{ij} = 0$ and $T_{ij} = 1$. Instead, $f_{ij} = \mu \cdot f_j$ is the smallest watchdog frequency. Both of the two design goals are achieved. □

Algorithm 2 lists the details of HWFA algorithm which will be ran by each watchdog node $v_i \in B_j$ given the target node $v_j \in V$. v_i will use Eq. (6) to update v_j's trustworthiness T_{ij} in line 4. We also propose a *HWFAE* algorithm to extend HWFA algorithm from one watchdog node v_i to a group of watchdog nodes W_j. HWFAE algorithm enables $\forall v_i \in W_j$ to run HWFA algorithm independently and simultaneously, hence maintaining trust robustness in the presence of discrimination attacks and bad-mouthing attacks.

Careful readers may notice that the HWFA(E) algorithms can only determine how many watchdog tasks (i.e., f_{ij}) are required within each N and do not discuss how to distribute those tasks to each discrete time slot $t \in N$. That is, the HWFA(E) algorithms only output $f_{ij} = \sum_{t \in N \wedge w_{ij}^t \neq \varnothing} 1$ but do not specify which $w_{ij}^t \neq \varnothing$ and which $w_{ij}^t = \varnothing$. Smart attackers may exploit this ignorance to evade the protection provided by our HWFA(E) algorithms. We will discuss this problem and propose potential solutions in Section VI.

TABLE II
WSN TOPOLOGY FOR WSNET SIMULATION

Case	Space size	Range r_j	# of node $\|\|V\|\|$	mean of $\|\|B_j\|\|$
①	100m*100m	20m	100	10.66
②	100m*100m	20m	200	21.49

TABLE III
MODEL SETTING FOR WSNET SIMULATION

Energy model	$L = 640$bits	$\varepsilon^{elec} = 50$nJ/bit	$\epsilon = 10$pJ/bit/m^2
Attack model	Bad-mouthing attack $\alpha = 0.5$	Sybil attack $\alpha = 0.01$	Other attacks $\alpha = 0.5$
Other setting	$N = 500$ms	Rounds of N: 20	$f_j = 100$

V. EVALUATION

In this section, we evaluate our watchdog optimization algorithms using a popular WSNET simulation platform in Section V-A, as well as an in-door WSN testbed in Section V-B.

A. WSNET Simulation

WSNET [26] is an event-driven module-based WSN simulation framework. It applies a loosely-organized architecture to modularize sensor node's key functionalities into a sequence of plugable models (e.g., the radio, MAC, routing protocol stack, battery and applications etc.). Due to this flexible design and excellent emulating performance [32], WSNET has drawn widely attention in the literature [33]–[35].

In our experiments, we implement watchdog optimization algorithms (i.e., DBP algorithm and HFWA(E) algorithm) as a new application module to WSNET, and apply our energy consumption model (described in Section III-B) by modifying the existing `linear` battery module. We choose `half1d` as the radio module and `idealmac` for the MAC layer. We set WSN's transmission error rate (due to noise) to 1%. We limit the routing distance to 1 hop since the watchdog mechanism only cares about neighborhood behaviors. We present the details of two WSN topologies used by our simulation in Table II, where the topology ② is more dense than topology ①. Sensor nodes are randomly deployed to these two topologies. Moreover, the true trustworthiness (draw from the node's internal behavior distribution $\mathbf{P}_j, \forall v_j \in V$) assigned to the j-th sensor node is $(j-1)/||V||$.

We also give our simulation model settings in Table III. We choose energy model parameters the same as those used by prior research [24]. We will explain our choice for the α value when we elaborate on Figure 5 and 6. $N = 500$ milliseconds and $f_j = 100$ indicate that the sensor nodes will renew their behaviors in every $N/f_j = 5$ milliseconds. For example, the nodes sense the temperature in every 5 ms.

We show our simulation results through Figure 2 to 6. We measure security in terms of trust accuracy or robustness, while show energy saving using the following equation.

$$Energy\ saving = \frac{cost(Baseline) - cost(WO)}{cost(Baseline)}, \quad (13)$$

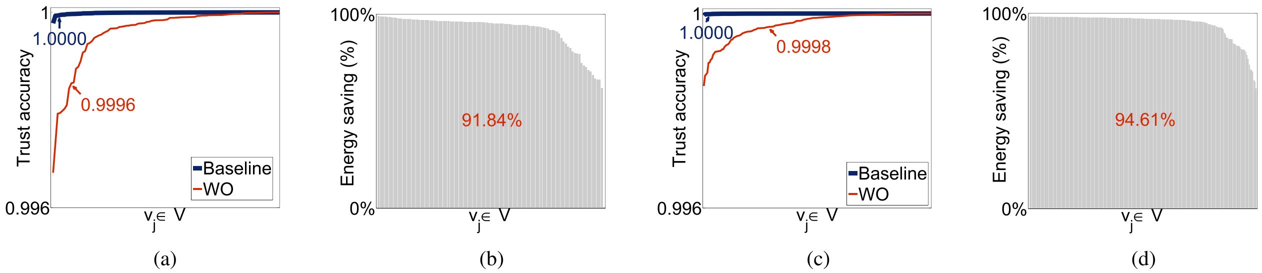


Fig. 2. Evaluation results for **WSN attacks**. WO refers our watchdog optimization (i.e., DBP with $||W_j|| = \pi_j \cdot ||B_j|| = 1$ and HWFA with $\mu = 0.2$). Baseline is for non-optimized watchdog methods implicitly used by [4], [6], and [23] with monitoring frequency $f_{ij} = f_j$. The value attached to each curve or bar chart is the mean value of that figure. (a) Trust accuracy, topology ①. (b) Energy saving, topology ①. (c) Trust accuracy, topology ②. (d) Energy saving, topology ②.

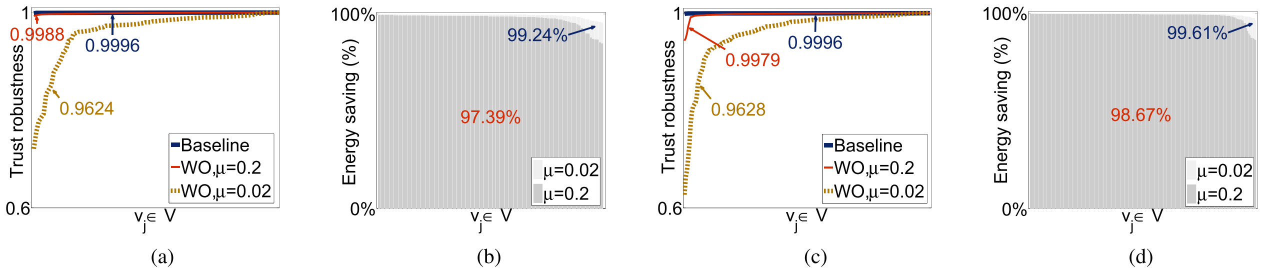


Fig. 3. Evaluation results for **on-off attacks**. WO refers to our watchdog optimization (i.e., DBP with $||W_j|| = \pi_j \cdot ||B_j|| = 1$ and HWFA). Baseline is for non-optimized watchdog methods with monitoring frequency $f_{ij} = f_j$. The value attached to each curve or bar chart is the mean value of that figure. (a) Trust robustness, topology ①. (b) Energy saving, topology ①. (c) Trust robustness, topology ②. (d) Energy saving, topology ②.

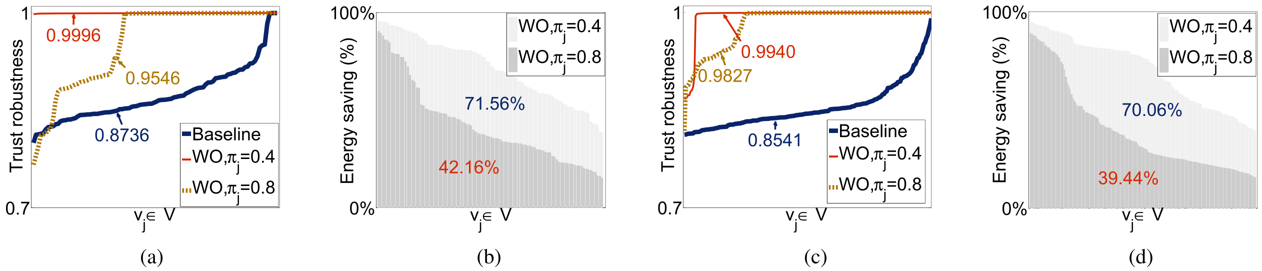


Fig. 4. Evaluation results for **discrimination attacks**. WO refers to our watchdog optimization (i.e., DBP and HWFAE with $\mu = 0.2$). Baseline is for non-optimized watchdog methods with monitoring frequency $f_{ij} = f_j$. The value attached to each curve or bar chart is the mean value of that figure. (a) Trust robustness, topology ①. (b) Energy saving, topology ①. (c) Trust robustness, topology ②. (d) Energy saving, topology ②.

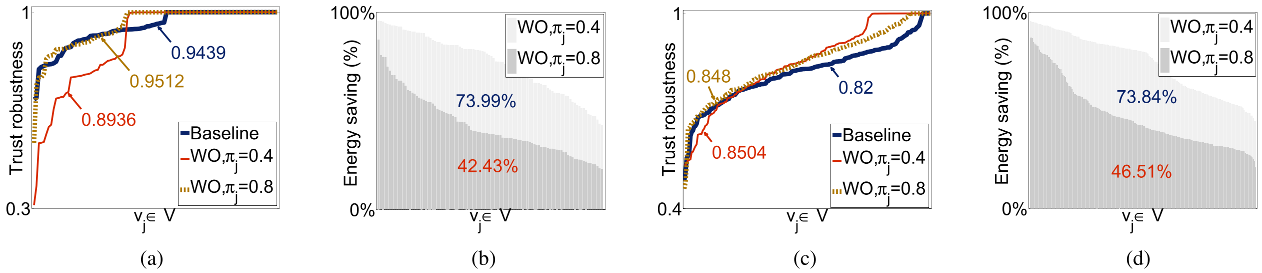


Fig. 5. Evaluation results for **bad-mouthing attacks**. WO refers to our watchdog optimization (i.e., DBP and HWFAE with $\mu = 0.2$). Baseline is for non-optimized watchdog methods with monitoring frequency $f_{ij} = f_j$. The value attached to each curve or bar chart is the mean value of that figure. (a) Trust robustness, topology ①. (b) Energy saving, topology ①. (c) Trust robustness, topology ②. (d) Energy saving, topology ②.

where, $cost()$ function returns the energy consumed by each sensor node during the simulation when our watchdog optimization algorithms (WO for short) are applied or a baseline algorithm (i.e., non-optimized watchdog method) is used. We choose the baseline algorithm in this paper as the neighbour-flooding watchdog method. This method is (implicitly) used by typical trust systems such as [4], [6], and [23] and represents the state-of-the-art watchdog technique. In each figure, the values attached to the curves or bar charts represent the average trust accuracy (robustness) or energy saving over

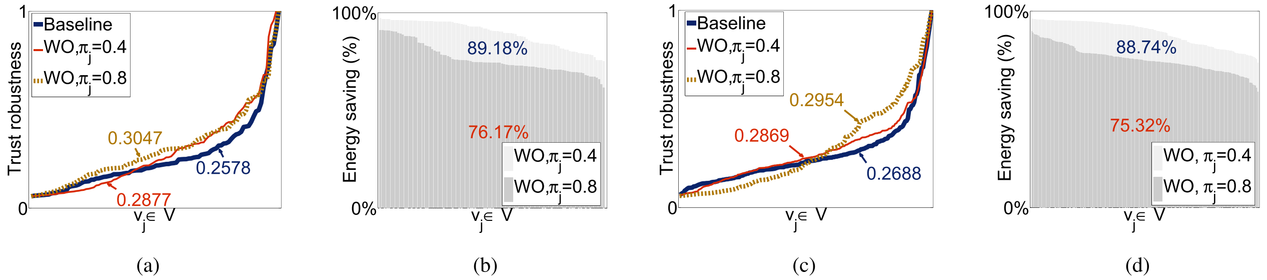


Fig. 6. Evaluation results for **sybil attacks**. WO refers to our watchdog optimization (i.e., DBP and HWFAE with $\mu = 0.2$). Baseline is for non-optimized watchdog methods with monitoring frequency $f_{ij} = f_j$. The value attached to each curve or bar chart is the mean value of that figure. (a) Trust robustness, topology ①. (b) Energy saving, topology ①. (c) Trust robustness, topology ②. (d) Energy saving, topology ②.

all the sensor nodes in V. In another word, those values are the mean values of Eq. (10) and Eq. (11) for a given WSN, hence being able to demonstrate the security and energy saving results achieved by our watchdog optimization algorithms and the baseline algorithm in the WSN.

Figure 2 shows the results in the presence of WSN attacks. In this attacking scenario, sensor nodes may only behave to disrupt WSN's functionalities such as reporting false sensed data or selectively dropping packets. They will not attempt to attack WSNTS itself. As a result, we can set $||W_j|| = \pi_j \cdot ||B_j|| = 1$ for DBP algorithm, since sensor nodes' behaviors observed by different neighbor nodes are the same. We also consider $\alpha = 0.5$ to calculate the optimal watchdog location for DBP algorithm. We choose $\mu = 0.2$ for HWFA algorithm to maintain some capability against WSN's noisy transmission nature. As can be seen in Figures 2(a)-2(b), our watchdog optimization algorithms can save 91.84% (or 94.61%) energy in average by sacrificing $1-0.9996 = 0.0004$ (or $1-0.9998 = 0.0002$) trust accuracy for topology ① (or topology ②).

Figure 3 shows the results in face of on-off attacks. Although this attack falls into the WSNTS attacking category, the on-off attacking nodes still do not behave differently to different neighbor nodes. Instead, they may only behave as normal for a long period of time and launch WSN attacks to all the neighbourhood suddenly. Therefore, we also choose $||W_j|| = \pi_j \cdot ||B_j|| = 1$ for DBP algorithm. But for HWFA algorithm, we test $\mu = 0.2$ and $\mu = 0.02$ respectively. In our experiments, we let on-off attackers perform normal behaviors for the first 18 rounds of N and then launch attacks in the last 2 rounds of N. The results show that, even the use of $\mu = 0.02$ can further slightly increase the energy saving in $99.24\% - 97.39\% = 1.85\%$ for topology ① (see Figure 3(b)) and $99.61\% - 98.67\% = 0.94\%$ for topology ② (see Figure 3(d)), the trust robustness can be decreased more than 0.03 ($0.9988 - 0.9624 = 0.0364$ in Figure 3(a) and $0.9979 - 0.9628 = 0.0351$ in Figure 3(c)). As a result, we suggest the use of $\mu = 0.2$ if WSN users prefer to keep WSNTS more robust.

Figure 4 shows the results under discrimination attacks. This attacking scenario considers that sensor nodes may behave differently to their neighborhood. In our experiment, we consider that the target node will always launch WSN attacks to the nearest 20% neighbor nodes but behave normally to others. In this experiment, we are surprisingly finding that our watchdog optimization algorithms can save energy and enhance security (i.e., increase trust robustness) simultaneously. In particular, watchdog optimization can save at least 39.44% energy (the smallest energy saving is found at topology ② in Figure 4(d)) and meanwhile increase trust robustness up to $0.994 - 0.8541 = 0.1399$ (the largest trust robustness increment is found at topology ② in Figure 4(c)). We can get this double-win results since our DBP algorithm can intelligently select a subset of neighbor nodes as watchdogs and thus get the chance to evade the discriminated neighbors. However, the baseline algorithm naively chooses the entire neighborhood to do watchdog tasks and can be necessarily disrupted by discriminated neighbor nodes.

Figure 5 and Figure 6 show the results for bad-mouthing and sybil attacks respectively. To launch bad-mouthing attacks, some watchdog nodes are malicious and can decrease benign node's reputation by continuously reporting bad behavior observations of that node to others. In this paper, we model sybil attack as a special case of bad-mouthing attacks when the majority of sensor node's neighborhood is malicious. In particular, we use different α to differentiate these two attacks. We set $\alpha = 0.01$ for sybil attack to let $Pr[v_i \in A | v_j \in A]$ decrease from 100% to 83.3% when d_{ij} increases from 0 to 20 meters. While in bad-mouthing attack, we set $\alpha = 0.5$ to let only the minority of the neighborhood be compromised. $\alpha = 0.5$ can decrease $Pr[v_i \in A | v_j \in A]$ from 100% to 9.1% when d_{ij} increases from 0 to 20. As shown in Figure 5, watchdog optimization can save at least 42.43% energy (the least saving is found at topology ① in Figure 5(b)) with the cost of no more than $0.9439 - 0.8936 = 0.0503$ trust robustness (the largest trust robustness reduction is also found at topology ① in Figure 5(a)) for bad-mouthing attack. For sybil attack, our watchdog optimization algorithms can get a slightly higher trust robustness than the baseline algorithm (see Figures 6(a) and 6(c)), and can save more than 75.32% energy (the smallest energy saving is found at topology ② in Figure 6(d)).

B. In-Door Testbed Experiments

In addition to WSNET simulation, we also investigate watchdog optimization in real-world settings. In particular, we deploy an WSN testbed in our collaborative lab and evaluate our algorithms on top of it. As shown in the left part

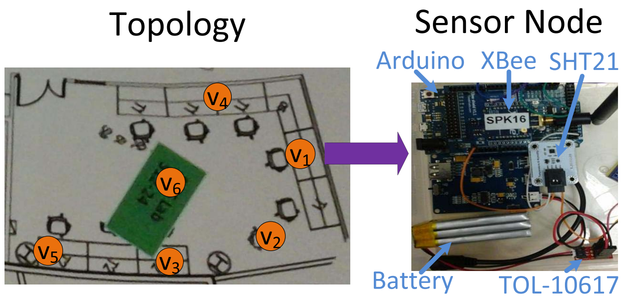


Fig. 7. In-door WSN testbed layout.

TABLE IV
EXPERIMENTAL RESULTS FOR IN-DOOR TESTBED

	Energy saving	Trust accuracy/robustness	
		Baseline	Watchdog optimization
WSN attack	87.00%	0.9997	0.9991
On-off attack	93.68%	0.9998	0.9998
Discrimination attack	74.83%	0.8585	0.9989
Bad-mouthing attack	77.62%	0.8829	0.8663
Sybil attack	72.96%	0.3613	0.3437

of Figure 7, the testbed consists of six sensor nodes in an around 5 × 10 m^2 in-door space and these nodes are within each other's neighborhood (i.e., $v_i \in B_j$, $\forall i, j \in [1, 6], i \neq j$). Each sensor node is built on an *Arduino Due* board, and consists of a *XBee-Pro RF Module* for radio transimission/receiving, a *SHT*21 *Digital Sensor Module* for humidity and temperature sensing, as well as a *TOL*-10617 *LiPo Fuel Gauge* for measuring residual energy left in the battery. We connect the SHT21 module and TOL-10617 gauge to the Arduino board using I^{2}C bus. The right part of Figure 7 shows an image of our sensor node.

To apply the DBP algorithm to this real-world setting, we need to estimate ϵ of XBee-Pro RF Module for calculating the optimal location $(4L\epsilon\alpha)^{-\frac{1}{3}}$. According to [36], this module has 250kbps maximum data transmission rate and 60mW output power. Although it claims that the largest transmission distance is up to 1500 meters, our out-door experiments confirm the valid distance is only 100 meters. As a result, we can estimate ϵ as $\epsilon = \frac{60 \cdot 10^{-3}}{250 \cdot 10^3 \cdot 100^2} = 24$ pJ/bit/m^2. In this real-world experiments, we also choose $L = 640$ bits (i.e., 80 bytes) and the same α as those in Table III for different attacks. In DBP algorithm, we use $||W_j|| = \pi_j \cdot ||B_j|| = 1$ for WSN attack and on-off attack, and $\pi_j = 0.4$ for other attacks. In HWFA(E) algorithms, we choose $\mu = 0.2$.

Table IV shows the mean values of trust accuracy/robustness and energy saving over the six nodes in our in-door testbed experiments. As can be seen, we can save up to 93.68% energy in this real-world scenario, and meanwhile induce trust accuracy/robustness reduction no more than $0.3613 - 0.3437 = 0.0176$. To sum up, our in-door testbed experimental results have the similar trend as those in WSNET simulation, hence proving the perfect adaptability of our watchdog optimization algorithms in real-world settings.

Compared with the watchdog techniques without any optimization, our algorithms can save such a large amount of energy mainly due to two reasons. The first is that we do not need to use the entire set of neighbor nodes (i.e., the set B_j given a target node v_j) to perform watchdog tasks. Instead, our DBP algorithm enables the selection of $\pi_j \cdot ||B_j||$ nodes as watchdog nodes. For example, if we choose $\pi_j = 0.4$, we can save at least 60% energy by DBP in theory. Moreover, our HWFA(E) algorithm can further reduce the energy cost by using a low frequency to monitor determined target nodes. The more target nodes with a high level trustworthiness or untrustworthiness, the more energy we can save. With these two benefits, we eventually achieve such a good result in our experiments.

VI. Discussion and Future Works

Although our watchdog optimization algorithms have demonstrated excellent performance in saving energy and maintaining security (see Section V), they are still subject to some challenges, which may need further investigation in the future.

The first challenge is to allocate watchdog tasks for each time window N. As described in the last paragraph in Section IV-C2, this is a major concern the HWFA(E) algorithms cannot address. Actually, a watchdog node v_i can simply distribute the f_{ij} watchdog tasks over the time window N using uniform distribution or some other patterns. However, such kind of deterministic allocation method can be easily recognized by smart attackers. These attackers can have the chance to predict watchdog nodes' future behaviors and then intelligently launch their attacks in the time slots where no watchdog tasks happen (like launching on-off attacks within a time window N). To mitigate this issue, our HWFA(E) algorithms should distribute watchdog tasks for each N in an unpredictable manner. That is, for different time window N, watchdog tasks are distributed in a very different pattern hence getting a higher probability to catch smart attacking behaviors. In our experiments in Section V, we just randomly assign attacking behaviors and watchdog tasks for each N, which implicitly follows this design requirement.

The second one is to estimate the attacking model's parameter α (required by Eq. 5). In our experiments, we simply consider $\alpha = 0.01$ for sybil attack while $\alpha = 0.5$ for other attacks. But in real scenarios, WSN designers cannot have the direct knowledge of α. Since α is a necessary parameter for DBP algorithm (i.e., the optimal location is $(4L\epsilon\alpha)^{-\frac{1}{3}}$), WSN designers are forced to estimate this parameter in real scenarios. To overcome this challenge, a potential solution is to infer α based on historical WSN attacking data collected from other mature WSNTS. Since different WSNTSs are likely heterogeneous, we acknowledge that this solution is not trivial to implement and its effectiveness requires further investigation. We leave this work in our future research.

The third challenge is the load balance problem. As can be seen in Figures 2-6, although our watchdog optimization algorithms can save significant amount of energy, it cannot balance the watchdog tasks across sensor nodes (i.e., some sensor nodes can save more than two times of energy than others). This will cause some of nodes to exhaust their energy before others. Some portion of WSN terminated in a great advance before some other parts is not expected, since every sensor node is deployed with unique purpose and is expected to work till the end of the whole WSN. As a result, we will seek an appropriate load balance algorithm to improve current methods in our future research.

The last one is to adapt our watchdog optimization techniques to mobile WSNs. In our current design, we simply assume a static WSN topology where each sensor node's neighborhood is fixed. However, in mobile WSNs, sensor nodes can move from time to time and thus make their optimal watchdog positions continuously changing. This dynamic issue could make our DBP algorithm very difficult to work at run time, because the watchdog nodes should be reselected upon any movement of the target node. As a result, we should redesign DBP algorithm if we attempt to apply watchdog optimization to mobile WSNs. We leave it as our future work.

In the future, we will continue the work and apply our watchdog optimization to other networking systems which face the similar trust-energy conflict like WSNs, such as the vehicle ad hoc networks [37] and the anonymity networks [38], [39].

VII. Conclusion

In this paper, we take the first step to answer an important research question on whether WSNTS can still maintain sufficient security when the trust's basic foundations (i.e., the first-hand experiences) are minimized. We give out a very positive result to this question through theoretical analysis and extensive experiments. Our studies thus shed light a promising research direction on the design of energy-efficient WSNTS by optimizing the collection procedure of first-hand experiences.

Acknowledgment

The authors would like to thank Prof. T. Charles Clancy and the anonymous reviewers for their careful review and helpful comments in this paper.

References

[1] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Commun. ACM*, vol. 47, no. 6, pp. 53–57, 2004.

[2] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1086–1090, Mar. 2009.

[3] Y. Zhou, Y. Zhang, and Y. Fang, "Access control in wireless sensor networks," *Ad Hoc Netw.*, vol. 5, no. 1, pp. 3–13, 2007.

[4] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. 6th Annu. Int. Conf. Mobile Comput. Netw.*, 2000, pp. 255–265.

[5] E. Shi and A. Perrig, "Designing secure sensor networks," *IEEE Wireless Commun.*, vol. 11, no. 6, pp. 38–43, Dec. 2004.

[6] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Trans. Sensor Netw.*, vol. 4, no. 3, 2008, Art. ID 15.

[7] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, S. Lee, and Y.-J. Song, "Group-based trust management scheme for clustered wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 11, pp. 1698–1712, Nov. 2009.

[8] G. Zhan, W. Shi, and J. Deng, "Design and implementation of TARF: A trust-aware routing framework for WSNs," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 2, pp. 184–197, Mar./Apr. 2012.

[9] S. Zheng and J. S. Baras, "Trust-assisted anomaly detection and localization in wireless sensor networks," in *Proc. 8th Annu. IEEE Commun. Soc. Conf. Sensor, Mesh, Ad Hoc Commun., Netw. (SECON)*, Jun. 2011, pp. 386–394.

[10] Y. Ren, V. I. Zadorozhny, V. A. Oleshchuk, and F. Y. Li, "A novel approach to trust management in unattended wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 13, no. 7, pp. 1409–1423, Jul. 2014.

[11] X. Li, F. Zhou, and J. Du, "LDTS: A lightweight and dependable trust system for clustered wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 6, pp. 924–935, Jun. 2013.

[12] D. Wang, T. Muller, Y. Liu, and J. Zhang, "Towards robust and effective trust management for security: A survey," in *Proc. 13th IEEE Int. Conf. Trust, Secur., Privacy Comput. Commun. (TrustCom)*, 2014.

[13] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A survey of trust and reputation management systems in wireless communications," *Proc. IEEE*, vol. 98, no. 10, pp. 1755–1772, Oct. 2010.

[14] J. Lopez, R. Roman, I. Agudo, and C. Fernandez-Gago, "Trust management systems for wireless sensor networks: Best practices," *Comput. Commun.*, vol. 33, no. 9, pp. 1086–1093, 2010.

[15] F. G. Nakamura, F. P. Quintão, G. C. Menezes, and G. R. Mateus, "An optimal node scheduling for flat wireless sensor networks," in *Proc. 4th Int. Conf. Netw.*, 2005, pp. 475–482.

[16] A. Salhieh, J. Weinmann, M. Kochhal, and L. Schwiebert, "Power efficient topologies for wireless sensor networks," in *Proc. Int. Conf. Parallel Process.*, Sep. 2001, pp. 156–163.

[17] J.-H. Cho, A. Swami, and R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Commun. Surv. Tuts.*, vol. 13, no. 4, pp. 562–583, Oct./Dec. 2011.

[18] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," *J. Netw. Comput. Appl.*, vol. 35, no. 3, pp. 867–880, 2012.

[19] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: A survey," *IEEE Commun. Surv. Tuts.*, vol. 11, no. 2, pp. 52–73, Apr./Jun. 2009.

[20] S. Tanachaiwiwat, P. Dave, R. Bhindwale, and A. Helmy, "Location-centric isolation of misbehavior and trust routing in energy-constrained sensor networks," in *Proc. IEEE Int. Conf. Perform., Comput., Commun.*, 2004, pp. 463–469.

[21] R. Yan, H. Sun, and Y. Qian, "Energy-aware sensor node design with its application in wireless sensor networks," *IEEE Trans. Instrum. Meas.*, vol. 62, no. 5, pp. 1183–1191, May 2013.

[22] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: Security protocols for sensor networks," *Wireless Netw.*, vol. 8, no. 5, pp. 521–534, 2002.

[23] P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Proc. IFIP TC6/TC11 6th Joint Working Conf. Commun. Multimedia Secur., Adv. Commun. Multimedia Secur.*, 2002, pp. 107–121.

[24] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Trans. Wireless Commun.*, vol. 1, no. 4, pp. 660–670, Oct. 2002.

[25] R. Di Pietro, G. Oligeri, C. Soriente, and G. Tsudik, "United we stand: Intrusion resilience in mobile unattended WSNs," *IEEE Trans. Mobile Comput.*, vol. 12, no. 7, pp. 1456–1468, Jul. 2013.

[26] G. Chelius, A. Fraboulet, and E. B. Hamida. (2009). *WSNet: An Event-Driven Simulator for Large Scale Wireless Sensor Networks*. [Online]. Available: http://wsnet.gforge.inria.fr/

[27] F. Bao, I. R. Chen, M. Chang, and J.-H. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," *IEEE Trans. Netw. Service Manage.*, vol. 9, no. 2, pp. 169–183, Jun. 2012.

[28] J. Duan, D. Yang, H. Zhu, S. Zhang, and J. Zhao, "TSRF: A trust-aware secure routing framework in wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 2014, Jan. 2014, Art. ID 209436.

[29] R. K. Tripathi, Y. N. Singh, and N. K. Verma, "Two-tiered wireless sensor networks—Base station optimal positioning case study," *IET Wireless Sensor Syst.*, vol. 2, no. 4, pp. 351–360, Dec. 2012.

[30] S. Kullback, *Information Theory and Statistics*. New York, NY, USA: Dover, 2012.

[31] A. J. Jerri, "The Shannon sampling theorem—Its various extensions and applications: A tutorial review," *Proc. IEEE*, vol. 65, no. 11, pp. 1565–1596, Nov. 1977.

[32] A. Fraboulet, G. Chelius, and E. Fleury, "Worldsens: Development and prototyping tools for application specific wireless sensors networks," in *Proc. 6th Int. Symp. Inf. Process. Sensor Netw.*, Apr. 2007, pp. 176–185.

[33] J. Tate, B. Woolford-Lim, I. Bate, and X. Yao, "Evolutionary and principled search strategies for sensornet protocol optimization," *IEEE Trans. Syst., Man, Cybern. B, Cybern.*, vol. 42, no. 1, pp. 163–180, Feb. 2012.

[34] A. Ziviani, T. B. Cardozo, and A. T. A. Gomes, "Rapid prototyping of active measurement tools," *Comput. Netw.*, vol. 56, no. 2, pp. 870–883, Feb. 2012.

[35] B. Pavkovic, A. Duda, W.-J. Hwang, and F. Theoleyre, "Efficient topology construction for RPL over IEEE 802.15.4 in wireless sensor networks," *Ad Hoc Netw.*, vol. 15, pp. 25–38, Apr. 2014.

[36] (2014). *XBee Pro 60 mW Wire Antenna*. [Online]. Available: https://www.sparkfun.com/products/8742

[37] J. Zhang, "A survey on trust management for VANETs," in *Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, Mar. 2011, pp. 105–112.

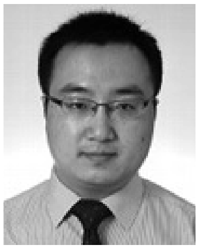
[38] P. Zhou, X. Luo, A. Chen, and R. K. C. Chang, "SGor: Trust graph based onion routing," *Comput. Netw.*, vol. 57, no. 17, pp. 3522–3544, 2013.

[39] P. Zhou, X. Luo, and R. K. C. Chang, "Inference attacks against trust-based onion routing: Trust degree to the rescue," *Comput. Secur.*, vol. 39, pp. 431–446, Nov. 2013.

Peng Zhou is currently a Lecturer with the Shanghai Key Laboratory of Power Station Automation Technology, School of Mechatronic Engineering and Automation, Shanghai University, Shanghai, China. He was a Research Fellow with the School of Computer Engineering, Nanyang Technological University, Singapore. He received the Ph.D. degree with the Department of Computing, Hong Kong Polytechnic University, Hong Kong, in 2014. His research includes network security, cyber-physical system security, and trust management for wireless sensor networks.

Siwei Jiang is currently a Research Fellow with the Singapore Institute of Manufacturing Technology, Singapore. He received the M.S. and Ph.D. degrees in computer science from the China University of Geosciences, Wuhan, China, in 2006 and 2011, respectively, and the Ph.D. degree from the School of Computer Engineering, Nanyang Technological University, Singapore, in 2014. His research interests include multiagent evolutionary algorithms, reputation systems, wireless sensor network, and vehicle routing.

Athirai Irissappane is currently pursuing the Ph.D. degree with Nanyang Technological University, Singapore. She received the master's degree in software engineering from the National University of Singapore, Singapore. Her research interests are artificial intelligence, multiagent systems, trust and reputation modeling, and fraud detection.



Jie Zhang is currently an Assistant Professor with the School of Computer Engineering, Nanyang Technological University, Singapore. He is an Academic Fellow with the Institute of Asian Consumer Insight, Singapore, and an Associate Fellow with the Singapore Institute of Manufacturing Technology, Singapore. He received the Ph.D. degree from the Cheriton School of Computer Science, University of Waterloo, Waterloo, ON, Canada, in 2009. During his Ph.D. studies, he held the prestigious NSERC Alexander Graham Bell Canada Graduate Scholarship rewarded for top Ph.D. students across Canada. He was also the recipient of the Alumni Gold Medal at the 2009 Convocation Ceremony. His papers have been published by top journals and conferences and received several best paper awards. He is also active in serving research communities.

Jianying Zhou is currently the Head of the Department of Infocomm Security with the Institute for Infocomm Research, Singapore. He received the Ph.D. degree in information security from Royal Holloway, University of London, Egham, U.K. His research interests are in applied cryptography, computer and network security, cyber-physical security, and mobile and wireless security. He received a large amount of R&D funding from the Singapore government and published intensively at international conferences and journals. He is also a cofounder of the International Conference on Applied Cryptography and Network Security. He served as the General Chair, the Program Chair, and a program committee member in many international cryptography and security conferences.

Joseph Chee Ming Teo received the Ph.D. degree in wireless network security from Nanyang Technological University, Singapore, under the Agency for Science, Technology and Research Graduate Scholarship. He was a Research Engineer/ Scientist I with the Institute for Infocomm Research, Singapore. He has been working on authentication and group key management in various types of wireless networks, such as wireless sensor networks, wireless mesh networks, vehicular networks, and mobile ad hoc networks, since 2004. His research areas include secure wireless communications, authentication, key exchange, vehicular networks, wireless sensor networks, and secure group communications.