Ad Hoc Networks 37 (2016) 209–227

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

A secure and energy-efficient stochastic multipath routing for self-organized mobile ad hoc networks

Sajal Sarkar [a,*], Raja Datta [b]

[a] Cyber Security-NTAMC, Power Grid Corporation of India Limited (POWERGRID), Gurgaon, Haryana, India-122 001
[b] Department of Electronics and Electrical Communication Engineering, Indian Institute of Technology, Kharagpur, India-721 302

ARTICLE INFO

Article history:
Received 18 December 2014
Revised 22 July 2015
Accepted 27 August 2015
Available online 4 September 2015

Keywords:
MANET
Multipath routing
Stochastic routing
Security
Approximation
Convergence

ABSTRACT

A wireless mobile ad hoc network (MANET) is an autonomous system of mobile nodes connected by wireless links. MANET is infrastructureless and dynamic in nature. As the nodes have limited battery power and communicate through shared wireless channel, it is hard to design a secure and energy efficient routing protocol in a MANET. In this paper[1], we propose a secure and energy-efficient stochastic multipath routing protocol based on a Markov chain for mobile ad-hoc networks (MANETs). The proposed routing protocol computes multiple paths between source– destination pairs and selects an energy-efficient path stochastically from those paths to forward the data packets. In addition, this protocol also secures data flow in the network as the packets are forwarded through random paths from the source node to the destination node. The random data flow paths make it difficult to jam, intercept, and hijack data packets as this will require the attacker to listen to all possible paths from the source to the destination. The performance analysis and numerical results show that our proposed protocol achieves significant performance gains in terms of energy consumption, delay, throughput, and security of routing protocols.

1. Introduction

Mobile ad-hoc network (MANET) can be installed easily and it is an economically feasible communication media for various applications. Although MANETs can easily be installed, the nodes of MANETs have limited battery power and it cannot efficiently serve the purpose of sensing and processing data during communications once the onboard battery power of the constituent nodes get exhausted. Therefore, it is necessary that the network utilizes its nodes' battery power efficiently. MANETs also have to be more secure for its applications as they take part in highly sensitive information transactions. However, being energy-efficient and secure at the same time is difficult as most existing security schemes are computationally intensive. On the other hand, MANETs used for surveillance and combat operations have brought about the need for a large amount of sensitive message transaction between command centers and the edge of the tactical communication networks [1,2]. These have necessitated the design and development of secure and energy efficient routing protocols for MANETs. Therefore, the routing protocols should be designed in such a way that they can counter popular attacks like jamming, intercepting, and hijacking of data in the network.

In order to ensure secure routing in MANETs, cryptographic approaches [3,4], trust based security mechanisms

* Corresponding author. Tel.: +91 8527990209.
E-mail addresses: sajals@ece.iitkgp.ernet.in, sarkar.sajal@gmail.com (S. Sarkar), rajadatta@ece.iitkgp.ernet.in (R. Datta).

[1] This paper has been presented in part at IEEE 20th NCC'14, Kanpur, India, February 2014.

http://dx.doi.org/10.1016/j.adhoc.2015.08.020
1570-8705/

[5,6], pricing-based methods [7,8] and game theoretic approaches [9,10] have been proposed in the past few years. The cryptographic approaches are usually computationally intensive and therefore difficult to implement in MANETs. The trust based mechanisms are application specific and not generic to be used in any kind of MANETs. These approaches demand trusted or tamper proof hardware in every node of a MANET. A few Game theoretic approaches have been introduced for strategic interactions among the nodes under a mathematical model. Game theoretic based security, defense mechanisms and decision making schemes may be used in the resource constrained networks. However, the performance of these techniques degrades when applied to an unfriendly MANET's environment and also when the attackers are adaptive in nature.

We investigated and found that in ad hoc networks stochasticity in routing can be a good solution for making data paths secure and at the same time energy efficient. Stochastic routing is a mechanism that can be used to select the next hop in a path according to a probability distribution. This routing scheme can also secure the routing path as it explores multiple neighbor nodes for selecting the next hop in a path thereby forcing packets to use paths randomly [11]. In order to utilize the benefits of stochastic routing, various approaches have been proposed in the literature [11–14]. A Markov chain based framework is developed in [12] for balancing the network load and studying the routing performance in wireless sensor networks. The convergence of the framework is highly questionable while the network is very dense. The authors of [13] suggested a stochastic semidefinite programming to deal with the location uncertainty of the nodes and obtain a clear understanding of tradeoff between message passing overhead and latency in the route discovery process. In [14], using a probabilistic local broadcast transmission model, the authors have showed that an index policy is not only optimal for stochastic routing but is also optimal for control transmission in an ad hoc network. Though all these works have utilized the stochastic routing to optimize the performance of routing in network, we investigated and found that it can also be used to ensure the routing security at the same time.

An optimal centralized stochastic routing algorithm for randomly duty-cycled wireless sensor network is proposed in [15]. However, the downside of this scheme is its centralized approach, which is inefficient in MANETs. In [16–19] modeling and optimization frameworks of stochastic routing is introduced for wireless multihop networks. An optimality criteria for routing decision in the network is defined in [16] and [17] by evolving a Markov chain based on the probability matrix whose entry is the packet delivery ratios of individual nodes. Similarly, the authors of [18] present a robust stochastic routing and scheduling technique so as to optimize the utility of a social network. In [19], the author presents a scheme where a node selects a neighbor to forward a packet according to a probability distribution in a stochastic routing framework. A distributed queue power aware and subband allocation design issue for a delay-optimal OFDMA uplink systems have been addressed in [20] and [21]. Here, the authors have modeled the problem as a multi-dimensional infinite horizon average reward Markov Decision Problem (MDP), where the control actions are assumed to be a function of the instantaneous Channel State Information (CSI) and the joint Queue State Information (QSI). The authors propose an online value iteration to solve the MDP by using stochastic approximation. Although the above mentioned approaches can ensure the randomness and hop selection decision for one hop distance in case of static networks, these approaches are not suitable in dynamic self-organized MANETs where data packets need to travel multiple hops to reach a desired destination.

In addition to securing the source– destination route, routing protocols should also be energy-efficient. A number of energy-efficient routing approaches have been proposed in the literature [22–28]. The protocols proposed in these papers search for the most energy-efficient path from source to destination node. A multipath routing protocol for mobile ad hoc networks, called MMRE-AOMDV based on AOMDV [33] has been proposed in [29]. The protocol finds the minimal nodal residual energy of paths and sorts these multiple paths by descending order based on nodal residual energy. Whenever a new path with greater nodal residual energy emerges, it reselects the new path to forward the rest of data packets. To maximize the network lifetime, the protocols in [30] and [31] attempted to balance the remaining battery-power at each node while searching for an energy-efficient path. We find that the authors of [23] and [24] have considered energy consumption of individual nodes while improving the throughput of the networks. On the other hand in [25] and [26] the nodes' residual energy has taken into account to provide energy-efficient MANET's environment. Most of the existing energy-efficient schemes modify the on-demand routing protocols like AODV [32] or AOMDV [33]. These protocols select a routing path deterministically and consider only energy consumption at the intermediate nodes. Moreover, these works may not perform well in presence of data flow attacks such as jamming, intercepting, and hijacking.

Although stochastic routing schemes can significantly increase the performance gains in multihop wireless networks, most of the existing schemes do not consider energy-efficiency of the routing techniques and very few of them have been designed specifically for mobile ad hoc networks. Further, to the best of our knowledge, stochastic routing for energy efficiency as well as secure routing has not been suggested in mobile ad hoc networks before. We have investigated this aspect and found that during transfer of data from a source to a destination, selection of a proper path is of utmost importance. A good path is necessary to optimize energy consumption, ensure secure delivery of data packets and to balance the load of the intermediate nodes of a MANET. Thus, in this paper we propose a stochastic multipath routing scheme for MANETs based on a Markov chain model to try and achieve all the above objectives. Our proposed protocol first establishes a set of paths between a source– destination pair. Thereafter, in each slot of a routing stage, an energy-efficient path is stochastically chosen from the set of the already established paths. We find that when the data packets are routed through these chosen paths at different time slots, the overall performance with regard to throughput and energy-efficiency improves. The main contributions of this work are as follows: