IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.047 ⁜ Vol. 10, Issue 10, October 2022

DOI: 10.17148/IJIREEICE.2022.101001

Energy Optimization in Wireless Sensor Networks

Dr A. Rajasekaran[1], Mr Nishanth Kiruthivasan[2]

Assistant Professor, Dept of ECE, SCSVMV University, Enathur, Kanchipuram[1]

UG scholar, Dept of ECE, SCSVMV University, Enathur, Kanchipuram[2]

Abstract: Wireless sensor nodes typically have short memory and battery life. This limitation requires powerful algorithms that can be used to reduce power consumption. The main energy is consumed when sending data. Some of the energy is spent processing data. This document introduces another approach to reduce energy consumption. We consider both shipping and handling charges. So, it uses short range and data compression to reduce power consumption. We designed and implemented TARF, a robust trust-aware routing framework for dynamic WSNs. Without strict time synchronization or known geographic information, TARF provides reliable and energy efficient routes. Most importantly, TARF has proven effective against malicious attacks created by impersonators. TARF's robustness is verified through extensive evaluation using both simulations and demonstration experiments on large-scale WSNs under various scenarios.

I. INTRODUCTION:

Keep in mind that the field of wireless networks and mobile computing is evolving rapidly. Compared to wired networks, wireless networks are more advantageous because they are easier to scale and quicker to deploy. Best of all, wireless networks are cheap. A sensor node is a low-power device with built-in sensor functionality. Sensor nodes have small processing power and are capable of wireless communication.

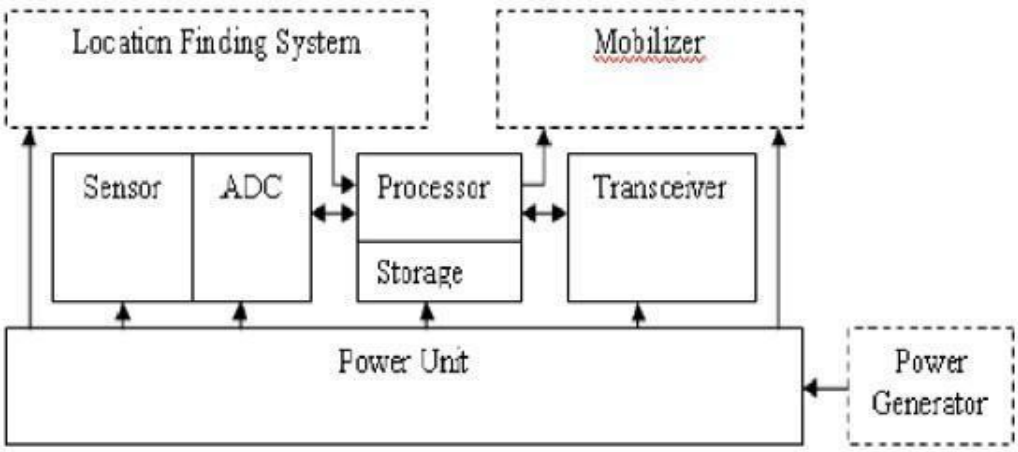

Fig. 1 Basic WSN Block Diagram

We look for secure routing of data collection tasks, which is one of the most basic features of WSN. In data acquisition tasks, sensor nodes send sampled data to remote base stations with the help of other intermediate nodes. There may be multiple base stations, but the routing approach is independent of the number of base stations. For simplicity of discussion, let's assume there is only one base station. An attacker can disguise the identity of a legitimate node by replaying that node's outgoing routing packets and forging acknowledgment packets. Replaying routing packets enables the malicious node to spoof the identification of this valid node because a node in a WSN typically depends exclusively on the packets received to learn about the sender's identity. Having "stole" this valid identity, this malicious node can misdirect the network traffic. For example, it can drop received packets, forward packets to another node that should not be in the routing path, or even form transmission loops where packets traverse indefinitely between malicious nodes. Even with eavesdropping techniques, it is often difficult to know if a node is forwarding received packets correctly.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.047 ⁜ Vol. 10, Issue 10, October 2022

DOI: 10.17148/IJIREEICE.2022.101001

A sinkhole attack is another type of attack launched after a valid identity is stolen. A sinkhole attack allows a malicious node to impersonate a base station by replaying all packets from the real base station. Such fake base stations can attract more than half of the traffic, creating a "black hole".
The same technique can be used to carry out another powerful form of attack, the Sybil attack. By replaying routing information for multiple legitimate nodes, an attacker can present multiple identities to the network. All these attacks can also be launched if a valid node is compromised. The damage of such malicious attacks based on techniques to reconstruct routing information is exacerbated by the introduction of WSN mobility and hostile network conditions. While mobility is being introduced in WSNs for efficient data collection and various applications, the potential for interaction between honest nodes and attackers is greatly increased. Additionally, poor network connectivity makes it very difficult to distinguish between an attacker and an honest node that has suffered a transient failure. Without proper protection, WSNs using existing routing protocols can be destroyed. For emerging sensor applications over WSN, keeping the network undisrupted is critical to the success of the application.

II. LITERATURE SURVEY

The challenges of using WSN are:

1. WSN is used to collect environment information and used to change environment information.
2. Limited resources and low memory. All complex functions must be managed using different topologies.
3. Nodes should be designed to be self-organizing and self-optimizing. This is one of the biggest challenges.
4. There may be many WSN nodes, but the network should have a limited number of nodes to guarantee the necessary WSN services.
5. WSN works in the real world. Therefore, real-time capabilities are required where necessary.

There are many techniques and protocols for optimizing the power consumption of sensor nodes. Categories are mainly classified into the following types:

1. MAC layer technology
2. Network layer approach
3. Transmission control approach
4. Automatic approach

A. MAC layer approaches

Most of a node's energy is spent on radio transmissions and listening to media for messages. The MAC protocol manages communication and coordinates shared media for better performance. For example, Zigbee technology uses MAC protocol to reduce energy consumption. The TDMA MAC protocol is based on cross-layer optimization based on physical layer and MAC.

B. Network layer (Routing) approaches

The main purpose of the WSN application is to collect data from nodes and send it to sinks in an energy efficient manner using appropriate routing protocols. REACA, EARQ, MMSPEED, Energy Efficient Broadcast Problem (EEBP), and Green Wave Sleep Scheduling (GWSS) are some of the algorithms used to reduce power consumption at the network level.

C. Transmission Control approaches

There are many methods of transmit power control (TPC). Its main goal is to reduce power consumption and improve channel capacity. A TPC solution operates with a single transmit power for the entire network. One of the algorithms is the Power Control Algorithm with Back Listing (PCBL). In this algorithm, each node transmits packets at different transmit power levels and finds the optimal transmit power based on packet reception rate (PRR). Local Mean Algorithm (LMA) and Equal Transmission Power (ETP) are other approaches used in this layer.

D. Automatic approaches

Autonomic computing was introduced by IBM in 2001 to describe self-managing systems. The main property is self-configuration. These relate to the ability to configure the system itself to achieve high-level goals.
Self-optimization: Actively optimizing performance and quality of service as the system changes.

III. DESIGN OF SYSTEM

As explained in the previous section, there are many approaches to energy optimization. Our approach falls into the category of network layer (routing) approaches. The proposed procedure is basically divided into two steps. The first

DOI: 10.17148/IJIREEICE.2022.101001

step handles the routing part, and the second step handles the compression and decompression part. Combining both steps can improve results, improve reliability, and reduce energy consumption. Our main goal is to reduce the power consumption of sensor nodes to achieve good battery life and ensure data reliability. Each step is detailed in the following subsections.

Step 1:

Routing on TARF Basis

TARF protects multihop routing within a WSN against intruders who mislead multihop routing by evaluating the trustworthiness of neighbours. Identify unreliable intruders and route data along paths that bypass these intruders to achieve satisfactory throughput. TARF is also energy efficient, highly scalable, and highly customizable. Before introducing the detailed design, here we first introduce some necessary terminology. Neighbours For a node N, a neighbour of N is a node reachable from N by wireless one-hop transmission. Trust Level For a node N, the neighbour's trust level is a decimal number in [0,1] representing N's opinion of the trustworthiness of that neighbour. Specifically, a neighbour's trust level N is an estimate of the probability that this neighbour will correctly deliver received data to the base station. This trust level is referred to as T in this document. Energy Cost For a node N, the neighbours energy cost is the average energy cost to successfully deliver a unit size data packet using that neighbour as the next hop node from N to the base station. This energy cost is called E in this paper.

For a TARF-capable node N to route data packets to a base station, N only needs to consider both reliability and energy efficiency when deciding which neighbouring nodes to forward data packets to. Once the data packet is forwarded to this next hop node, the rest of the task of delivering the data to the base station is fully delegated to the base station and N has no knowledge of what routing decisions the next hop node is making. not. N maintains a neighbour table of certain known neighbour confidence level and energy cost values. It may be necessary to remove entries for some neighbours to keep the table size within an acceptable range. Woo, Tong, and Culler show how to maintain a reasonably sized neighbourhood table. The same technique can be used with TARF. In addition to sending data packets, TARF requires the exchange of two types of routing information. Broadcast messages from base stations regarding data delivery and energy cost report messages from each node. You do not need to confirm any messages. Broadcast messages from base stations are flooded throughout the network. A broadcast message's freshness is checked by its source sequence number field. Another type of routing information exchanged is energy cost report messages for each node. This is broadcast only once to neighbours. A node receiving such an Energy Cost Report message will not forward it. Two components, EnergyWatcher and TrustManager run on the node to maintain such a neighbour table containing the trust level and energy cost values of certain known neighbours for each node N in the WSN. EnergyWatcher is responsible for recording the energy cost of each known neighbour based on the N observations of one-hop transmissions to reach the neighbour and the energy cost reports from those neighbours. A compromised node can falsely report a very low energy cost to trick neighbours into choosing the compromised node as their next hop node. However, these TARF-enabled neighbours, as tracked by the TrustManager, are unreliable and will eventually abandon this compromised next-hop node. TrustManager tracks neighbouring trust level values based on network loop detection and broadcasts messages from base stations via data transmission. N broadcasts an energy report message when it can determine its next hop neighbour according to its neighbour table. Broadcast the energy cost of delivering a packet from a node to a base station to all neighbours. Energy costs are calculated in the EnergyWatcher section. Such energy cost reports also serve as input to the recipient's EnergyWatcher.

Step 2:

Compression and Decompression

Before sending the data, it can be compressed to save power in the sending node and intermediate nodes. This can be achieved using compression algorithms.

IV. RESULTS

This can be achieved using JavaScript. Data is sent from source to destination using the Trust-Aware Routing Framework, and data is compressed to optimize sensor node energy by sending compressed data using TARF. This improves energy efficiency and throughput. This can be achieved using JavaScript.

V. CONCLUSION

In this article, we proposed a simulation system based on power optimization using Trust Aware routing protocols. From the simulation, we conclude that:

High Throughput: Throughput is defined as the ratio of the total number of data packets delivered to the base station and the total number of data packets sampled.

DOI: 10.17148/IJIREEICE.2022.101001

Energy Efficiency: Data transfer accounts for most of the energy consumption.
Scalability and Adaptability: In highly dynamic contexts, should work well with large WSNs.
Application: This application can be implemented in any wireless network mobile ad-hoc.

REFERENCES

[1] Debmalya Bhattacharya and R. Krishna moorthy, "Power Optimization in Wireless Sensor Networks", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, September 2011.pp 415-419.
[2] M.Ismail, M. Y. Sanavullah, "Security Topology in Wireless Sensor Networks With Routing Optimisation" IEEE 2008.
[3] G.M. Ben Ezovski, S.E. Watkins, "The Electronic Sensor Node and the Future of Government-Issued RFID-Based Identification", RFID 2007.IEEE International Conference, pp 15-22, 2007.
[4] I.F. Akyiliz, W. Su, Y.Sankarasubramaniam and E. Cayirci, "A Survey on Sensor Network", IEEE Communication Magazine, pp 102-114, 2002.
[5] G. Zhan, W. Shi, and J. Deng, "Tarf: A trust-aware routing framework for wireless sensor networks," in Proceeding of the 7th European Conference on Wireless Sensor Networks (EWSN'10), 2010.
[6] F. Zhao and L. Guibas, Wireless Sensor Networks: An Information Processing Approach. Morgan Kaufmann Publishers, 2004.
[7] A. Wood and J. Stankovic, "Denial of service in sensor networks,"Computer, vol. 35, no. 10, pp. 54–62, Oct 2002