Computers and Electrical Engineering 41 (2015) 301–313

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

Enhancing secure routing in Mobile Ad Hoc Networks using a Dynamic Bayesian Signalling Game model ☆

M. Kaliappan [a,*], B. Paramasivan [b]

[a] Department of Information Technology, National Engineering College, Kovilpatti, Tamil Nadu 628503, India
[b] Department of Computer Science and Engineering, National Engineering College, Kovilpatti, Tamil Nadu 628503, India

ARTICLE INFO

Article history:
Received 25 April 2014
Received in revised form 28 November 2014
Accepted 28 November 2014
Available online 22 December 2014

Keywords:
Belief updating system
Dynamic Bayesian Signalling Game
Mobile Ad Hoc Networks
Secure routing
Vulnerabilities

ABSTRACT

Collaboration between mobile nodes is significant in Mobile Ad Hoc Networks (MANETs). The great challenges of MANETs are their vulnerabilities to various security attacks. Because of the lack of centralized administration, secure routing is challenging in MANETs. Effective secure routing is quite essential to protect nodes from anonymous behaviours. Game theory is currently employed as a tool to analyse, formulate and solve selfishness issues in MANETs. This work uses a Dynamic Bayesian Signalling Game to analyse strategy profiles for regular and malicious nodes. We calculate the Payoff to nodes for motivating the particular nodes involved in misbehaviour. Regular nodes monitor continuously to evaluate their neighbours by using the belief evaluation and belief updating system of the Bayes rule. Simulation results show that the proposed scheme could significantly minimize the misbehaving activities of malicious nodes and thereby enhance secure routing.

1. Introduction

The characteristics of MANETs pose great challenges with respect to security design because of their dynamic network topologies, lack of centralized control and self organizing character. Collaboration between MANET nodes is the most problematic issue for forwarding packets among nodes. Each node can forward data packets for other nodes. This makes it difficult to design secure routing. Secure routing plays a vital role in forwarding packets in critical applications. Node mobility creates more opportunities for various security attacks in any network; because of node mobility, cooperation between nodes is more challenging in MANETs. Therefore it is essential to develop an effective secure routing protocol to protect the nodes from anonymous behaviours. In general, malicious nodes do not want to forward a neighbour's packets in networks that degrade the network performance. Existing schemes are not suitable for enhancing MANET security because of routing overhead and vulnerabilities. To minimize the activities of malicious nodes, they should be monitored continuously and not allowed to participate in routing. Game theory approaches ([1]) provide effective solutions to security problems in MANETs; they prevent conflict in cooperation among the mobile nodes. They apply to a variety of disciplines including computer networks, economics, behavioural biology and political science as well. A Dynamic Bayesian Signalling Game allows a player with a number of possible actions to have a clear strategy for making an effective decision. In each

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Associate Editor Dr. Mubashir Rehmani.
* Corresponding author. Tel.: +91 9003613335.
E-mail addresses: kalsrajan@yahoo.co.in (M. Kaliappan), bparamasivan@yahoo.co.in (B. Paramasivan).

http://dx.doi.org/10.1016/j.compeleceng.2014.11.011
0045-7906/

message set, the sender with a strategy must have a belief as to which node should receive it to ensure secure MANET routing.

Various methods have been described for preventing nodes from attacks. Daojing et al. [2] proposed a Secure and Distributed Reprogramming Protocol (SDRP). It used an identity based cryptography mechanism to enhance security for reprogramming in wireless sensor networks. It did not provide confidentiality against message interception. Feng Li et al. [3] proposed a Game Theoretic Based Analysis (GTBA) of cooperation between regular (normal) and malicious nodes in MANETs. In this approach, selfish nodes are motivated by building a reputation system. GTBA does not take multiple attacks into consideration. Ze Li and Haiying Shen [4] used game theoretic approaches to analyse cooperation incentives for nodes provided by reputation systems and price-based systems. They addressed the issues of enforcing cooperation among selfish nodes and discriminating malicious nodes from regular nodes. This scheme does not sufficiently address security problems such as compromised cooperative nodes.

We propose a protocol, enhancing secure routing for Mobile Ad Hoc Networks, that uses a Dynamic Bayesian Signalling Game model (SRPDBG); its goal is to analyse the strategy profile for regular and malicious nodes. Differently from the above methods, this work reveals the best actions of individual strategy for each node. The contributions of this work are summarized as follows:

- First, we formulate a two player Dynamic Bayesian Signalling Game for the sender and receiver.
- To find the best outcome of the strategic interaction between sender and receiver, three Nash Equilibrium strategies are analysed: Pure Strategy with Nash Equilibrium, Mixed Strategy with Nash Equilibrium and PBE with Bayesian Nash Equilibrium.
- We then calculate the payoff for nodes for motivating the particular nodes that are misbehaving.
- A belief update of each node is determined based on the Bayes rule in terms of action chosen, message sent and strategy chosen based on the probability of the node's type.
- We design an algorithm for finding belief-strategy pairs for the PBE strategy and the best response strategy for players.
- Through extensive simulation results, we evaluate the performance of the proposed SRPDBG. The results show that the SRPDBG outperforms other strategies in analysing the malicious node's behaviour and also in evaluating the strategies of regular and malicious nodes.

The remainder of the paper contains eight sections. Section 2 summarizes related work and highlights the differences between it and our work. Section 3 describes our Dynamic Bayesian Signalling Game in MANETs in terms of payoff formulation and analysis of three Nash Equilibrium Strategies: the Pure Strategy with Nash Equilibrium, the Mixed Strategy with Nash Equilibrium and the PBE with Bayesian Nash Equilibrium and payoff calculation. Section 4 presents the Belief update mechanism based on the Bayes rule. Section 5 describes our algorithm for finding the Belief strategy pairs for the PBE strategy and finds the best response strategy for players. Section 6 presents our simulation results and a relevant performance analysis. Finally, Sections 7 and 8 presents our conclusions and discusses future direction.

2. Related work

Security in MANETs is a challenge for several applications. Game theory plays significant role in providing security in MANETs. Roy et al. [5] surveyed the impact of the game theoretic approaches and their applications to network security. They presented a taxonomy of game theoretic solutions to various security problems. Manshaei et al. [6] addressed the various research approaches in applying game theoretic methods to MANET network security. Several such approaches have been developed, such as providing a Certainty Oriented Reputation System [7], preventing Selfish and Tariff Free nodes [8], analysing the cooperation incentives for individual nodes [9], detecting misbehaving nodes [10], investigating the interactions between nodes and providing incentives for good behaviour [11] and using a reputation system to enforce node cooperation. Buchegger et al. [12] presented reputation systems to reveal the truth about other nodes based on reputation ratings and trust ratings.

Mohammed et al. [13] proposed a mechanism design theory to provide incentives for encouraging nodes to participate honestly in a cluster process. The incentives are based on the Vickrey, Clarke, and Groves technique that ensures that truth-telling is the dominant strategy for any node in the clusters. It causes routing overhead as the cluster size increases. Nabil El-Kadhi and Hazem El-Gendy [14] proposed a bidirectional authentication scheme in which authentication is considered to be a non-cooperative non-zero sum bi-matrix game for Bluetooth devices. This mechanism alerts trusted Bluetooth devices of possible threats and malicious devices. This scheme is suitable only for short-range communication devices and not scalable to long-range devices. Nguyen et al. [15] introduced a secure many-to-many routing protocol for wireless sensor and actuator networks for providing both security and power efficiency. Security is achieved by using authenticated broadcast for task registration and secure multicast for data transmission. Power efficiency drives from multicast nature of the communication. Lin et al. [16] proposed a Role-Based Privacy Aware secure routing protocol to ensure privacy of information in Wireless Mesh Networks. It combines a dynamic reputation scheme with role based multilevel security and a hierarchical key-management protocol to protect the nodes against internal attacks. The dynamic reputation scheme can not always