ENHANCE ENERGY PROFICIENT DEPENDENCE SYSTEM THROUGH WATCHDOG OPTIMIZATION FOR WSN

Ms.Meenadevi.M, Mr.NandhaKumar.S, Mr.Raja.G,Ms.Nivethitha.N

Student, Dept.of comp.sci.,Dhanalakshmi Srinivasan Engineering College,Tamilnadu,India

Professor, Dept.of comp.sci.,Dhanalakshmi Srinivasan Engineering College,Tamilnadu,India

Assistant Professor,Dept.of comp.sci., Dhanalakshmi Srinivasan Engineering College,Tamilnadu,India

Student, Dept.of comp.sci., Dhanalakshmi Srinivasan Engineering College,Tamilnadu,India

---***---

Abstract – *WSNTs using the Watchdog technique which is used to monitor and identify the malicious node in network. This technique is used for trust behavior collection, and hence gets a very good performance in guarding data sensing and multi-hop routing. This technique has been proved as a very effective approach to build up WSNTS's foundations. However, this kind of technique consumes much energy and hence decreases the lifespan of WSN. In existing system, watchdog introduces a large amount of additional energy consumptions and does not provide appropriate solutions to reduce the energy consumption problem. Due to those challenges, energy saving plays a very important role in WSNs. This paper reveals the improficient use of watchdog technique in existing trust systems, and thereby proposes an optimization method to reduce the energy cost of watchdog usage, while keeping the security in a satisfactory level*

Key Words: *Wireless Sensor Network Trust Systems, Network Security, Energy Efficiency, Optimization Techniques.*

1. INTRODUCTION

A wireless sensor network sometimes called a wireless sensor and actor network are 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.

The WSN is built of nodes from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. A critical complement to security mechanisms such as cryptographic methods, authentication and access control logics etc. These trust systems are widely applied to protect wireless sensor networks from being attacked by trust sensor node. Those nodes can bypass traditional security protections using their trust identities, but can be possibly captured by trust systems due to their poor reputation or past misbehavior. However, collecting enough past behaviors through business traffic to build a reliable trust system for WSN is not a trivial task.

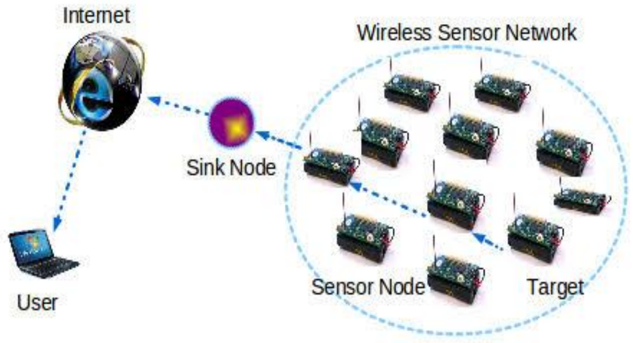


Fig- 1: WSN network

First, the powerful base station and cluster head, both of which are likely to have business requirements to interact with the whole network, may not locate in the communication range 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, the experience of one kind of behaviors cannot be used to build up trust for another kind. To overcome those challenges and facilitate past behavior 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 neighborhood nodes.

2. SYSTEM MODEL

In this section we consider the existing system design and the proposed system.

2.1 Existing System

WSN provide 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 watchdog technique. This technique allocate the watchdog task the node performs to monitor its neighbor node at time slot. A watchdog task consists of a bidirectional communication between the watchdog node and the target node. But this technique required large amount of energy. The inefficient use of watchdog technique in existing trust systems.

It increases energy consumption in WSNTs. Sensor nodes are usually equipped with limited battery and work in an unattended mode for a long period of time. Rechargement or Replacement of those nodes power is very difficult and expensive. So overcome by this problem saving the energy is important in WSN. In Existing, WSNTs not gives correct solutions to save the energy consumption. And also WSNTSs do not discuss how to schedule watchdogs.

Drawbacks:

- This kind of technique consumes much energy.
- They not give correct solution for energy consumption.
- This technique is not efficiently identified and blocks the attacking nodes.
- Decrease the network lifetime.

2.2 Proposed System

Due to overcome by this problem, propose the optimizing watchdog techniques for WSNTSs. This technique is used to balance energy efficiency and security in terms of trust accuracy and robustness. 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 using watchdog optimizes techniques in two levels.

First level to optimize watchdog locations given a target node to minimize the overall risk in terms of both energy consumption and security. Watchdog Location Optimization technique using DBP (Distance Based Probabilistic) algorithm to identify the target node and create shortest distance communication. It identifying misbehaving sensor nodes and preventing those nodes from being used for future routing. So proposed an energy efficient secure routing algorithm to choose efficient and trustworthy next-hop node in a route.

Second level to optimize watchdog frequency and reduce its redundancy. Watchdog Frequency Optimization technique using HWFA (Heuristic Watchdog Frequency Adjustment) algorithm to estimate energy units for each node. Based on this energy consumption node transfer the data to intermediate nodes. This algorithm define the number of watchdog tasks taken for watchdog node performs to monitor a target node within a time window as watchdog frequency. Also, define a nodes behavior frequency and attacking frequency within the time window. Based on this to adjust watchdog frequency and reduce it redundancy.

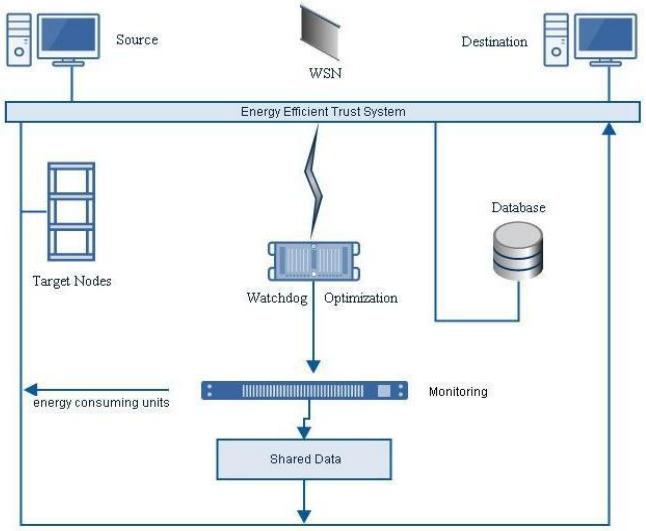


Fig-2: Architecture Diagram

Benefits:

- This technique efficiently saves the energy.
- It also decreases the energy consumption.
- Watchdog optimization to minimize the energy cost watchdog usage.
- This technique save the nodes energy.
- So it increases the network lifetime and trust accuracy.

3. DESIGN CONSTRUCTION

This Section consists of the following module design. These are to be explained in this section.

3.1 Trust Systems

Intermediate nodes are computing or networking is a distributed application that partitions watchdog's task between source and target nodes. These nodes are connected and communicate by using IP address and host name. Often Inheritor nodes 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.

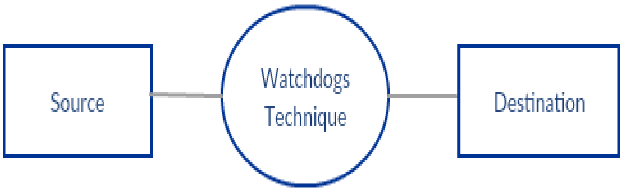


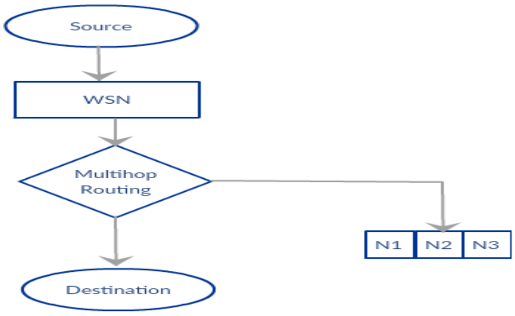
Fig-3: Trust Systems

3.2 Target Nodes

Choose the target node from the intermediate nodes. Then the number of connections to establish between each pair of target node and 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. After to choose the neighbor nodes and communicate with each other and also set the priority queue in the network communications. In multipath data transmission, send the data from source node that means which type of file size and file extension.

3.3 Watchdog Optimization Techniques

This technique is used to create shortest path between intermediate nodes to target node. Using Watchdog Location Optimization techniques to identify the nodes location. Using DBP algorithm to find the minimum location distance of the target node. Based on Neighboring Multi hop Routing algorithm to design the routing between nodes. This algorithm is used to calculate the routing path. 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.



F

ig-4: Multi-hop Routing

3.4 Energy Consumption

In proposed system, 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. Watchdog Frequency Optimization techniques is used to estimate energy consumption of each nodes. Energy watcher using the HWFA algorithm to calculate energy value of each nodes.

Depends on this value the files is transfer to the target node. 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.

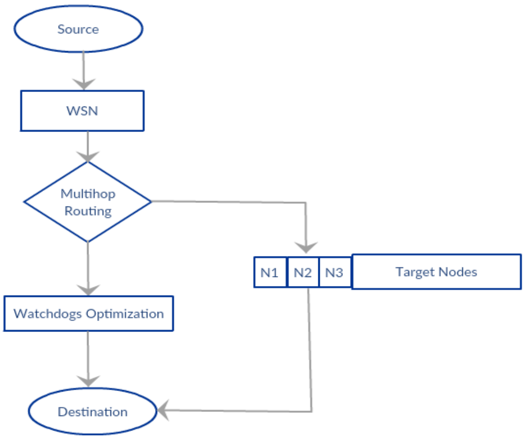


Fig-5: Watchdog Optimization

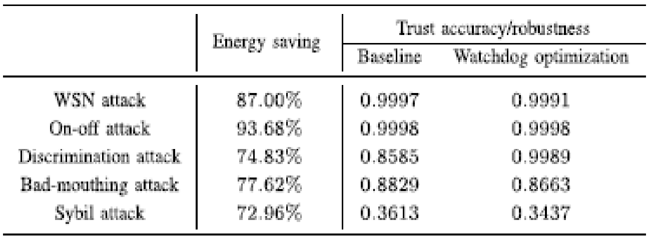
4. Evaluation and Performance

This Experiment is implemented on Intel Core i3 with CPU of 2.40 GHz and RAM of 2 GB. WSNET is an event-driven module-based WSN 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 this experiments, 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. We measure security in terms of trust accuracy or robustness, while show energy saving using the following equation.

Energy saving=cost(Baseline)−cost(WO) cost(Baseline),

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. 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 ||Wj|| = πj · ||Bj||= 1 for DBP algorithm, since sensor nodes' behaviors observed by different neighbor nodes are the same. We also consider α = 0.5 to calculate the optimal watchdog location for DBP algorithm. We choose μ=0.2 for HWFA algorithm to maintain some capability against WSN's noisy transmission nature. 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.

Table 1: Experimental Results



	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

To apply the DBP algorithm to this real-world setting, we need to estimate of XBee-Pro RF Module for calculating the optimal location. 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 as 60·10−3 250·103·1002 = 24 pJ/bit/m2. 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 ||Wj||=πj·||Bj||=1 for WSN attack and on-off attack, and πj = 0.4 for other attacks. In HWFA algorithms, we choose μ= 0.2.

The mean values of trust accuracy/robustness and energy saving over the six nodes. As can be seen, we can save up to 93.68% energy in this real-world scenario, and meanwhile induce trust accu- racy/robustness reduction no more than 0.3613 − 0.3437 = 0.0176. 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 Bj given a target node vj) to perform watchdog tasks. Instead, our DBP algorithm enables the selection of πj ·||Bj|| nodes as watchdog nodes. For example, if we choose πj = 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.

5. CONCLUSION

In this project, Watchdog Optimization algorithm is presented by considering a new approach. It can be used to solve several optimal problems. It is aimed to minimize the length of the tour and find the target path. Algorithm is highly flexible and can be effectively used to find shortest path by considering very few control parameters as compared with the other heuristic algorithms. This study thus shed light a promising research direction on the design of energy-efficient WSNTS by optimizing the collection procedure of first-hand experiences. Future concerns are to identify which type of attacker and to block the attacker using algorithm. And also to estimate the attacking models parameter. Using this optimization technique to improve watchdog tasks allocation for each time window. Then the important problem is load balancing problem. This will be solving in future work. In the future will continue the work and apply 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.

REFERENCES

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

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

[3] Marti S. Giuli T. J. Lai K. and Baker M. (2000) 'Mitigating routing misbehavior in mobile ad hoc networks', in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw, pp. 255–265.

[4] Perrig A. Stankovic J. and Wagner D. (2004) 'Security in wireless sensor networks', Commun . ACM, vol. 47,no. 6, pp. 53–57.

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

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

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

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

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