Volume 4, Issue 5, May 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Review Paper on 4-Neighbour Parametric Route Selection Approach to Reduce Communication in Mobile Networks

Meetu Galhotra
M.Tech CSE Department
Geeta Engineering College

Shakti Nagpal
HOD, CSE Department
Geeta Engineering College

Abstract— Routing is about to generate the optimum communication path in terms of energy and distance. But in an adhoc network, the network is having limitations. It has limitations such as congestion, the attack over some particular nodes. In such case to perform the effective communication there is the requirement of some such routing approach that can provide efficient path with optimized energy and distance. To achieve this we can implement ACO based routing approach is defined to generate the intruder safe path over the network.

Keywords: Routing, ACO, Effective Communication, Intruder Safe

I. INTRODUCTION

Wireless sensor network (WSN) has gained world-wide attention in recent years. It is a sensing technology where autonomous devices called sensor nodes are deployed in a remote area to observe phenomena, collect data and process it and then transmit information to users via radio frequency (RF) channel.

Wireless sensor networks (WSNs) are self-configured and are without infrastructures. WSN collects data from the environment and sends it to a destination site where the data can be observed, memorized and analyzed.

II. ARCHITCTURE

The basic block diagram of a wireless sensor node is presented in Figure 1 It is made up four basic components: a sensing unit, a processing unit, a transceiver unit and a power unit.

There can be application dependent additional components such as a location finding system, a power generator, mobilizing system,etc.

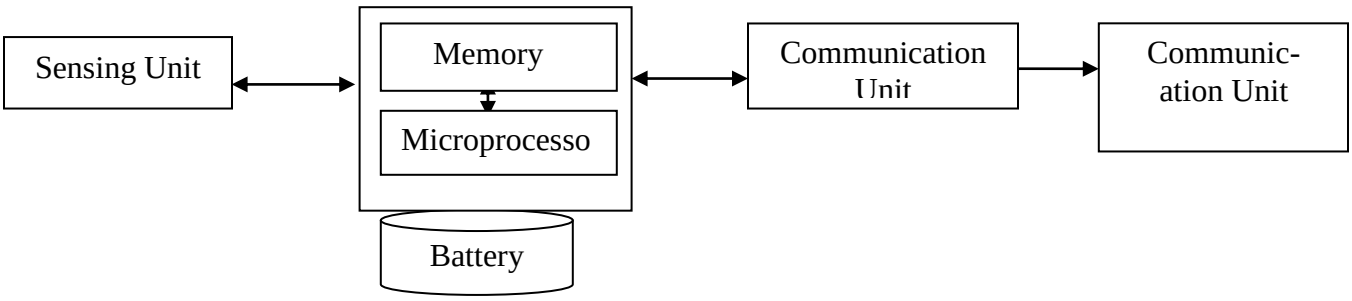

FIGURE 1 ARCHITECTURE OF WIRELESS NODE

Sensing Unit: Sensing units are usually composed of two subunits: sensors and analog to digital converters . Sensor is a device which is used to translate physical phenomena to electrical signals. Sensors can be classified as either analog or digital devices.

Processing Unit: The processing unit mainly provides intelligence to the sensor node. The processing unit consists of a microprocessor, which is responsible for control of the sensors, execution of communication protocols and signal processing algorithms on the gathered sensor data.

Transceiver Unit: The radio enables wireless communication with neighboring nodes and the outside world. It consists of a short range radio which usually has single channel at low data rate and operates at unlicensed bands of 868-870 MHz (Europe), 902-928 MHz (USA) or near 2.4 GHz (global ISM band).

Battery: The battery supplies power to the complete sensor node. It plays a vital role in determining sensor node lifetime. The amount of power drawn from a battery should be carefully monitored. Sensor nodes are generally small, light and cheap, the size of the battery is limited.

III. APPLICATIONS

Military applications: The various characteristics of Wireless sensor networks like self-organization and fault tolerance make them a very reliable sensing technique for military command, communications, computing, intelligence, surveillance and targeting system.

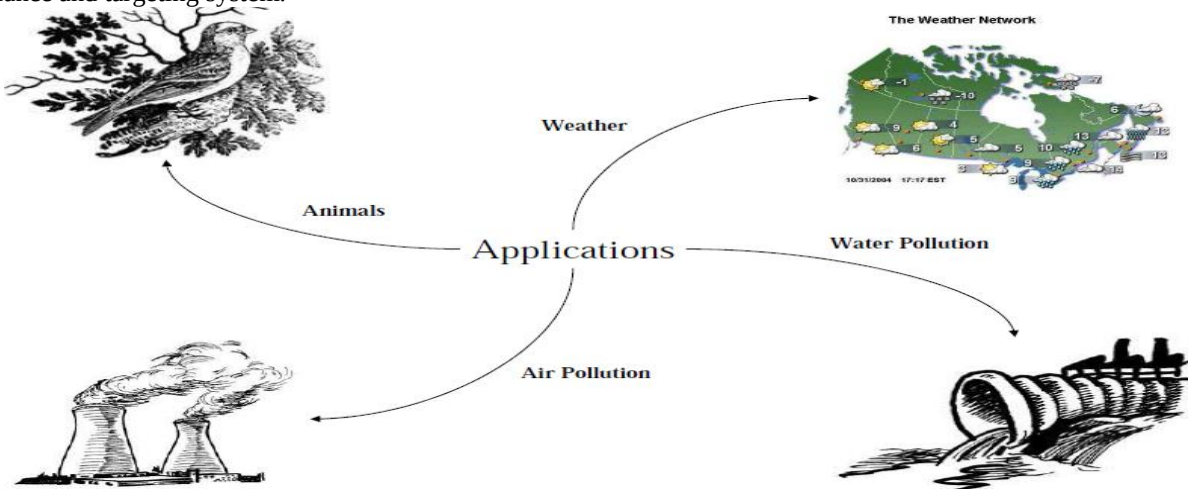

FIGURE 2 VARIOUS APPLICATIONS OF WIRELESS SENSOR NETWORKS

Military sensor networks can be used to detect and gain as much information as possible about enemy movements, explosions, and other phenomena of interest, such as battlefield surveillance, nuclear, biological and chemical attack detection.

Environmental applications: Wireless sensor networks have been deployed for environmental monitoring, which involves tracking the movements of small animals and monitoring environmental conditions that affect crops and livestock. In these applications, WIRELESS SENSOR NETWORK collect readings over time across a space large enough to exhibit significant internal variation. Each sensor node measures air temperature, relative humidity, and photo-synthetically-active solar radiation. Sensor nodes are placed at different heights of the tree. Plant biologists track changes of spatial gradients in the microclimate around a redwood tree and validate their biological theories.

Healthcare applications: WIRELESS SENSOR NETWORK based technologies such as Ambient Assisted Living and Body Sensor Networks provide dozens of solutions to healthcare's biggest challenges such as an aging population and rising healthcare costs. Body sensor networks can be used to monitor physiological data of patients The Body sensor networks can provide interfaces for disabled, integrated patient monitoring.

Traffic control: Traffic conditions can be easily monitored and controlled at peak times by WIRELESS SENSOR NETWORKs. Temporary situations such as road works and accidents can be monitored in situ. Further, the integration of monitoring and management operations, such as signpost control, is facilitated by a common WIRELESS SENSOR NETWORK infrastructure.

IV. CHALLENGES IN WIRELESS SENSOR NETWORK

Wireless Based Sensor Networks bear unique features and challenges such as sensor selection, sensing technology, networking and security design issues. Body sensors should be easy, comfortable to wear, the reliability of sensor nodes is critical in emergency situations and thus is required to be very high; the communication range is extremely short, rendering most attacks impossible or very difficult. One challenge threatening the successful deployment of sensor networks is privacy.

V. UNRELIABLE COMMUNICATION

Unreliable Transfer: Normally the packet-based routing of the sensor network is connectionless and thus inherently unreliable. Packets may get damaged due to channel errors.

Conflicts: This is due to the broadcast nature of the Wireless sensor network. If packets meet in the middle of transfer, conflicts will occur and the transfer itself will fail.

Latency: The multi-hop routing, network congestion and node processing can lead to greater latency in the network, thus making it difficult to achieve synchronization among sensor nodes

VI. SECURITY

Often, the utility of a sensor network will rely on its ability to accurately and automatically locate each sensor in the network. A sensor network designed to locate faults will need accurate location information in order to pinpoint the location of a fault. Unfortunately, an attacker can easily manipulate non-secured location information by reporting false signal strengths, replaying signals, etc.

A technique called verifiable multilateration in which, a device's position is accurately computed from a series of known reference points. In authenticated ranging and distance bounding are used to ensure accurate location of a node. Because of distance bounding, an attacking node can only increase its claimed distance from a reference point. However, to ensure location consistency, an attacking node would also have to prove that its distance from another reference point is shorter. Since it cannot do this, a node manipulating the localization protocol can be found. For large sensor networks, the SPINE (Secure Positioning for sensor Networks) algorithm is used. It is a three phase algorithm based upon verifiable multilateration.

VII. EXISTING WORK

Energy efficiency is the most important issue in all facets of Wireless sensor networks operations because of the limited and energy supply. And wireless sensor network are deployed in environments where sensors can be exposed to conditions that might interfere with the sensor readings. Moreover, a variety of sensors may be attached to wireless sensor network to monitor the environment. Data aggregation, eliminating the data redundancy and improving the accuracy of information gathering, is essential for wireless sensor network. Hence, BPNDA was proposed, a data aggregation scheme based on back-propagation network (BPN). In the BPNDA, a three-layer BP neural network was used. The input layer neurons are located in cluster members (CMs), while the hidden layer neurons and the output layer neurons are located in cluster head (CH). Only the extracted data that represented the features of the raw data will be transmitted to the sink, so the efficiency of data gathering is improved and the total energy consumption is reduced[2]. This paper an intelligent analysis is used to process the structure of a Wireless sensor network and produce some information which can be used to improve the performance of WIRELESS SENSOR NETWORK's management application. Wireless sensor networks need to be managed in different ways; e.g. power consumption of each sensor, efficient data routing without redundancy, sensing and data sending interval control, etc. The random distribution of wireless sensors, numerous variables which affect WIRELESS SENSOR NETWORK's operation and the uncertainty of different algorithms give a fuzzy nature to WIRELESS SENSOR NETWORK's. Considering this fuzzy nature and numerous details, a neural network is an ideal tool to be used to cover these details which are so hard to be explicitly discovered and modeled.

In this paper they introduce our neural network based approach which results in a more efficient routing path discovery and sensor power management. They define a set of attributes based on sensors' location and neighborhood and use them as inputs of our neural network and the output of the neural network will be used as a factor in the route path discovery and power management. They designed a simulator based on our approach and observed the effect of our method on Wireless sensor network lifetime and sensor power consumption which will be presented in this paper**[3].**

This paper describes the concept of sensor networks which has been made viable by the convergence of microelectro-mechanical systems technology, wireless communications and digital electronics. First, the sensing tasks and the potential sensor networks applications are explored, and a review of factors influencing the design of sensor networks is provided. Then, the communication architecture for sensor networks is outlined, and the algorithms and protocols developed for each layer in the literature are explored. Open research issues for the realization of sensor networks are also discussed**.[4]**

VIII. PROPOSED WORK

In this present work we have improve the routing approach by improving the existing path selection algorithm with the inclusion of Ant Optimization approach. The first step is to setup the network with specific parameters. These parameters includes

i) Number of Packets: This property represents the number of successful packet delivery for a specific communication.
ii) Number of Packet loss: Due to the congestion or any block node there are the chances of the data loss over the network. This parameter will analyze the packet loss over the transmission. It is the decision parameter that will perform the analysis the next node is a valid node or not.
iii) Packet Delivery Ratio: This parameter is basically defines the ratio of packets transmitted and the packet successfully arrived to the destination. The packet delivery ratio we have analyzed on 4 intermediate nodes to identify the problem area over the network.
iv) Time Delay: It defines the delay in the communication. The delay will occur because of congestion over the network.
v) Energy: As each node in the communication is a sensor node, because of this each node is defined with specific energy we have defined 5 Jule to each node. With each communication over the network some energy is lost. If the energy is less then minimum required energy or 0 the node will be dead itself.
vi) Turn Around Time: It is the actual time taken to perform the communication over the network.

1. Define N Number of Sensor Nodes in the WIRELESS SENSOR NETWORK with specific parameters in terms of energy, transmission rate etc.
2. Each Node Ni start Moving in Direction of Specific Direction Di
3. Find M Neighbor Nodes of Nodes Ni and Maintains the respective Information
4. Perform the Normal Communication

The description of the Ant concept is presented here

1. At regular interval any node s(Source) is selected to send data to some destination node d.
2. Each forward ant selects the next hop node using the routing table information. The next node selected depends on some random scheme. If all nodes already visited a uniform selection will be performed
3. If the selected node is some attack or damage node then the forward ant wait to turn in the low priority node from the queue.
4. It will identify any of the next non visited node and pay some delay on it.
5. If some cycle detected the ant is forced to turn on the visited node.
6. When the ant reaches the destination node a backward ant is generated to transfer all its memory.
7. Backward ant uses same path generated by forward ant.

By default route is chosen on the basis of Path selection formula and i.e. we will choose the lowest energy path. It means every time the selected path is using lowest energy. In case there is problem in the selection of the path then we apply the Ant Colony Algorithm the purpose of which is to continue sending data using the previous path.

VIII. CONCLUSION

In this work, an improved routing approach is presented that gives the effective route generation in terms of energy, distance and the bad node analysis. The approach will provide the safe path so that the effective communication is expected from the network.

REFERENCES

[1] Walters, J. P., Liang, Z., Shi, W., and Chaudhary, V., (2007) "Wireless sensor network security – A survey", Security in Distributed, Grid, Mobile, and Pervasive Computing, Auerbach Publications, CRC Press.

[2] K. Akkaya and M. Younis, "A survey on Routing Protocols for Wireless sensor networks" Ad hoc networks, 2005-Elsevier.

[3] Stephan Olariu, "Information assurance in Wireless sensor networks", Sensor network research group, Old Dominion University.

[4] Fernandes, L. L., (2007) "Introduction to Wireless sensor networks Report", University of Trento.

[5] Y.-C. Hu, A. Perrig, D.B. Johnson, Packet leashes: a defense against wormhole attacks in wireless networks, in: IEEE Infocom, 2003.

[6] Prabhudutta Mohanty, Sangram Panighari, Nityananda Sharma and S. S. Satapathy "Security issues in Wireless sensor network data gathering protocols: A Survey" Journal of Theoretical and Applied Information Technology, 2005, pp 14-27.

[7] Dimitrievski, A., Stojkoska,B, Trivodaliev, K. and Davcev, D., (2006) "Securing communication in WSN trough use of cryptography", NATO-ARW, Suceava.

[8] Chris Karlof and David Wagner "Secure routing in Wireless sensor networks: Attacks and countermeasures" Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, vol. 1, issue 2-3, pages 293–315, September 2003.

[9] Mayank Saraogi. "Security in Wireless sensor networks". In ACM SenSys, 2004.

[10] D. Ganesan, R. Govindan, S. Shenker, D. Estrin, Highly-resilient, energy-efficient multipath routing in Wireless sensor networks, Mobile Computing and Communications Review 4 (5) (2001) 11–25.

[11] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. Tygar, SPINS: security protocols for sensor networks, in: Proceedings of Mobile Networking and Computing 2001, 2001.

[12] J. N. Al-Karaki and A. E. Kamal. "Routing techniques in Wireless sensor networks: A survey". IEEE Wireless Communications, vol. 11, issue 6, pages 6–28, 2004.

[13] Prabhudutta Mohanty, Sangram Panigrahi Nityananda Sharma and Siddhartha Sankar Satapathy "Security Issues in Wireless sensor network data gathering protocol: A Survey", Journal of Theoretical and Applied Information Technology- 2010.

[14] Jian Yin and Sanjay Madria "SecRout: A Secure Routing Protocol for Sensor Networks" doi.ieeecomputersociety.org/10/1109/AINA.2006.297-314

[15] Rampur Srinath, A. Vasudev Reddy and Dr. R.Srinivasan "AC: A Cluster-based Secure Routing Protocol for WSN" Third International Conference on Networking and Services (ICNS'07) 2007.

[16] Nidal Nasser and Yunfeng Chen "Secure Multipath Routing Protocol for Wireless sensor networks" International Conference on Distributed Computing Systems Workshops, www.ieee.org

