Energy Efficient With Secured Reliable Routing Protocol (EESRRP) For Mobile Ad-Hoc Networks

R.Vadivel a, V. Murali Bhaskaran b

a Assistant Professor, Department of IT, School of CSE, Bharathiar University, Coimbatore, TN, India
b Principal, Pavai College of Engineering, NH-7, Pachal, Namakkal, TN, India

Abstract

In this paper, energy efficient with secured reliable routing protocol towards mobile ad hoc networks is proposed. Residual energy metric is estimated for providing energy efficiency and improved reliability. To provide security against malicious attacks an effective intercept detection and correction (IDC) algorithm is presented. The IDC algorithm uses the residual energy estimation and traffic inspection. The traffic inspection is carried out by estimating the loss rate at a particular node. When the estimated loss rate at a particular node surpasses than the ordinary loss rate, the nodes involved will be determined as attacker nodes. Through NS2 simulations, the proposed EESRRP protocol is compared with the AODV protocol. With the simulation results it is proved that the proposed EESRRP protocol achieves better reliability along with reduced energy consumption. Also, the simulation results promises the detection of malicious nodes and improved security.

© 2011 Published by Elsevier Ltd. Selection and/or peer-review under responsibility of C3IT

Keywords: MANETs; Security; Energy Efficient; Reliability.

1. Introduction

Ad hoc wireless network is a unique wireless network lacking backbone infrastructure. Flexibility and quickly deployable characters of wireless ad hoc networks are due to this aspect. However, this property possesses major technological challenges. These challenges include issues of efficient routing, medium access, power management, security and quality of service (QoS). The nodes correspond over wireless links and so the nodes must be able to fight against the unpredictable character of wireless channels and interference from the additional transmitting nodes. Though the user required QoS in wireless ad hoc networks is achieved, these factors lead to a challenging problem in the direction of data throughput.

Either a direct link or a multi-hop route is used for the communication between source nodes and destination nodes. For this, it is necessary that all nodes should have some fundamental routing potential to make sure that packets are delivered to their relevant destinations [12]. While implementing ad hoc...
networks, huge complications occur due to the frequent route changes, which is due to the mobility of the nodes and intrusion between nodes.

1.1. Failures in Routing

Maximizing the data packet delivery in the face of fast changing network topology devoid of incurring a large routing overhead is the major issue in mobile ad hoc networks. The packet delivery ratio can be reduced by slow detection of broken links which causes the data packets to be forwarded to stale or invalid paths.

The main reason for packet loss in ad hoc networks is the link failure or node failure which is due to energy draining in nodes. A link failure is caused if there is more than one packet using this link after the physical layer failure. Though after a failure, the routing protocol takes off such packets from the queue, new packets still keep coming into the queue without any checking. If the new incoming packets make use of the failed link, then they will block all other packets resulting in network wide low throughput and long delay [1]. Detection of link failures in an ad hoc network becomes challenging due to the lack of centralized monitoring and management point. This makes the faulty nodes to remain long time in the network, which affects the performance of routing in the ad hoc network. For instance, if a defective node participating in the routing process drops data packets, subsequently a large number of packets will be lost [2].

In order to increase the reliability, it is needed to distinguish and moderate the failures. By knowing individual link stability along a path by calculating the node remaining energy, path stability can be identified. This can be done by means of estimating the node remaining energy.

Also securing the ad hoc networks plays an important role. For security there are algorithms which is consuming high overhead of packets and much computing time. Hence, a security mechanism is needed which consumes less overhead and reduced computation time. This paper provides an adaptive security algorithm called as Intercept detection and correction (IDC) which identifies the malicious data forwarding through the network from source, intermediate and destination nodes.

2. Related Works

Wesam AlMobaideen [3] has presented a Stability-based Partially Disjoint AOMDV (SPDA) protocol which is a modification of the AOMDV protocol. His SPDA finds partially disjoint paths based on links stability. His idea is that accepting partially disjointed paths that are more stable than other maximally disjoint ones could increase paths lifetime. This in turn improves MANET performance in terms of delay, routing packets overhead, and the network throughput.

Kambiz Homayounfar [4] has described an algorithm that helps MANET routing in two ways. First, it provides a metric that by its nature warns of the possibility that links can break. This metric, which can be considered a link stability index, accumulates at each node to form a path stability index. Therefore, his algorithm enables intermediate nodes to balance stability of the route with end-to-end delay. His principle is that intermediate nodes must wait before they re-broadcast a request they just picked up from a neighbor. This waiting mechanism has, in turn, two advantages. First, in case a better link comes along, there is no need for re-broadcast. This reduces overhead of redundant broadcasts. Second, by using a simple waiting mechanism that depends on link stability, end-to-end delay reduces.

Ming Yu et al [5] have proposed a link availability-based QoS-aware (LABQ) routing protocol for mobile ad hoc networks based on mobility prediction and link quality measurement, in addition to energy consumption estimation. Their goal is to provide highly reliable and better communication links with energy-efficiency. To consider the impact of the node mobility on the links, in stead of directly predicting the mobility patterns of mobile links, they incorporated link availability into routing metrics so that links
predicted to have higher availability will be more likely to be chosen. Also to consider the impact of the mobility on the link quality, they proposed the ETX as link quality metric and also incorporate it into routing metrics. Thus, their routing metric consist of link availability and quality in addition to power consumption, which is for energy efficiency.

In [6], the authors propose a scheme that randomly selects part of the intermediate nodes along a forwarding path as checkpoint nodes which are responsible for generating acknowledgments for each packet received. If suspicious behavior is detected, it will generate an alarm packet and deliver it to source node. Some of the key disadvantages of the scheme are: (1) The algorithm suffers from high overhead because for each received packet the intermediate nodes need to send an acknowledgment back to the source node; (2) The algorithm assumes that the channel is perfect and any packet loss is due to the presence of malicious nodes.

In [7], the authors present a game theoretic analysis of securing cooperative ad hoc networks against insider attacks in the presence of noise and imperfect monitoring. Several secure routing protocols resilient to external attacks, such as SAODV [8], SEAD [9], ARAN [10] and Ariadne [11], were proposed. However, none of these protocols are capable in defending against internal attacks.

3. Energy Efficient With Secured Reliable Routing Protocol (EESRRP) for MANET

Our EESRRP is having two distinct methodologies (1) To calculate residual energy in nodes (2) a intercept detection and correction (IDC) algorithm to effectively recognize the selective forwarding misbehavior from the normal channel losses with the help of the residual energy parameter.

3.1. Calculating Residual Energy in Nodes

It is assumed that all nodes are equipped with a residual power detection device and know their physical node position. The packet transmitting energy for a packet can be computed as

$$\text{Energy}_{tx} = \frac{P_{size} \times \text{Power}_{tx}}{\text{LBW}}$$  \hspace{1cm} (1)

where $P_{size}$ is the data packet size, $\text{Power}_{tx}$ is the packet transmitting power and LBW is the wireless link bandwidth. When a mobile node performs power control during packet transmission, the transmitting energy for one packet relative to the node distance is given as

$$\text{Energy}_{tx} = kd^{\alpha}$$  \hspace{1cm} (2)

where $k$ is the proportionality constant, $d$ is the distance between the two neighboring nodes, and $\alpha$ is a parameter that depends on the physical environment (generally between 2 and 4). The shorter distance between the transmitter and the receiver, the smaller amount of energy required. At each node, the total required energy is given by

$$\text{Energy}_{tot} = p \times (\text{Energy}_{tx} + \text{Energy}_{pro})$$  \hspace{1cm} (3)

where $p$ is the number of packets. The energy required for packet processing ($\text{Energy}_{pro}$) is much smaller than that required for packet transmitting. The node remaining energy or the residual energy is the energy left after the packet transmission (i.e.) residual energy $\text{Energy}_{res}$ is given by

$$\text{Energy}_{res} = \text{Energy}_{initial} - \text{Energy}_{tot}$$  \hspace{1cm} (4)
3.2. The Intercept Detection and Correction (IDC) Algorithm

This section discusses about the working of IDC algorithm in brief. The above section focused on estimation of residual energy. The residual energy is estimated when the source node tries to create a connection with the intermediate node. The core concept of IDC is briefed as follows. Each intermediate node along a given route Ri implements both the downstream and upstream traffic inspection. Downstream traffic inspection is observing the activities of its downstream node R_{i+1} to decide if the node is misbehaving. The term “misbehaving” refers when the node is dropping or tampering the data packets. Upstream traffic examining is monitoring the behavior of its upstream node R_{i-1}. These monitoring by node R_i are then put into comparison with the upstream/downstream detection thresholds to find misbehaviors. The threshold value is computed by assigning the number of packets sent to the intermediate node by the source node. The key advantages of the proposed IDC algorithm are (i) the upstream and downstream nodes are examining the neighboring node’s behavior and calculating the residual energy of the neighboring nodes. (ii) Usually in mobile ad hoc networks when the topology changes, the threshold values are dynamically attuned with the normal loss rates in order to maintain the detection accuracy. For a node R_i in a forwarding route, it is referred to R_{i-1} as its upstream node and R_{i+1} as its downstream nodes. The IDC algorithm uses INSPECT packet and INSPECT_ACK packet.

\[
Th = \frac{n_t + n_d}{n_f} \quad (5)
\]

Where Th denotes the threshold, n_t denote number of packets tampered and n_d denote the number of packets dropped by the downstream node. n_f denotes the total number of packets transferred to the downstream node.

4. Result and Discussions

![Fig.1 Reliability](image1)

![Fig.2 Energy](image2)
Acknowledgements

The first author thanks UGC for granting fund for Minor Research Project Grant No: 39-947/2010 (SR). The first author also thanks Manonmaniam Sundaranar University for providing opportunity to do Doctoral Research. The second author thanks Manonmaniam Sundaranar University for authorizing as Research Supervisor towards Doctoral Research.

References