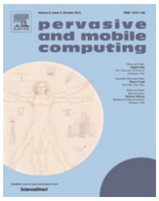
Contents lists available at ScienceDirect

Pervasive and Mobile Computing

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



Fast track article

A game theoretic framework for stochastic multipath routing in self-organized MANETs

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

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

ARTICLE INFO

Article history:
Received 16 February 2016
Received in revised form 22 June 2016
Accepted 12 September 2016
Available online xxxx

Keywords:
MANET
Stochastic game
Security
Zero-sum game
Reinforcement learning

ABSTRACT

In this paper we propose a game theoretic framework for stochastic multipath routing in mobile ad hoc networks (MANETs). In a MANET, intelligent and adaptive attackers may try to hijack, jam or intercept data packets traveling from source to destination. In our proposed game, at each stage the source node keeps track of the available multiple paths, the residual bandwidth of the paths and the strategy of the attackers from the information gathered during the previous stage. Based on these observations, the source node selects a path for data communication and switching strategy among the multiple established paths between the source node and the destination node. Accordingly, it selects an optimal routing strategy to send data packets to the destination at each stage of the game. Using minimax-Q learning, the selected routing strategy maximizes the expected sum of per stage discounted payoff, which is the utilization of residual bandwidth between a source–destination pair along with the probability that the path is safe. Performance analysis and numerical results show that our proposed scheme achieves significant performance gains in terms of residual bandwidth utilization, average end-to-end delay, packet delivery ratio, routing overhead and security.

1. Introduction

Nowadays sensitive and confidential data are required to be transferred within mobile ad hoc networks due to its wide spread applications in different areas, specifically in military and health monitoring. Therefore, it is necessary that a cooperative and appropriate environment prevails among the nodes of a MANET. We find that it is a challenging task to design routing strategies in these types of networks that include design of counter mechanisms so that attacks by highly intelligent and adaptable adversaries can be thwarted without loading the nodes with much computational complexities. Although MANETs can be installed in a hostile environment, it has to be made adaptable to its dynamic topology and constrained battery power. Further, MANET nodes have to be protected against security threats and problems arising out of shared wireless bandwidth.

In order to improve security and performance of the routing protocols in MANETs, various approaches have been proposed over the past decade. These include cryptographic approaches [1–3], trust based security mechanisms [4–8], pricing-based methods [9,10] and game theoretic approaches [11–20].

In a game theoretic approach, generally a strategic interaction technique is introduced among the nodes under a mathematical model. The game model of [12,13] designs an efficient self-enforcing distributed framework to derive well-defined

[*] Corresponding author.
E-mail addresses: sajals@ece.iitkgp.ernet.in (S. Sarkar), rajadatta@ece.iitkgp.ernet.in (R. Datta).

http://dx.doi.org/10.1016/j.pmcj.2016.09.008
1574-1192/© 2016 Elsevier B.V. All rights reserved.

equilibrium criteria for measuring the optimality of game outcomes in various network scenarios. In [14–17] the authors developed game models for cooperation and strategic interaction among the nodes of a network without considering any adaptive attacking strategy of the attackers. The authors of [18–21] suggested game theoretic based security, defense mechanisms and decision making schemes for 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.

The paper [9] proposed path variation scheme to meet its goals in a cost-efficient and incentive compatible routing. Again utilizing a similar path variation technique, the paper [22] predetermined the pricing and routing protocols in a static network scenario. To encourage packet-forwarding through multiple paths in a MANET, router-based auction approaches are also available in the literature [9,23]. In these techniques, each router constitutes an auction market for submitting bids to the source node. A sender-centric auction method utilizing path variation scheme for cost-efficient and truthful routing in MANETs has been proposed in [9]. Here, an incentive compatible property is considered to ensure truthful routing among the nodes.

A generalized two-hop relay protocol for packet routing with limited packet redundancy has been proposed in [24,23]. The authors of [24] have proposed a theoretical framework based on a Markov chain model to show how the mean value and variance of delay in packet delivery vary with other parameters. Here, issues likes medium contention, interference and traffic contentions are carefully incorporated into the analysis. In [23] the authors propose a forwarding game among the nodes, where each node individually decides a probability to deliver its own traffic and helps to forward other traffic with a probability while its payoff is the achievable throughput capacity of its own traffic.

A novel channel adaptive routing protocol is proposed in [25] extending the Ad hoc On-Demand Multipath Distance Vector (AOMDV) [26] routing protocol to accommodate channel fading. The proposed Channel-Aware AOMDV (CA-AOMDV) uses a channel average non fading duration as its routing metric to select stable links during path discovery. It then applies a preemptive handoff strategy to maintain reliable connections by exploiting channel state information. Using the same information paths can be reused when they become available again rather than being discarded. A Markov Chain based stochastic multipath routing protocol is proposed in [27,28] for MANETs. The proposed stochastic routing protocol constructs multiple paths between a source–destination pair and then it selects an energy-efficient path stochastically from the multiple paths to forward the data packets energy-efficiently. At each stage of the stochastic routing, data packets are transferred via multiple paths from source to destination stochastically. As a result, data flow is secured from jamming, intercepting and hijacking attacks. Although the performance analysis of the stochastic multipath routing protocol shows that the protocol achieves significant performance gains, the performance can be improved further if the data routing strategy is adaptive with respect to the attacking strategy of the adaptive and intelligent attackers.

Most of the work in the literature have assumed that selfish nodes and attackers adopt a fixed strategy while attacking other nodes and links in an ad hoc network. For efficient spectrum utilization, the authors of [15] considered adaptive attacking strategy of the attackers in a cognitive radio network using game theoretic infrastructure. In this infrastructure, the primary users along with the secondary users and the attackers try to access the spectrum of a network. The secondary users and attackers can access the spectrum when only the primary users are not doing so. Here, the spectrum utilization is controlled solely by the primary users here. On the other hand, in a MANET the users and nodes are more vulnerable because of its highly mobile environment and also due to the absence of a centralized controlled access patterns of the mobile nodes. Therefore, we have investigated and found that if the data routing scheme is adaptive and can counter the attacking strategy of the intelligent attackers, the routing performance and security may be improved considerably. Further, selection of the best routing path adaptively is of utmost importance to balance the load of mobile nodes and ensure secure delivery of data packets in a MANET. In this paper we propose a stochastic multipath routing scheme for MANETs based on a game theoretic framework to fulfill the above mentioned objectives. Our proposed routing scheme first establishes multiple paths between a source–destination pair based on multiple routing metrics. In each and every slot of the routing game, a path is stochastically chosen from the constructed multiple paths. Through simulation we find that the overall performance of routing protocol improves considerably in terms of bandwidth utilization, end-to-end delay, routing overhead and packet delivery ratio. Further, it also ensures data routing security while the data packets are routed through the chosen paths stochastically in different time slots of the routing game. The main contributions of this work are as follows:

- We propose a routing scheme that establishes multiple paths based on multiple routing metrics between a source–destination pair.
- The data routing problem is modeled as a non-cooperative zero-sum stochastic multipath discrete time routing game for strategic and dynamic interactions between the source node and the attackers in a mobile ad hoc network.
- The *path variation* and *time variation* at different stages of the proposed routing game are used to counter the attacks for ensuring reliable data flow in MANETs. The actions of a source node, the residual bandwidth of the links between two nodes and observation of the attackers' actions are used as the states of the routing game.
- The payoff of the game is the bandwidth utilization of a path from source to destination and is determined in each discrete time slot. More specifically it is the expected achievable residual bandwidth of the available multiple paths between a source–destination pair in a MANET along with the probability that the path is safe.
- An optimal stochastic approximation is used to determine the value function for an optimal routing strategy. Specifically, minimax-Q learning is used to select an optimal routing strategy for maximizing the expected sum of per stage discounted payoff.