SECURE AND EFFICIENT WATCHDOG OPTIMIZATION FOR CLUSTER-BASED WIRELESS SENSOR NETWORKS

Kalaiselvi M., V. Parthasarathy,

Department of Computer Science and Engineering, Veltech Multitech Engineering College, Avadi, Chennai, India. kalaiselvi693@gmail.com, sarathy.vp@gmail.com

ABSTRACT

Watchdogs are an effective mechanism to detect selfish and malicious attacks from computer networks. In networks, such as MANETs, attack analysis and detection is a more importantfor the whole network. Watchdog systems detect the misbehavior and that neighbor node by using data collection and analysis, so accuracy, less delay and effectiveness are achieving much more security and performance in wireless sensor networks.In previous process watchdog has inefficient trust system for security in the network.In this paper, we propose a watchdog technique for improving the trust system in networks by using effective optimization methods. To expose this method,:we can achieve better efficiency compare to existing and minimum energy cost for using watchdog technique and also keeping sufficient level security. In our contributions of the proposed method, it consists of theoretical analyses and practical algorithms. Using this watchdog approach the detection of misbehaved nodes is reduced, sufficient security, less energy consumption and the overall accuracy increased.

Index Terms: Clustering techniques, AODV, WSNET, WatchDog

I. INTRODUCTION

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today, such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. In order to achieve an appropriate level of security in WSNs we cannot depend on cryptographic techniques as these techniques fall prey to insider attacks. So, to counter this threat some additional measures need to be taken such as an intrusion detection system. The intrusion detection system tries to detect any kind of intrusions made into the system hornet work and gives an alert for the malicious event occurred. There are three basic approaches in intrusion detection system according to the used detection techniques which can be classified as, Misuse Detection, Anomaly Detection and Specification Based Detection. First approach (Misuse Detection) compares the observed behavior of the nodes with known attack patterns i.e. signature based. It can measure instances of attacks accurately and effectively, but it lacks the ability to detect any unknown attack. Anomaly detection is based on monitoring the changes in the behavior of nodes rather than searching for some known attack signatures. The main disadvantage of this system is the high false positive rates of the nodes being identified. The third approach is similar to anomaly detection, but the normal behavior is specified manually as a system of constraints. We will fill in this gap by optimizing watchdog techniques for WSN's trust systems (WSNTS for short). WSNTSs to balance energy efficiency and security (in terms of trust accuracy and robustness). Our 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, these nodes are more likely of being compromised together and launch collaborative attacks. 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.

II. 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, or secure multi-hop routing or protect both of them. Many of those WSNTSs, 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 trustevaluation through watchdogs. For example, 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. 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, 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 implemented an energy watcher 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 clusteringtechnology is widely used by the literature 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, 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 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 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 proposes an energy-efficient, securerouting algorithm to choose efficient and trustworthy nexthop node in a route, it cannot reduce the energy used to build up WSNTS, which is the major problem to be solved. Third, unlike the clustering techniques 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, designs an energy-efficient WSNTS by reducing unnecessary communications of trust recommendations (a.k.a. Secondhand 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, 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.

III. PROPOSED SYSTEM

We propose a watchdog technique for improving the trust system in networks by using effective optimization methods. To expose this method, we can achieve better efficiency compare to existing and minimum energy cost for using watchdog technique and keeping sufficient level security. In our contributions of the proposed method, it consists of theoretical analyses and practical algorithms. Using this watchdog approach the detection of misbehaved nodes is reduced, sufficient security, less energy consumption and the overall accuracy increased.

Our project is mainly concerned in detecting the selfish Node effectively in the network Detecting the selfish nodes is mainly done using watchdog and here we are going to increase the effectiveness of detecting the watchdog. We modelled its performance using combined Ad-hoc on- demand Distance Vector Routing (AODV) and WatchDog. A Combined AODV and WatchDog can reduce the overall detection time.

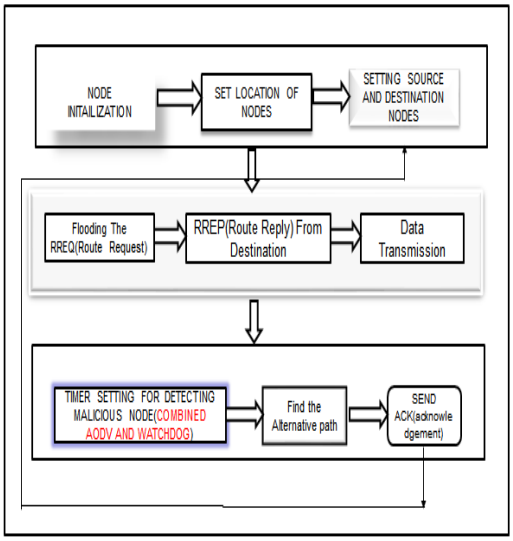

Fig.1 Overview of the proposed method

We conduct a novel study to reveal trust-energy conflict induced by the inefficient use of watchdog techniques in WSNTSs. 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. We evaluate our optimization techniques using extensive experiments in a WSNET simulation platform and an in-door test bed in our collaborative lab. The experimental results have successfully confirmed the effectiveness of our design. 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.

IV. MODULE ANALYSIS

A. Energy Consumption Model

We follow a typical free space, wireless radio model, which is widely adopted by the literature. 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 and to assume that a proper power controller has been deployed to adjust transmit power amplifier according to the transmission distance. 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.

We assume that a proper power controller has been deployed to adjust transmit power amplifier according to the transmission distance. Let ε elect 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 be free space constant measured in J/bit/m2. We then can calculate the energy consumption when vi transmits 1 bit information to its neighbor node v j (dij ≤ ri) as:

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

Meanwhile, the energy consumed by the node *vi* for receiving 1bit information from neighbour node *v j* can be computed as:

$$\varepsilon_{ij}^{RX} = \varepsilon^{elec}. \quad (2)$$

As, to accomplish a watchdog task wt ij , the watchdog node vi should first send query to the target node then receive all the target node's reply, while the target node vj should first receive the query from the watchdog node then send back the reply to the source node.

As a result, if a watchdog task wt ij requires L bits information for either query or response, the energy consumed by the watchdog node vi for this task is:

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

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

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

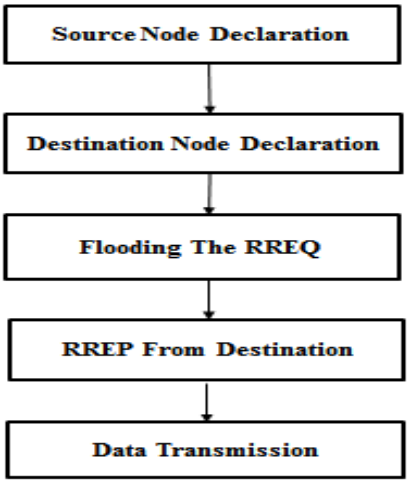

Fig. 2: Proposed model

B. Trust Model

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 the 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 vi '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 vi 's expectation among all the vj's behaviors watched by vi in a time window N. We denote this trustworthiness as Tij. We then define I tij as the event to represent whether v j 'sbehavior is expected by vi at time slot t. I tij returns 1 if v j 's behavior follows vi '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 Tij as:

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

where, w tij = ∅ means the watchdog node vi actually performs watchdog task to monitor v j at time slot t.

2) Trust Accuracy and Trust Robustness: We let I t j be the event to describe a sensor node vj 's internal behavior and draw it according to a binary distribution function P j. I tj = 1 if v j behaves well at time slot t while I t j = 0 if v j performs attacks against WSN at t (e.g., reporting corrupted sensing data or refusing packet forwarding etc.). Watchdog node vi can sample P j to discrete events Iij t s. We then model the accuracy of Tij (i.e., trust accuracy) using the Kullback-Leibler divergence between the probability distribution of I t j s (i.e., P j) and the distribution of Iij t s (denoted as Qij). 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 an excellent choice to measure trust accuracy. Let I be the random variable of distribution P j and Qij. We then can follow to calculate KL divergence as:

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

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

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

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 watch-dog 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:

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

where, W j ⊆ B j is a set of cooperative watchdog nodes, which will monitor vj together, and ‖ ∗ ‖ is the size of set ∗. Since ∀vi ∈ W j , ij ∈ [0, 1], we also have ϒ j ∈ [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.

C. *LOCATION OPTIMIZATION*

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 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 neighbor nodes located at the optimal watchdog location. 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. 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.

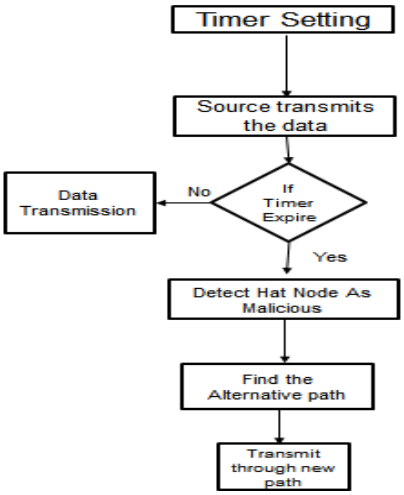

Fig.3 Watchdog Technique

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 vi performs to monitor a target node vj within a time window N as watchdog frequency fij. We have fij = t∈NΛw tij =∅ 1. Also, we define a nodev j 's behavior frequency and attacking frequency within the time window N as f j and f a j respectively. We then have f j = t∈N 1 and f a j = t∈N(1 − I t j). 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 predefined 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.

Algorithm 1 Distance-Based Probabilistic (DBP) Algorithm

Input: π_j, B_j, d_{ij} for $\forall v_i \in B_j$, L, ϵ, α

Output: W_j

1: $W_j \leftarrow \varnothing$

2: **while** $||W_j|| < \pi_j \cdot ||B_j||$ **do**

3: $x \leftarrow random(0, \sum_{k \in B_j} \frac{1}{|d_{kj} - (4L\epsilon\alpha)^{-\frac{1}{3}}|})$

4: **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**

5: $W_j \leftarrow W_j \vee v_i$

6: **end if**

7: **end while**

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 Tij approximates 1 (i.e., the most trustworthy) or 0 (i.e., th emost untrustworthy), the watchdog node vi can use a smaller watchdog fre-

quency to monitor target node v jsince v j 's behaviors are more deterministic. But if trustworthiness Tij = 0.5, v j 's behaviors are particularly uncertain and vi 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 vi performs watchdog tasks to establish an initial trustworthiness.

Then enter the second phase watchdog tasks and updates. The second phase will be repeated till the end. Because can well transform trustworthiness to behavior uncertainty, and μ ∈ (0, 1] is a value for maintaining some watchdog task redundancy to resist the unreliable and noisy transmission nature.

Algorithm 2 Heuristic Watchdog Frequency Adjustment (HWFA) Algorithm

Input: μ, 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**

Proof: In the HWFA algorithm, we have two design goals: one is that the watchdog frequency fij should increase when Tij grows up from 0 to 0.5 but decrease when Tij climbs from 0.5 to 1, and the other is that the smallest fij 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, 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 the next Section.

D. *PERFORMANCE EVALUATION*

In this section, we evaluate our watchdog optimization algorithms using a popular WSNET simulation platform. Here we analysis about the energy consumption, energy efficiency, trust model and transmission delay ratio.

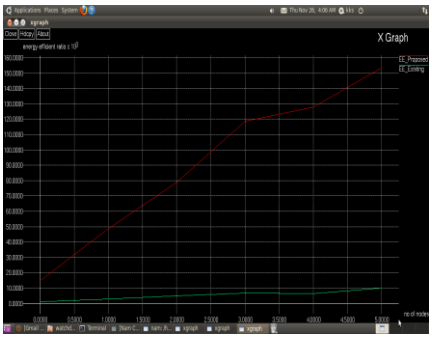

Fig no. 4: Energy efficiency ratio

The above picture shows the energy efficiency ratio of our proposed model. This comparison between existing transmission and trust model energy efficiency ratio and proposed energy model ratio. Here in proposed method having high efficiency of energy ratio compare to our existing method energy ratio.

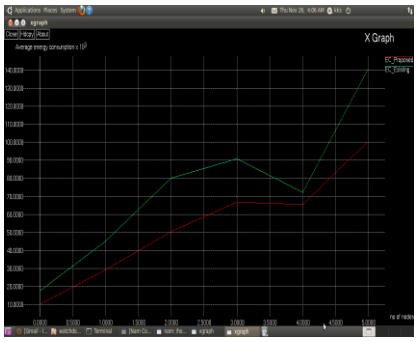

Fig no. 5: Average Energy Consumption

The average energy consumption ratio comparison is shown in the above picture. Here compared the usage level of energy in existing and proposed models. We got high energy consumption that means min level of energy used and more energy saved in our proposed method. So, in our proposed we decreased energy usage and increased energy efficiency ratio.

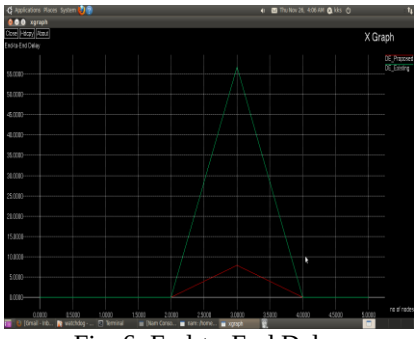

Fig. 6: End-to-End Delay

The above comparison describes the Delay in proposed and existing models. In this proposed we achieved less amount of delay and we improved our energy efficiency, energy consumption to decrease our end-to-end transmission and packet forwarding delay and improve security. Above all analysis gives better performance compared to existing methods.

V. CONCLUSION AND FUTURE WORK

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.

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 and the anonymity networks.

VI. REFERENCES

[1] T. Hara, V.I. Zadorozhny and E. Buchmann, Wireless Sensor Network Technologies for the Information Explosion Era, Studies in Computational Intelligence, vol. 278. Springer-Verlag (2010).

[2] Y. Wang, G. Attebury and B. Ramamurthy, A Survey of Security Issues in Wireless Sensor Net-works. IEEE Comm. Surveys & Tutorials 8(2): 2-23 (2007).

[3] A.A. Abbasi and M. Younis, A Survey on Clustering Algorithms for Wireless Sensor Networks. Computer Comm. 30(14/15): 2826-2841 (2006).

[4] W. Heinzelman, A. Chandrakasan and H. Balakrishnan, An Application-Specific Protocol Architecture for Wireless Microsensor Networks. IEEE Trans. Wireless Comm. 1(4): 660- 670 (2002).

[5] A. Manjeshwar, Q.A. Zeng and D.P. Agrawal, An Analytical Model for Information Retrieval in Wireless Sensor Networks Using Enhanced APTEEN Protocol. IEEE Trans. Parallel & Distributed Systems 13(12): 1290 -1302 (2002).