Ad Hoc Networks 8 (2010) 181–192

Contents lists available at ScienceDirect

Ad Hoc Networks

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

A protocol for data availability in Mobile Ad-Hoc Networks in the presence of insider attacks

E. Ayday *, F. Fekri

School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332, USA

ARTICLE INFO

Article history:
Received 31 December 2008
Received in revised form 9 June 2009
Accepted 10 July 2009
Available online 17 July 2009

Keywords:
Trust
Reputation
Security
Game theory

ABSTRACT

In Mobile Ad-Hoc Networks (MANETs), establishing trust relationships between the nodes in a decentralized fashion has been an important research issue for a long time. If the sender nodes accurately identify the legitimate nodes in the network, a robust routing can be provided while mitigating the effects of malicious nodes. Further, there is always a mutual interaction between a sender and its neighbor nodes during the communication. This mutual interaction can be easily modeled as a game between two or more players (one player being the sender and the rest being the receivers). Regardless of its type (legitimate or malicious), each player attempts to maximize its benefit during the game by choosing an optimal strategy. In this paper, we propose a secure and robust routing scheme in which the interaction between the sender and receiver nodes is modeled using a dynamic Bayesian game model. A repeated game is considered and opinions of a node about the types of other nodes is established using an acknowledgement mechanism from the destination. The proposed method uses the intersection of game theory, trust establishment and coding theory to resist colluding Byzantine (insider) attacks. The scheme guarantees the availability of message as long as a legitimate path exists. Through simulations we will show the efficiency of the scheme with respect to latency, availability and energy consumption in the presence of adversary.

Published by Elsevier B.V.

1. Introduction

Mobile Ad-Hoc Networks (MANETs) play key roles in many military and civilian applications such as battlefields, environment monitoring and emergency response. The lack of infrastructure in MANETs requires the network nodes to implement the network tasks by themselves. Hence, network operation is based on the cooperation of nodes within neighborhood. For routing, intermediate nodes are used to forward a packet from a source to a destination node. Therefore, security becomes a challenging problem in this multihop environment with unreliable intermediate nodes.

The main threat for routing in a MANET is the existence of selfish and malicious nodes. The goal of a selfish node is to maximize its own welfare, on the other hand a malicious node tries to prevent the network from operating efficiently or properly. Without any countermeasures against these threats, the network performance decreases considerably.

We propose a secure and efficient routing scheme using a game theoretical approach and trust relationships between the nodes. We assume a "Dynamic Bayesian Game" model [1] among the nodes to find the optimal strategies of legitimate and malicious nodes. Moreover, using the "watchdog" technique [2] and the "acknowledgement" mechanism (ACK), we construct trust relationships between the nodes. Recent works [2–10] either do not consider the malicious nodes or build the trust relationships based on the watchdog mechanism, which has serious

* Corresponding author. Tel.: +1 404 518 7037; fax: +1 404 894 8363.
E-mail addresses: erman@ece.gatech.edu (E. Ayday), fekri@ece.gatech.edu (F. Fekri).

1570-8705/$ - see front matter Published by Elsevier B.V.
doi:10.1016/j.adhoc.2009.07.001

drawbacks in a wireless medium (especially in the presence of malicious nodes). Our main objective in this work is to mitigate the effects of malicious nodes to the network performance by establishing trust relationships and using a game theoretical approach between the network nodes. The network under interest is a MANET. Moreover, the network is assumed to be connected at any time instant. In other words, we assume that a path can be established between any two nodes at any time.

The rest of this paper is organized as follows. In the rest of this section, we summarize the related work in trust establishment and game theory in ad hoc networks and also mention the contributions of this paper. A brief description of the scheme is provided in Section 2. In Section 3, we analyze the game model, describe the parameter selection and show how the game changes dynamically. Trust establishment and using the trust values (node credentials) are studied in Section 4. In Section 5, we describe the adversarial model and the possible threats specific to our scheme. We evaluate and compare our scheme using computer simulations in Section 6. Eventually, the concluding remarks are provided in Section 7.

1.1. Related work

The main goal for building trust values (node credentials) among the nodes in MANETs is to protect Dynamic Source Routing (DSR) [11] from attackers and increase the performance of the network. In MANETs, a node evaluates another by using either direct or indirect measurements. Direct measurements are the ones that the node conducts itself to rate another node. On the other hand, indirect measurements are the ones that are received from other nodes regarding the credential of a specific node. Building node credentials by direct measurement is either achieved by using the watchdog mechanism or by using the ACK from destination. Building node credentials by relying on the direct measurements and using the watchdog mechanism is proposed in [2,3,5]. The purpose of the watchdog mechanism is to identify a malicious node by overhearing the communication of the next hop. In [2,3], when a misbehavior is detected, it is reported to the source of the communication and the source updates the credential for the detected node. In [5], legitimate nodes reject the traffic initiated by the detected malicious nodes. In [6,7,4,12–14], the use of indirect measurements to build node credentials is also allowed while the watchdog mechanism is used to obtain the direct measurements. In [12,13], credentials obtained by direct and indirect measurements are updated using the Bayesian approach. [14] proposes an information theoretical approach to trust and reputation. Some major drawbacks of using the watchdog mechanism to obtain direct measurements are listed below:

1. The fact that the monitoring node (the one which uses the watchdog mechanism) hears the transmission of its next hop does not mean that the following node in the path actually receives the packet. In other words, a malicious node may transfer a packet such that its previous-hop neighbor (who uses the watchdog mechanism) hears the transmission while its next-hop neighbor (who is supposed to receive the packet) does not. This can easily be achieved by adjusting the transmission power of the antenna (given that the previous-hop neighbor is located closer than the next-hop neighbor) or by using a directional antenna. Hence, the malicious node achieves its goal by preventing the legitimate flow without being penalized.
2. When there are consecutive malicious nodes in the path, it becomes very easy to cheat a monitoring node and gain credit for a malicious node (even though it keeps misbehaving). If one of the next-hop neighbors of a malicious node is also malicious, it can always send its packets to its malicious neighbor. Hence, its previous-hop neighbor (who uses the watchdog mechanism) hears the legitimate transmission and gives credit to the malicious node while its malicious next-hop neighbor drops the packets to prevent the legitimate flow.

We note that it is not guaranteed that the scenarios we listed above will occur all the time. However, as the malicious nodes in the network and the resources of the adversary increases, it is very likely to observe these scenarios. Hence, we claim that relying on the watchdog mechanism to obtain direct measurements (hence, to build trust relationships) is deceptive and misleading most of the time.

In [15,16], node credentials are constructed using the ACK messages sent by the destination node. The major drawback of these schemes is that, if a path dies due to a malicious node, the source will need to retransmit all the packets it sent via a different path. Moreover, the diversity of latency for different paths can affect the overall scheme negatively. On the other hand, as we will describe, our scheme does not suffer from this because of the use of rateless coding. In [15,16], possible routes from the source to the destination are established before the data transfer begins. Hence, even if one node is compromised from these routes, data availability is lost even though source and destination may have other alternative paths. In contrast, our scheme provides data availability as long as there is a legitimate path between the source and destination, since we construct the paths on-the-fly using our trust-metric.

Recently, researches started to use game theory to analyze wireless networks. Especially Bayesian game theoretical model [1] is commonly used to analyze wireless networks with selfish/attacker nodes. In reputation based schemes which use the Tit-for-tat strategy (e.g., [6,17]), each node monitors its neighbors and behaves based on the previous behavior of its neighbors. However, in these schemes, even if all the nodes are willing to cooperate, packet collision or noise may infer with accurate monitoring, resulting in zero throughput even if there is no malicious node in the network. Generous Tit-for-tat is proposed in [8] to fix this problem. However, to achieve full cooperation in [8], the probability that a forwarded packet was not overheard by the originating node (p_e) should be accurately estimated. In [9], authors proposed a reputation mechanism called DARWIN which does not depend on the perfect estimation of p_e. However, the scheme does not consider malicious nodes and assumes that all nodes share their perceived dropping probabilities