Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 4, April 2015, pg.549 – 553

RESEARCH ARTICLE

Energy Optimization in Wireless Sensor Networks

Banakar Vinodkumar[1], Mrs. Geetha N B[2], Mohamed Rafi[3]

[1]Department of, Computer Science, UBDTCE (VTU), India

[2]Assistant Professor, UBDTCE, Department of Computer Science, UBDTCE (VTU), India

[3]Professor, UBDTCE, Department of Computer Science, UBDTCE (VTU), India

[1] vinodsbanakar@gmail.com, [2] nbgeetha@yahoo.co.in, [3] rafimohamed17@gmail.com

Abstract — ***Wireless Sensor Nodes are generally having less memory and low battery life. Due to this constraint, we need a strong algorithm by which we can reduce the energy consumption. The main energy is utilized during sending of the data. Some part of energy is utilized in processing the data. In this paper, we will give another approach for reduced energy consumption. We will consider the cost of sending as well as processing. So, we will use short distance path as well as compression of the data to reduce the power consumption. We have designed and implemented TARF, a robust trust-aware routing framework for dynamic WSNs. Without tight time synchronization or known geographic information, TARF provides trustworthy and energy-efficient route. Most importantly, TARF proves effective against those harmful attacks developed out of identity deception; the resilience of TARF is verified through extensive evaluation with both simulation and empirical experiments on large-scale WSNs under various scenarios***

Keywords— Wireless Sensor Network, Energy optimization, compression, efficiency, TARF

I. INTRODUCTION

It is found that the area of wireless network and mobile computing is evolved fastly. When we compare Wireless network with wired networks, we have more benefit with wireless networks as they are capable of scaling easily, rapidly deployable. Wireless networks most importantly cost effective. Sensor nodes are low-power devices that is having inbuilt functionality of sensing, sensor nodes are having small amount of computing and wireless communication.

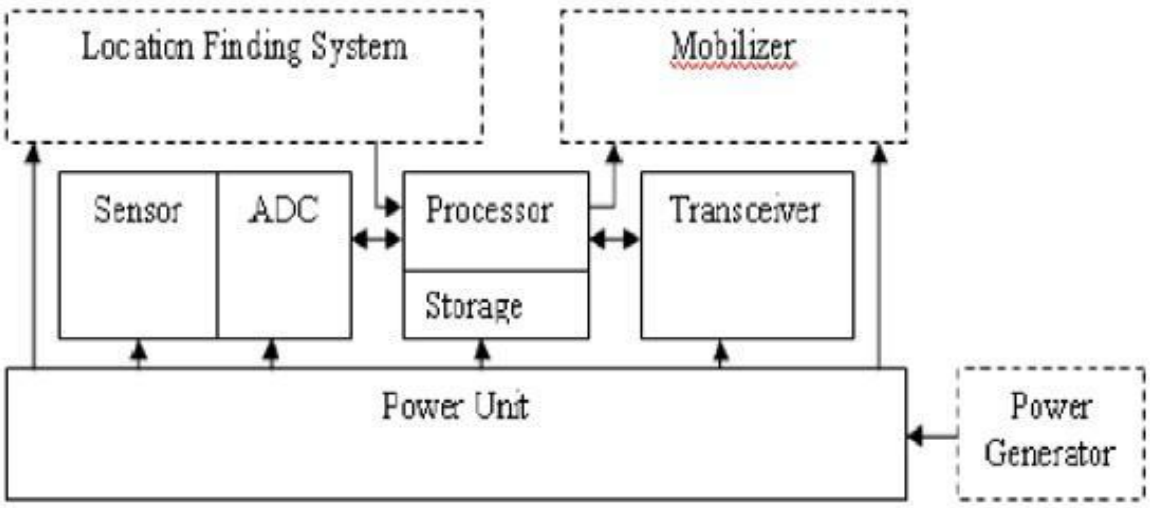

Fig: Components of sensor node

We look for secure routing for data collection tasks, which are one of the most fundamental functions of WSNs. In a data collection task, a sensor node sends its sampled data to a remote base station with the aid of other intermediate nodes Though there could be more than one base station, our routing approach is not affected by the number of base stations; to simplify our discussion, we assume that there is only one base station. An adversary may forge the identity of any legal node through replaying that node's outgoing routing packets and spoofing the acknowledgement packets, even remotely through a wormhole. Since a node in a WSN usually relies solely on the packets received to know about the sender's identity, replaying routing packets allows the malicious node to forge the identity of this valid node. After "stealing" that valid identity, this malicious node is able to misdirect the network traffic. For instance, it may drop packets received, forward packets to another node not supposed to be in the routing path, or even form a transmission loop through which packets are passed among a few malicious nodes infinitely. It is often difficult to know whether a node forwards received packets correctly even with overhearing techniques. Sinkhole attacks are another kind of attacks that can be launched after stealing a valid identity. In a sinkhole attack, a malicious node may claim itself to be a base station through replaying all the packets from a real base station. Such a fake base station could lure more than half the traffic, creating a "black hole". This same technique can be employed to conduct another strong form of attack - Sybil attack: through replaying the routing information of multiple legitimate nodes, an attacker may present multiple identities to the network. A valid node, if compromised, can also launch all these attacks. The harm of such malicious attacks based on the technique of replaying routing information is further aggravated by the introduction of mobility into WSNs and the hostile network condition. Though mobility is introduced into WSNs for efficient data collection and various applications greatly increases the chance of interaction between the honest nodes and the attackers. Additionally, a poor network connection causes much difficulty in distinguishing between an attacker and a honest node with transient failure. Without proper protection, WSNs with existing routing protocols can be completely devastated under certain circumstances. In an emergent sensing application through WSNs, saving the network from being devastated becomes crucial to the success of the application.

II. LITERATURE SURVEY

The challenges in deployment of WSNs are as follows:

1. The WSNs are used for collecting environmental information and it is also used for changing the environment information.
2. They are having limited resources and having less memory. It should manage all the complex functionality using different topologies. .
3. We have to make the node as self-organizing and self-optimizing which is one of the major challenge.
4. There may be a large number of WSN nodes but network must have limited number of nodes that guarantee the desired WSN service.
5. WSN operates in the real world. So, it must have real-time features as per need.

There are lot of techniques and protocols available for optimizing energy used by sensor nodes. The categories are mainly categorized into following types.

1. MAC layer techniques
2. Network layer approaches
3. Transmission control approaches
4. Automatic approaches

A. MAC layer approaches

The main portion of the node's energy is spent on radio transmission and on listening the medium for message MAC protocols manage communication and regulate the shared medium such that performance is improved. For example, Zigbee technology uses MAC protocol for less energy consumption. The TDMA MAC protocol is based upon cross layer optimization based upon Physical layers and MAC.

B. Network layer (Routing) approaches

The main objective of WSNs application is to gather the data from nodes and transfer the data to sink in energy efficient way using proper routing protocol. REACA, EARQ, MMSPEED, Energy Efficient Broadcast Problem (EEBP) and Green Wave Sleep Scheduling (GWSS) are some of the algorithm used for less energy consumption at network layer.

C. Transmission Control approaches

There are many Transmission Power Control (TPC) approaches available. Its main goal is to reduce the energy consumption and improve the channel capacity. TPC solutions work with single transmission power for whole network.One of the algorithm is Power Control Algorithm with Back Listing (PCBL), in this algorithm, each node transmit the packet with different transmission power levels to find optimal transmission power based on Packet Reception Ratio (PRR). Local Mean Algorithm(LMA) and Equal Transmission Power (ETP) are other approaches used at this layer.

D. Automatic approaches

Autonomic computing was introduced by IBM in 2001 to describe the systems that are self- manageable .The main properties with are Self- configuration: It concern with system's ability to configure by itself for achieving high level goals. Self-optimization: It concern with the change in system pro-actively to optimize the performance or quality of service.

III. SYSTEM DESIGN

There are many approaches available to optimize the energy as discussed in previous work section. Our approach comes under the category of Network layer (Routing) approaches. The proposed approach is basically divided into 2 steps. First step deals with the routing part and second step deals with the compression-decompression part. Both the steps when combined, can give better result and benefits of reliability and also less energy consumption. Our main objective is to reduce the energy consumed by the sensor node to have good battery life and also provide reliability of data. Each step is explained in details in following sub-sections.

Step 1:Routing Based on TARF

TARF secures the multi-hop routing in WSNs against intruders misdirecting the multi-hop routing by evaluating the trustworthiness of neighboring nodes. It identifies such intruders by their low trustworthiness and routes data through paths circumventing those intruders to achieve satisfactory *throughput*. TARF is also energyefficient, highly scalable, and well adaptable. Before introducing the detailed design, we first introduce several necessary notions here.

Neighbor For a node N, a neighbor (neighboring node) of N is a node that is reachable from N with one-hop wireless transmission.

Trust level For a node N, the trust level of a neighbor is a decimal number in [0, 1], representing N's opinion of that neighbor's level of trustworthiness. Specifically, the trust level of the neighbor is N's estimation of the probability that this neighbor correctly delivers data received to the base station. That trust level is denoted as T in this paper.

Energy cost For a node N, the energy cost of a neighbour is the average energy cost to successfully deliver a unitsized data packet with this neighbor as its next-hop node, from N to the base station. That energy cost is denoted as E in this paper.

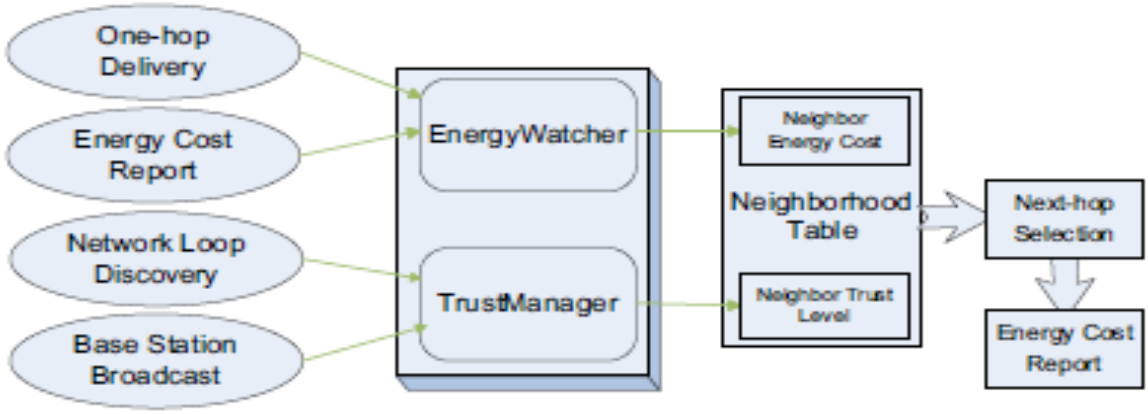

Fig : Design of TARF

For a TARF-enabled node N to route a data packet to the base station, N only needs to decide to which neighboring node it should forward the data packet considering both the trustworthiness and the energy efficiency. Once the data packet is forwarded to that next-hop node, the remaining task to deliver the data to the base station is fully delegated to it, and N is totally unaware of what routing decision its next-hop node makes. N maintains a neighborhood table with trust level values and energy cost values for certain known neighbors. It is sometimes necessary to delete some neighbors' entries to keep the table size acceptable. The technique of maintaining a neighborhood table of a moderate size is demonstrated by Woo, Tong and Culler. TARF may employ the same technique.

In TARF, in addition to data packet transmission, there are two types of routing information that need to be exchanged: broadcast messages from the base station about data delivery and energy cost report messages from each node. Neither message needs acknowledgement. A broadcast message from the base station is flooded to the whole network. The freshness of a broadcast message is checked through its field of source sequence number. The other type of exchanged routing information is the energy cost report message from each node, which is broadcast to only its neighbors once. Any node receiving such an energy cost report message will not forward it. For each node N in a WSN, to maintain such a neighbourhood table with trust level values and energy cost values for certain known neighbors, two components, *EnergyWatcher* and *TrustManager*, run on the node. *EnergyWatcher* is responsible for recording the energy cost for each known neighbor, based on N's observation of one-hop transmission to reach its neighbors and the energy cost report from those neighbors. A compromised node may falsely report an extremely low energy cost to lure its neighbors into selecting this compromised node as their next-hop node; however, these TARF-enabled neighbors eventually abandon that compromised nexthop node based on its low trustworthiness as tracked by *TrustManager*. *TrustManager* is responsible for tracking trust level values of neighbors based on network loop discovery and broadcast messages from the base station about data delivery. Once N is able to decide its nexthop neighbor according to its neighborhood table, it sends out its energy report message: it broadcasts to all its neighbors its energy cost to deliver a packet from the node to the base station. The energy cost is computed as in Section by *EnergyWatcher*. Such an energy cost report also serves as the input of its receivers' *EnergyWatcher*.

Step 2: Compression and Decompression

Before sending the data, we can compress it to save the energy of the transmitting node as well as intermediate nodes. It can be achieved by using the compression algorithms.

IV. RESULTS

This can be achieved by using JavaScript. In this the data is transferred from source to the destination by using the Trust-Aware Routing Framework and the data is compressed so that the energy of the sensor nodes are optimized by sending the compressed data using the TARF. This will increase the energy efficiency and throughput. This can be achieved by using JavaScript.

V. CONCLUSION

In this paper, we proposed a simulation system based on energy optimization using the Trust Aware routing Protocol.

From simulation , we conclude as follows:

High Throughput:

Throughput is defined as the ratio of the number of all data packets delivered to the base station to the number of all sampled data packets.

Energy Efficiency:

Data transmission accounts for a major portion of the energy consumption.

Scalability & Adaptability:

It should work well with WSNs of large magnitude under highly dynamic contexts.

Application:

We can implement this application in all Wireless network Mobile Ad hoc network.

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.

