Volume 6, Issue 5, May 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Optimized Employee Communicate to WSN Monitering Operation

L. M. Muthu Lakshmi
Research Scholar, Dept. of Computer Science,
Tamil University, Thanjavur, Tamilnadu, India

A. Senthil Kumar
Asst. Professor, Dept. of Computer Science,
Tamil University, Thanjavur, Tamilnadu, India

Abstract: A network of these devices will collaborate for a common application such as environmental monitoring. We expect sensor networks to be deployed in an ad hoc fashion, with individual nodes remaining largely inactive for long periods of time, but then becoming suddenly active when something is detected. The technique of using watchdog is a fundamental building block to many trust systems that are designed for securing wireless sensor networks (WSNs). But this kind of technique consumes much energy and hence largely limits the lifespan of WSN. Watchdog is a monitoring technique which detects the misbehaving nodes in the network. Watchdog technique is a fundamental building block to many trust systems that are designed for securing wireless sensor networks (WSNs). In our work the power consumption models of the microcontroller and the sensor node are defined based on their digital operations so that the parameters of the digital algorithms can be optimised to achieve the best energy efficiency. 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.

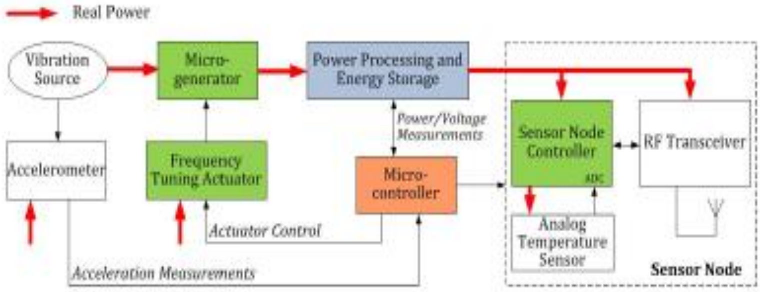
Keywords: Ad-hoc, DSR, Routing alogorithms.

I. INTRODUCTION

The inefficient use of watchdog implementation in existing trust systems lead me to propose a suite of optimization methods to minimize the energy consumption of watchdog, while keeping a sufficient level system security. The optimization method consist of theoretical analyses and practical algorithms, which can effectively and efficiently schedule the watchdog tasks depending on the sensor node's locations and the target node's trustworthiness.

A Wireless Sensor Network (WSN) is a specialized wireless network that is composed of a number of sensor nodes deployed in a specified area for monitoring environment conditions such as temperature, air pressure, humidity, light, motion or vibration, and can communicate with each other using a wireless radio device. WSNs are powerful in that they are amenable to support a lot of very different real-world applications; they are also a challenging research and engineering problem because of this very flexibility.

Vibration-based energy harvesters are used in many commercial applications since mechanical vibrations are widely present. Most of the reported vibration energy harvester designs are based on a spring-mass-damper system with a characteristic resonant frequency. These devices normally have a high Q-factor and generate maximum power when their resonant frequency matches the dominant frequency of the input ambient vibration. Consequently, the output power generated by the micro generator drops dramatically when there is a difference between the dominant ambient frequency and the micro generator's resonant frequency.


Real Power
Vibration Source
Micro-generator
Power Processing and Energy Storage
Power/Voltage Measurements
Accelerometer
Frequency Tuning Actuator
Micro-controller
Sensor Node Controller
ADC
RF Transceiver
Actuator Control
Analog Temperature Sensor
Acceleration Measurements
Sensor Node

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.

II. TRUST SYSTEM COMMUNICATED

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.

Sensor nodes, the nodes are either compromised or selfish or on fault. Those nodes can bypass traditional security criteria using their identification, but can be possibly captured by trust systems due to their poor reputation or past misbehavior. That is, trust is built upon sensor nodes reputation and past behaviors, and can be used to label these node's internal states and honesty. Although many trust systems enable trust recommendations to extend the trust from neigh borhood to a global network view, the direct experience of past behaviors is still the basis for securing those recommendations. In another word, sensor node's past behaviors constitute the basic foundation. Collecting enough past behaviors through business traffic to build a reliable trust system for a wireless sensor network is not a trivial task.

As a result of which it sends the message through an intermediate node B. When the node B receives a packet from A it then forwards it to C. Here we may consider SA be a set of nodes which hear messages sent from A to B and SB be a set of nodes that hear message from B to C. In this way we may define a set of possible watchdogs of the node B as an intersection of SA and SB. This means that any node that lies in the intersection region is able to hear both messages and is able to decide whether node B forwards message from node A. This approach relies on the broadcast nature of Wireless communications and the assumption that sensors are usually densely deployed. When a message is broadcasted in a network the packet is not only received by the intended node but it is also received by the neigh boring nodes within that range. Normally such nodes should discard the packet, but this can be used for intrusion detection. Hence, a node can activate the IDS agent and monitor the packets that are sent by its neighbours by overhearing them.

They have proposed optimization on the first watchdog approach. There are two techniques for watchdog optimization: one is watchdog location optimization and the other is watchdog frequency optimization. In watchdog location optimization, the optimal watchdog positions are identified. Once the optimal node is identified where on which the watchdog mechanism has to be performed, the selection of nearby neighbour node of that optimal node will perform the watchdog mechanism in order to reduce its energy cost. The algorithm proposed here is DBP Distance Based Probabilistic algorithm.

2.1. Advantage of Employing Multiple Base Stations

Consider two different sensor network deployments as sensor node A is one hop away from its nearest base station when two base stations are deployed. For sensor node B the hop-count from its nearest base station is same in both the cases. Thus, by employing two base stations instead of one we have effectively either reduced or retained the hop count of each sensor node in the network. Since the energy consumed in routing a message from any sensor node to its nearest base station is proportional to number of hops the message has to travel, employing multiple base stations effectively reduces the energy consumption per message delivered.

The authors attribute this to the fact that nodes which are one hop away from base station need to forward messages originating from many other nodes, in addition to delivering their own messages. In doing so, these sensor nodes deplete their energy quicker and become in operational. As a result, many sensor nodes will be unable to communicate with the base stations and the network becomes in operational.

To increase the lifetime of sensor network we propose to employ multiple base stations, and periodically change their locations. We propose two strategies to choose base station

locations and compare the performance of these strategies with three other strategies. We also propose a routing protocol based on flow information. Through simulations we show that our strategies outperforms all the other strategies.

Latency can be important or unimportant depending on what application is running and the node state. During a period that there is no sensing event, there is normally very little data flowing in the network. Most of the time nodes are in idle state. Sub-second latency is not important, and we can trade it off for energy savings. S-MAC therefore lets nodes periodically sleep if otherwise they are in the idle listening mode. In the sleep mode, a node will turn off its radio. The design reduces the energy consumption due to idle listening. However, the latency is increased, since a sender must wait for the receiver to wake up before it can send out data.

To demonstrate the effectiveness and measure the performance of our MAC protocol, we have implemented it on our tested wireless sensor nodes, Motes, developed by University of California, Berkeley. The mote has a 8-bit Atmel microcontroller running at 4. It has a low power radio transceiver module TR1000 from RF Monolithic, which operates at 916.5 MHz frequency and provides a transmission rate of 19.2 Kbps. The mote runs on a very small event-driven operating system called TinyOS. In order to compare the performance of our protocol with some other protocols, we also implemented a simplified on this platform.

III. SENSOR-MAC PROTOCOL DESIGN PROCES

The main goal in our MAC protocol design is to reduce energy consumption, while supporting good scalability and collision avoidance. Our protocol tries to reduce energy consumption from all the sources that we have identified to cause energy waste, idle listening, collision, overhearing and control overhead. To achieve the design goal, we have developed the SMAC that consists of three major components: periodic listen and sleep, collision and overhearing avoidance, and message passing. Before describing them we first discuss our assumptions about the wireless sensor network and it applications.

3.1. Watchdog optimization

Two ultimate goals when optimizing watchdog techniques: First is to minimize the energy usage or consumption of the whole WSN and the other is to maximize the security in terms of trust accuracy and trust robustness. The optimization goals as follows: Minimize the energy consumption throughout the whole WSN and maximize trust accuracy of WSN. Hence the Watchdog Optimization is the core area of energy optimization.

The optimization approach mentioned above can be used in such hierarchical approach where the optimization techniques like the watchdog location optimization might give a better result. In this case, since the watchdog mechanism is applied only on the cluster-head nodes, identifying the optimal node that performs watchdog mechanism can be easily identified. The improved watchdog mechanism has overcome most of the limitations of its previous watchdog approach, the watchdog frequency optimization can be used for referencing the trust worthiness to overcome the remaining limitations of the improved watchdog approach.

3.2. Base Stations

In the authors demonstrated through experimental results that the sensor nodes which are one-hop away from a base station drain their energy faster than other nodes in the network. The authors attribute this to the fact that nodes which are one hop away from base station need to forward messages originating from many other nodes, in addition to delivering their own messages. In doing so, these sensor nodes deplete their energy quicker and become in operational. As a result, many sensor nodes will be unable to communicate with the base stations and the network becomes in operational.

To increase the lifetime of sensor network we propose to employ multiple base stations, and periodically change their locations. We propose two strategies to choose base station locations and compare the performance of these strategies with three other strategies. We also propose a routing protocol based on flow information. Through simulations we show that our strategies outperforms all the other strategies.

IV. CONCLUSIONS

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. The identified design parameters are investigated using response surface model based design space exploration and optimisation. We use Systems-A to model the system's analogue Components as well as the digital processes and MATLAB to generate and optimise the response surface model.

REFERENCES

[1] Seung-Jun Kim, Xiaodong Wang, and Mohammad Madihian, "Distributed Joint Routing and Medium Access Control for Lifetime Maximization of Wireless Sensor Networks", vol. 6, no. 7, July 2007 2669

[2] Riaz Ahmed Shaikh, Hassan Jameel, Brian J. d'Auriol, Member, IEEE Computer Society,Heejo Lee, Member, IEEE, Sungyoung Lee, Member, IEEE, and Young-Jae Song, "Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks" IEEE transactions on parallel and distributed systems, vol. 20, no. 11, Nov 2009 [3] Xiaoyong Li, Feng Zhou, and Junping Du,"LDTS: A Lightweight and Dependable Trust System for Clustered Wireless Sensor Networks",IEEE transactions on information forensics and security, vol. 8, no. 6, June 2013

[4] Sergio Marti, T. J. Giuli, Kevin Lai, "Energy Mitigating routing misbehavior in mobile adhoc networks", in MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking, pp.255–265, New York, NY, USA, 2000.

[5] Abror Abduvaliyev, Al-Sakib Khan Pathan, "On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks", Vol. 15, Issue 3, Third Quarter 2013.

[6] A. Forootaninia and M. B. Ghaznavi-Ghoushchi, "An Improved Watchdog Technique based on Power-Aware Hierarchical design for IDS in Wireless Sensor Networks", Vol.4, Issue 4, pp.161-178, July 2012.

[7] J. Agre and L. Clare. An integrated architecture for cooperative sensing networks. *Computer,* 33(5):106 – 108, 2000.

[8] J. Chlebikova. Approximability of the Maximally balanced connected partition problem in graphs. *Inform. Process. Lett.,* 60:225 – 230, 1996.

[9] L.Wang, T. Kazmierski, B. Al-Hashimi, A.Weddell, G. Merrett, and & (DATE 2011), March 14-18, 2011, pp. 1267–1272.

[10] J. Jacquez, "Design of experiments," Journal of the Franklin Institute, vol. 335, no. 2, pp. 259–279, 1998.