SRDD-AD: SECURED ROUTING AND DATA DELIVERY BY ABNORMAL DETECTION IN WIRELESS SENSOR NETWORKS

Shefin.A.J[1] | R.Sujitha[2]

[1](UG Student, Christ the King Engineering College, shefinaj777@gmail.com)
[2](Assistant Professor, Christ the King Engineering College, srisuji14@gmail.com)

Abstract— *This paper focuses on the abnormal nodes detection of poisonous gas in wireless sensor networks, namely, finding these nodes whose concentrations are higher than the threshold. In order to detect abnormal nodes, we had better collect sensory data from all nodes. However, this strategy requires much more energy consumption, so we should try to wakeup these nodes near the abnormal filed. Based on this observation, we propose a novel energy efficient -- method to wake them up. The main idea is to let abnormal nodes send out control packets to activate their one-hop neighbor nodes, then neighbor nodes continue detecting, and finally, all abnormal nodes send information to the sink node through the shortest paths. Thereafter, we further propose to handle these information in the sink node, including extracting boundary nodes, drawing isolines, estimating the location of leakage source. To extract boundary nodes, we divide all abnormal nodes into different intervals in an ascending or descending order, then find two nodes with minimum and maximum in each interval, so these nodes are regarded as boundary nodes.*

1. INTRODUCTION

In recent years, we have witnessed a drastic growth in demand for multimedia services such as different styles of media streams (i.e., video, voice and data streams) and different priority classes of one traffic streams which are referred to as multiple services having different quality of service (QoS) requirements in wireless networks. Given the proliferation of smart devices in distributed intelligent networks, each node is expected to be endowed with smart autonomic functions. By instinct, the individual network nodes would prefer to act selfishly rather than altruistically in distributed network.

A distributed wireless network which consists of nodes exhibiting a selfish behavior is referred to as a distributed selfish wireless network (SeWN). In such network scenarios, the selfish behavior of network nodes, referred to as "node selfishness", may degrade the network performance, e.g., the network connectivity, the reliability of the selected path and the probability of the successful End-to-End (E2E) multiservice delivery. The node selfishness of the network node is affected by some intrinsic and extrinsic factors, such as its own energy and bandwidth resources, the QoS requirements and the employed incentive mechanisms. For improving the network performance, the node individuals need to obtain the information on the node-selfishness of the other nodes and to determine the relationship between the aforementioned factors and the node-selfishness. In such distributed network scenarios, each network node may obtain the aforementioned information, directly collected by itself and/or indirectly received from its neighboring nodes.

Accordingly, each network node should establish a distributed node-selfishness management for managing the aforementioned information on the node-selfishness, whilst improving the network performance of delivering multiservice, i.e., the reliability of the selected path and the successful probability of delivering multi-services. Many literatures have investigated the multi-service delivery in distributed wireless networks. A cross-layer resource allocation scheme was developed in for guaranteeing the QoS requirements of the voice and data traffic. A spatial-correlation aware QoS routing algorithm was proposed in for efficiently delivering visual service under QoS constraints. A geographic opportunistic routing was explored in for delivering packets with both E2E reliability and delay constraints in wireless sensor networks. The feasibility of the aforementioned schemes disregard the impact of the node-selfishness on the multi-service delivery in distributed wireless networks. Due to the effect of the node-selfishness on the network performance, some management approaches of dealing with the nodes' selfish behaviors have been studied for distributed wireless networks. A heterogeneous trust management was proposed in for evaluating the trust of a network node in terms of its social and QoS behavior.

2. RELATED WORKS

2.1 Introduction to networks

The different types of networks available today are Wired and Wireless networks. Wired are differentiated
from wireless as being wired from point to point. Each of these types of networking has their advantages and disadvantages according to security. Wired networking has different hardware requirements and the range and benefits are different. Wireless networking takes into consideration the range, mobility and the several types of hardware components needed to establish a wireless network. There are different types of configurations of networks and the

security measures that need to be taken to ensure a secure network.

Organizations rely heavily on the ability to share information throughout the organization in an efficient and productive manner. Computer networks have allowed for this technology and are now a part of almost every business. An organization has two options when it comes to setting up a network. They can use a completely wired network, which uses networking cable to connect computers, or they can use a wireless network, which uses radio frequencies to connect computer. Wireless networks have allowed organizations to become more therefore organizations are now using a combination of both wired and wireless networks.

2.2 Wired Networks

These networks are generally connected with the help of wires and cables. Generally the cables being used in this type of networks are CAT5 or CAT6 cables. The connection is usually established with the help of physical devices like Switches and Hubs in between to increase the strength of the connection. These networks are usually more efficient, less expensive and much faster than wireless networks. Once the connection is set there is a very little chance of getting disconnected. Wired networks provide users with plenty of security and the ability to move lots of data very quickly. Wired networks are typically faster than wireless networks, and they can be very affordable. A wired network is a common type of wired configuration. Most wired networks use Ethernet cables to transfer data between connected PCs. In a small wired network, a single router may be used to connect all the computers. Larger networks often involve multiple routers or switches that connect to each other.One of these devices typically connects to a cable modem, T1 line, or other type of Internet connection that provides Internet access to all devices connected to the network. Wired networks, also called Ethernet networks are the most common type of local area network (LAN) technology.

A wired network is simply a collection of two or more computers, printers and other devices linked by Ethernet cables. Ethernet is the fastest wired network protocol, with connection speeds of 10 megabits per second (Mbps) to 100 Mbps or higher. Wired networks can also be used as part of other wired and wireless networks. To connect a computer to a network with an Ethernet cable, the computer must have an Ethernet adapter (sometimes called a network interface card, or NIC). Ethernet adapters can be internal or external. Some computers include a built-in Ethernet adapter port, which eliminates the need for a separate adapter.

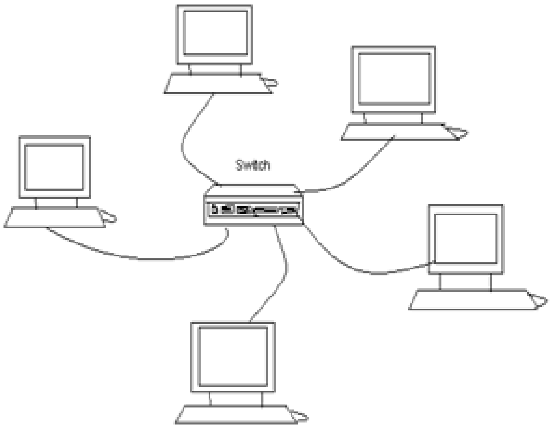

Figure 1Wired Networks

2.3 Wireless Network

Wireless networks use some sort of radio frequencies in air to transmit and receive data instead of using some physical cables. The most admiring fact in these networks is that it eliminates the need for laying out expensive cables and maintenance costs. A basic wireless network consists of multiple stations communicating with radios that broadcast in either the 2.4GHz or 5GHz band though this varies according to the locale and is also changing to enable communication in the 2.3GHz and 4.9GHz ranges. Once an access point is selected, the station needs to authenticate before it can pass data. Authentication can happen in several ways. The most common scheme, open authentication allows any station to join the network and communicate.

A desktop computer or laptop with either wireless networking support, or a network interface card (NIC). You can use either an Ethernet (wired) connection or a wireless connection from the computer to the access point. For Macintosh wireless network support is usually offered by AirPort card. A router is a device that routes data from one network to another network. A router is connected to at least two networks, commonly two networks or a network and its ISP's network. A router allows for everyone on the network to access the internet.

The next component that you will need to setup a network is a hub or sometimes a switch. A hub is a device that connects the cables from computers and other devices such as printers in a network. Traditionally, hubs are used for star topology networks, but they are often used with other configurations to make it easy to add and remove computers without bringing down the network. The difference between a hub and a switch is that a switch filters the data that passes through it and a hub does not. These components have all been modified and are capable of establishing wireless networks. A router can be purchased with wireless capability but a more efficient way of adding wireless to your network is to simply add wired access points. An access point will bride a wired network with a wireless network and can be hard wired in to your existing system.

3 .NETWORK MODEL

In this module used to initialize the nodes in network topology. We used network topology and topography for our network animator window (nam) we have syntax for create nodes in network animator window. Then we can create nodes in two types like random and fixed motions. In random motion we fixed range for X and Y, fixed particular range then the nodes are randomly generate in that range of nam window. In fixed motion we give X and Y dimension position for all nodes then all the nodes are fixed in that particular dimension. Determining the position of the nodes might be achieved using a satellite based positioning system such as global positioning system (GPS) or one of the energy-efficient localization methods proposed specifically for MANETs.

4. ROUTE DISCOVERY

Normally the source can find the route using DSR algorithm In this scheme, we are creating the fake route request. The source will generate fake request with destination address as cooperating neighbor. But incase if there is reply from any node, then that node will be identified as malicious by using the source routing mechanism. If route is failed means the intermediate node will share the error message. Based on the error message the source node will find another route to destination. The beacon generator can generate the packet and that packet can be read by any neighbor node, the beacon life is only for one hop.

5. ANONYMOUS DETECTION

This proposed which integrates the Proactive and reactive defense architectures, and randomly establishing a cooperation with adjacent node. The address of the adjacent node is used as the bait destination address, baiting malicious nodes to send RREP reply messages and identifies the malicious nodes by using the reverse tracing program. Finally the detected malicious node is

listed in the anonymous list and notifies the remaining nodes in the network to halt any communication with them. As a result, my proposed scheme can reduce packets loss that can be cause by malicious nodes and have better throughput.

REFERENCE

[1] D. ALANIS, P. BOTSINIS, S. X. NG, and L. HANZO, “Quantum-assisted routing optimization for self-organizing networks,” IEEE Access, vol. 2, pp. 614– 632, 2014.

[2] Y. Liu, J.-S. Fu, and Z. Zhang, “K-nearest neighbors tracking in wireless sensor networks with coverage holes,” Personal and Ubiquitous Computing, pp. 1–16, 2016.

[3] S. C. Tu, G. Y. Chang, J. P. Sheu, W. Li, and K. Y. Hsieh, “Scalable continuous object detection and tracking in sensor networks,” Journal of Parallel and Distributed Computing, vol. 70, no. 3, pp. 212–224, 2010.

[4] J. Zhu and Y. Zou, “Cognitive network cooperation for green cellular networks,” IEEE Access, vol. 4, pp. 849–857, 2016.

[5] B. Huang, W. Wu, and T. Zhang, “An improved connectivity based boundary detection algorithm in wireless sensor networks,” in IEEE Conference on Local Computer Networks, 332–335, 2013.

[6] K. A. M. K. Azmi, W. A. T. Wan Abdullah, and Z. Ibrahim, “Hough transform method for track finding in center drift chamber,” AIP Conference Proceedings, vol. 1704, 2016.

[7] B. Zhou and Y. He, “Fast circle detection using spatial decomposition of hough transform,” International Journal of Pattern Recognition and Artificial Intelligence, 2016.

[8] W. Cho and J. Jeon, “Edge detection in wavelet transform domain,” in The Workshop on Frontiers of Computer Vision, pp. 1–4, 2015.

[9] H. Yang, L. I. Xunbo, Z. Wang, Y. U. Wenjie, and B. Huang, “A novel sensor deployment method based on image processingand wavelet transform to optimize the surface coverage in wsns,” Chinese Journal of Electronics, vol. 25, no. 3, pp. 495–502, 2016.

[10] H. Du, Z. Huang, and J. He, “The research of image edge detection based on wavelet-transform,” Automation and Instrumentation, 2016.

[11] X. Wu, H. Chen, Y. Wang, L. Shu, and G. Liu, “Bp neural network based continuous objects distribution detection in wsns,” Wireless Networks, vol. 22, no. 6, pp. 1917–1929, 2016.

[12] F. U. Guangjie, D. Zhao, Q. Zhao, and S. Wang, “Research on detection and location system of pipeline leakage based on acoustic wave technology,” Modern Electronics Technique, 2015.