Sudhir Chowdary.N, Siva Rama Krishna.Ch / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 4, July-August 2012, pp.345-348

Energy Minimization for Wireless Sensor Networks using Opportunistic Routing

Sudhir Chowdary.N[*], Siva Rama Krishna.Ch[**]
[*](department of Electronics and Communication, SRM University,Chennai)
[**](department of Electronics and Communication, SVIST Engg.Coll,Tiruvuru)

ABSTRACT

Wireless sensor networking research has received considerable attention in recent years as it represents the next phase of networking evolution. Efficient and reliable routing of data from the source to destination with minimal power consumption remains the crux of the research problem. Source privacy is one of the looming challenges that threaten successful deployment of these sensor networks, especially when they are used to monitor sensitive objects. In order to enhance source location privacy in WSN Opportunistic routing scheme is used. In this each sensor node transmits the packet over a dynamic path to the destination. Energy minimized Opportunistic routing technique is used for the efficient utilization of the power. The energy can be efficiently utilized by reducing transmission power of each node. By using the Energy minimized Opportunistic routing algorithm packets are sent in a secured manner with minimal power.

I. INTRODUCTION

Currently wireless sensor network research has received considerable attention since it is the next generation of the surveillance and monitoring scenario. We can deploy WSN throughout the geographical location for collecting data. The efficiency of the WSN depends on the effective routing of the data.

In [5] introduction about WSN and applications of the WSN are discussed. It also explains the hardware and software used in WSN like microprocessors, power, storage, bandwidth and operating systems used in WSN are discussed.

In [1] authors describe Opportunistic Routing (OR), a new unicast routing technique for multi-hop wireless networks. OR forwards each packet through a sequence of nodes, deferring the choice of each node in the sequence until after the previous node has transmitted the packet on its radio.

In [2] authors proposed to examine source-location privacy through opportunistic routing. In [3] authors provide a formal model for the source-location privacy problem and examine the privacy characteristics of different sensor routing protocols. They introduce two metrics for quantifying source-location privacy in sensor networks, the safety period and capture likelihood. The authors propose new techniques to enhance source-location privacy that augment these routing protocols.

In [4] authors focus on the multi-hop performance of such a solution, in terms of average number of hops to reach a destination as a function of the distance and of the average number of available neighbors. An idealized scheme (in which the best relay node is always chosen) is discussed, and its performance is evaluated by means of both simulation and analytical techniques. Even though they provide some discussion about practical issues and briefly outline a possible protocol based on the main ideas presented in this paper.

Such protocol is described and analyzed in detail in this paper. In [6] authors describe security solutions for collecting and processing data in Wireless Sensor Networks (WSNs). In [7] the author proposes to use large-scale cognitive networking methods to resolve the wireless multi-hop challenges. In this paper, we propose a new Energy Minimized Opportunistic Routing [EMOR] protocol. It makes use of the OR protocol technique for forwarding the packets from source to destination, but in this source location privacy is increased by reducing the transmission power of each node with this energy is also minimized.

This paper organized as follows. Section 2 presents sensor network and threat model. Section 3 describes EMOR principles. Section 4 presents simulation results for the energy minimized opportunistic routing. Finally, Section 5 presents the conclusion.

II. SENSOR NETWORK AND MODELS

Assume a large predefined geographical area that needs to be monitored, and deploy a wireless sensor network consisting of many randomly distributed sensor nodes. The network continuously monitors

activities and locations of the target in the area. When the target is discovered, the corresponding sensor becomes the source. Every sensor can be the source, and can send packets to neighboring sensors that are in the limited radio range. The source will continuously send packets until the adversary discovers the source, or the target disappears from the monitoring area.

The system is assumed to have the following characteristics:

- There is only one destination node at any time; while there can be more than one source.
- All the nodes in the network can participate in message transmission; hence, apart from detection capabilities they all have transmit and receive functionality, based on the applied protocol.
- Every node in the network knows the address of the destination node.
- Every node in the network knows its relative location.
- The adversary is assumed to have the following characteristics:
- The adversary knows the location of the destination and can determine the location of the sender sensor from the instance of the packet that it overhears.
- The adversary can physically move from one sensor to another and has unlimited amount of power.
- The adversary will not interfere with the proper functioning of the network.

III. ROUTING PROTOCOL PRINCIPLES AND PRIVACY PROTECTION

A. Opportunistic Routing principles:

During the last decade, a number of protocols have been developed in order to improve the performance in wireless sensor networks. One promising approach is referred to as opportunistic routing; relay node is opportunistically decided by dynamic network conditions such as interference, channel status and congestions. In general opportunistic routing has three steps:

1) Select Forwarding Candidates
2) Acknowledgements
3) Deciding whether to forward a packet

In first step transmitting node prepares a set of forwarding candidates based on shortest path and network conditions. The node which is nearer to the destination has highest priority and next nearest node has the second priority based on this the forwarding candidate set is prepared. Then the transmitting node broadcasts packets by giving forwarding candidate set in the data frame. Transmitted packets are received by number of nodes which are in the hearing radius of the transmitting node.

In next step the received nodes have to acknowledge back according to the priority given in the candidate header set. First node in the candidate header set should send acknowledgement in first time slot if it receives the packet, remaining nodes which receive packets sends acknowledgement in the time slots assigned to them. In final step received nodes have to decide whether to forward the or not. If the packet is received by the node with highest priority then it will forward the packet else next node will forward. These steps are repeated until the packet reaches the destination.

In opportunistic routing protocol the chances of forwarding the packet by same node is very less, so the path between the source and destination changes dynamically. Source location privacy is achieved by using OR since the packet follows different routes to reach the destination.

B. Energy Minimized Opportunistic Routing:

Energy Minimized Opportunistic Routing [EMOR] also makes use of the OR principles for transmitting data between source and destination. Apart from the source location privacy EMOR also address the energy minimization. As wireless nodes are powered by limited energy source efficient utilization of energy is required. There are many techniques used for efficient energy utilization of the sensor nodes, one of them is reducing the transmission power [6]. By combining the transmission power reduction technique with OR it provides better source location privacy then the existing OR and it also reduces the power consumption.

In EMOR data is transmitted with the reduced transmission power, so it takes more number of hops for packets to reach the destination. As number of hops between source and destination increases it takes more time for the adversary to trace the source, so it provides better source location privacy then the existing OR. Since the transmission power of each node is reduced life time of the node is also increases as energy consumption is reduced. The transmission power of nodes is reduced in such a way that it does not degrade the total network performance.

IV. SIMULATION RESULTS

All simulations are performed in the Network simulator-2 [NS-2] which is a discrete event network simulator for simulating the networks [5]. The topology we selected was 500 × 500 where the sensor nodes are deployed. The simulation parameters considered are listed in Table-I. Initially, the adversary is located next to the destination node. Once it detects a packet, it moves to the node which transmits that

packet. In the same time slot, the adversary may detect more than one packet, because in the opportunistic routing each packet can choose different paths to the destination node, with different number of hops. When the adversary detects multiple packets, it moves randomly to one of the transmitters.

Parameter	Set To
Channel type	Channel/Wireless Channel
MAC type	Mac/802_11
Antenna model	Antenna/OmniAntenna
Max packet in queue	50
Routing protocol	DSR/OR
X dimension of topography	500
y dimension of topography	500
Time of simulation end	150

Table 1: Simulation Parameters

Safety period is the time taken for eavesdropper to reveal the location of the source before target disappears from the monitoring area. Fig. 1 shows the safety periods of the opportunistic routing and energy minimized opportunistic routing are compared. As in the case of EMOR since transmission power is reduced it take more number of hops for the packet to reach the destination, so intruder also takes more time to trace the source. In this way EMOR performs better than the OR protocol by increasing the safety period.

In Energy minimized opportunistic routing power of transmitter is reduced so energy consumed by each node is also decreases.

Fig.1 Safety period Vs Number of Nodes

Fig. 2 shows the curves between the energy consumed by system and the number of nodes participated in the communication.

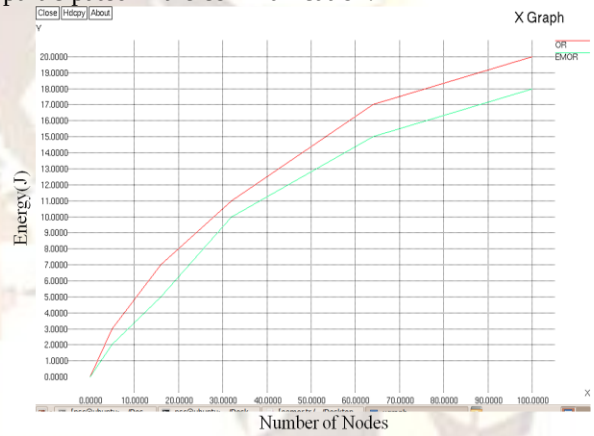

Fig. 2 Energy Vs Number of Nodes.

In Figure 2 on X-axis number of nodes is taken and on Y-axis energy is taken. From above plot it infers that EMOR consumes less energy when compared to the OR. If optimal transmission power is not correctly chosen then the energy consumption by the system will increase. The ability of the EMOR depends on the correctly choosing of the optimal transmission power. So EMOR offers better performance than OR in terms of security and energy.

V. CONCLUSION

Source-location privacy is critical to the successful deployment of many wireless sensor networks, especially in monitoring applications. In this thesis Energy minimized opportunistic protocol is proposed and simulated in extension to the opportunistic routing. The proposed Energy minimized opportunistic routing protocol provides better source location privacy than the opportunistic routing protocol and it also consumes less energy.

REFERENCES

[1] Sanjit Biswas and Robert Morris, "Opportunistic Routing in Multi-Hop Wireless Networks" In *ACM SIGCOMM* , pp. 133–144, NY, USA, Jan. 2004.

[2] Petros Spachos, Liang Song, and Dimitrios Hatzinakos, "Opportunistic Routing for Enhanced Source-Location Privacy in Wireless Sensor Networks" *IEEE Transaction on Communications*, pp. 315-318, Kingston, Canada, May 2010.

[3] P. Kamat, Yanyong Zhang, W. Trappe, and C. Ozturk, "Enhancing Source-location Privacy in Sensor Network Routing," in Distributed Computing Systems, *2005. ICDCS* 2005. *Proceedings. 25th IEEE International Conference*, pp. 599–608, Columbus, OH, June 2005.

[4] Michele Zorzi**,** and Ramesh R. Rao, "Geographic Random Forwarding (GeRaF) for adhoc and sensor networks: multi-hop performance" *IEEE Transactions on Mobile Computing*, vol. 2, no. 4, pp.337-348, Oct.-Dec. 2003

[5] David Culler, Deborah Estrin and Mani Srivastava, "Overview of Sensor Networks", *Published by the IEEE Computer Society*, vol. 37, no. 8, pp. 41-49, August-2004

[6] Dirk WESTHOFF, Joao GIRAO, and Amardeo SARMA, "Security Solutions for Wireless Sensor Networks", *Special Issue: Dependable IT and Network Technology*, vol. 3, no. 3, Nov. 2006.

[7] Liang Song and Dimitrios Hatzinakos, "Research Article: Real-Time Communications in Large-Scale Wireless Networks", *Hindawi Publishing Corporation International Journal of Digital Multimedia Broadcasting*, vol. 2008, Article ID 586067, pp. 1-17, Sep. 2008.

Sudhir chowdary.N received his B.TECH. degree in Electronics and Communication Engineering from Chaitanya Institute of Engg. & Technology, JNTUH University, India in 2009, M.TECH. degree in Communication Systems from S.R.M. University, Chennai in 2011. His research interests include wireless communications.

Siva Rama krishna received his B.TECH. degree in Electronics and Communication Engineering from Mother Teresa Institute of Science & Technology, JNTUH University, India in 2009, M.TECH. degree in Communication Systems from S.R.M. University, Chennai in 2011. He is currently working as an Assistant Professor in the Department of Electronics and Communication Engineering at SVIST Engineering College, Tiruvuru, India. Since 2011. His research interests include wireless communications, error control coding, diversity combining and MIMO.