International Journal of Power Control and Computation(IJPCSC)
Vol 8. No.1 – 2016 Pp.44-50
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-268X

ENERGY-EFFICIENT TRUST SYSTEM THROUGH WATCHDOG OPTIMIZATION

B.Thaiyumanaswamy
Dept. of Computer Science and Engineering.
PRIST UNIVERSITY,Thanjavur, Tamilnadu, India

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 test bed 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.

INTRODUCTION

As a critical complement to traditional security mechanisms(e.g., cryptographic methods , authentication and access control logics etc.), trust systems are widely applied to protect wireless sensor networks for short) from being attacked by "legitimate" sensor nodes (i.e., the nodes are either compromised or selfish or on fault) . 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 misbehaviour . That is, trust is built upon sensor nodes' reputation and past behaviours, and can be used to model these nodes' honesty and internal states. Although many trust systems enable trust recommendations to extend the trust from neighbourhood (i.e., direct trust) to a global network view (i.e., indirect trust), the direct experience of past behaviours is still the basis for securing those recommendations. In another word, sensor nodes' past behaviours constitute the basic foundation for building WSN's trust systems (WSNTSs for short).

However, collecting enough past behaviours 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) and cluster heads (when a hierarchical topology), 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., neighbourhood) 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 behaviours are hard to be collected using business traffic. Third, since trust is context aware, the experience of one kind of behaviours 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 behaviours 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 behaviour collection, most of existing WSNTSs have adopted a so-called watchdog technique. 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 neighbourhood nodes.

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 , 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. We thus seek appropriate watchdog frequency depending on target nodes' trustworthiness.

2. 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, 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 trust evaluation 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 clustering.

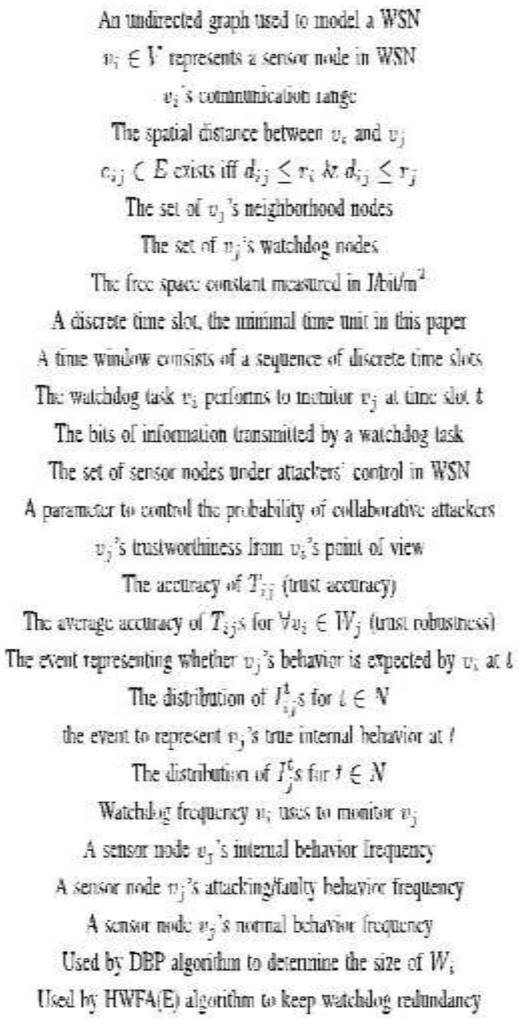
Despite those preliminary efforts, none has taken watchdog technique, perhaps the largest energy consumption unit in WSNTS, into consideration. We thereby conduct an innovative study in this paper to optimize watchdog scheduling. Our research is very different compared to the literature and opens a new door to energy-efficient WSNTS design. First, unlike 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 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 , 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 .

3. 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. We then model WSN's energy consumption law in Section. Afterwards, we reason about WSNTS on top of a threat model in Section III-C and a trust model in Section, respectively. For the ease of reference, we summarize important notations used by this paper.

3.1 SYSTEM MODEL

We model a WSN as an undirected graph $G = (V , E)$, where $v_i \in V$ represents a sensor node in WSN and $e_{ij} \in E$ means that the nodes v_i and v_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 v_i and v_j , and let r_i be the communication range of v_i . We consider that $e_{ij} \in E$ exists.



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

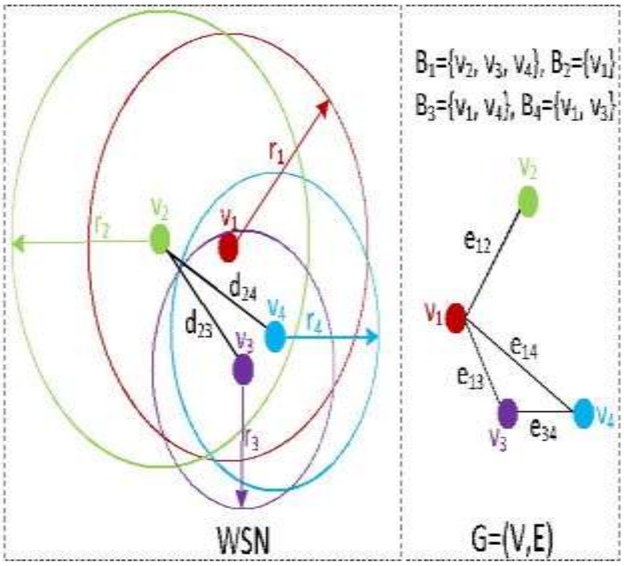


Fig. 1. An example of WSN and the system model *G*

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 v_i performs to monitor its neighbor node v_j at time slot *t*. A watchdog task w_{ij}^{t} consists of a bidirectional communication between the watchdog node v_i and the target node v_j. That is, v_i should send a request packet to v_j and then wait for v_j's response. By this requirement, v_i can take watchdog task

3.2 ENERGY CONSUMPTION MODEL

In proposed a energy-efficient trust model by applying a geographic target nodes 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 watchdog's technology is widely used to estimate energy consumed by each task typical free space wireless radio model. In this model, a sensor node's transmitter unit to the main node as file request and then the facts can be sends multiple requested node and DBP algorithms to avoid the WSNTS attacks. The source node sends all type of file, and then enters the data sends from source node to destination node over the network. As well as data must be send from source node to intermediate node automatically in this module the data's are successfully transfer from source to destination without attacks.

3.3 TRUST SYSTEM

Client-server computing or networking is a distributed application that partitions watchdog's task between source and target nodes. Often clients and servers operate over a network on separate functionalities. A server machine is a high-performance host that is running one or more tasks which share its resources with nodes. All the active nodes in WSN, Once the correct destination router is found, an end-to-end peer connection (TCP or IP) is established to carry end-system. This connection remains active as long as the file requested transferred and it is dynamically shut down when not in use, permitting casual, any-to-any communication without the burden of specifying peer connections in advance. When performing watchdog tasks to monitor routing behaviour, the watchdog nodes may waste some watchdog tasks if they miss the target node’s forwarding packets due to noises. The number of connections to establish between each pair of target node is established between each and every nodes for network communication. From the source node to the destination node and intermediates node must have connection between source nodes after communicate between combinations of multi node each and every node must be link to each other. In multipath data transmission, send the data from source node that means which type of file size and file extension.

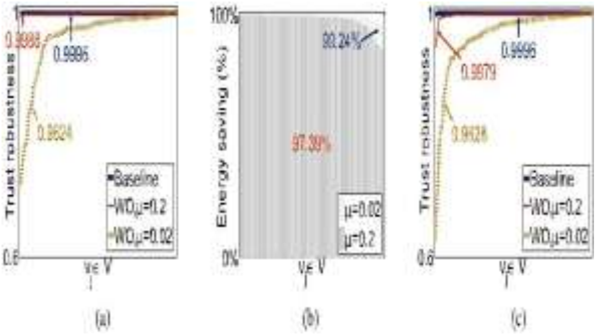


Fig. 2. Evaluation results for **on-off attacks**. WO refers to our watchdog optimization

4. WATCHDOG OPTIMIZATION TECHNIQUES

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.

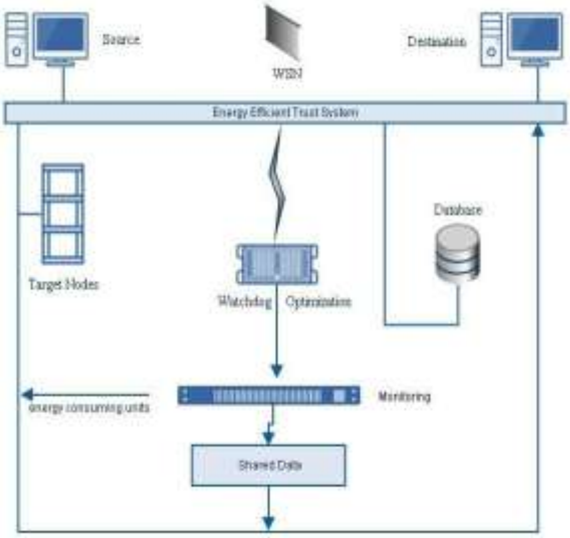


Fig. 3. An example of WSNs WATCHDOG model.

4.1 WSNET SIMULATION

WSNET 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 pluggable models (e.g., the radio, MAC, routing protocol stack, battery and applications etc.). Due to this flexible design and excellent emulating performance, WSNET has drawn widely attention in the literature .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 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 watch-dog mechanism only cares about neighbourhood behaviours.

$$\mathit{Energy\ saving} = \frac{\mathit{cost\ (\ Baseline)} - \mathit{cost\ (W\ O)}}{\mathit{cost\ (\ Baseline)}}$$

4.2 IN-DOOR TESTBED EXPERIMENTS

In addition to WSNET simulation, we also investigate watchdog optimization in realworld 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.

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.

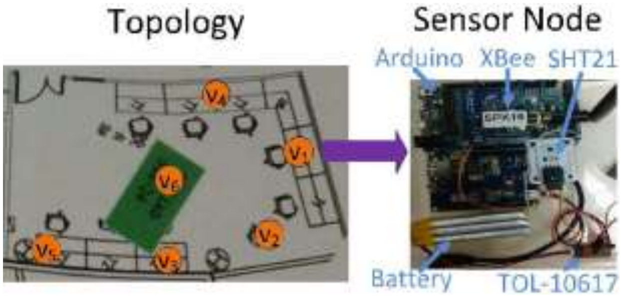


Fig. 4. An example of Indoor Testbed model

5. DISCUSSION AND FUTURE WORKS

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 behaviours 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 behaviours. In our experiments in Section V, we just randomly assign attacking behaviours 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 $(4L\_\alpha)^{-\ 13}$), 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).

6. 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.

ACKNOLEDGEMENT

The author would like to thank to all my faculties PRIST University, without whose cooperation this venture would not have been a successful one.

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 wire-less 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 local-ization in wireless sensor networks,” in *Proc. 8th Annu. IEEE Commun. Soc. Conf. Sensor, Mesh, Ad Hoc Commun., Netw. (SECON)*, Jun. 2011, pp. 386–394.