Pervasive and Mobile Computing 13 (2014) 164–180

Contents lists available at ScienceDirect

Pervasive and Mobile Computing

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

A light-weight trust-based QoS routing algorithm for ad hoc networks

Bo Wang*, Xunxun Chen, Weiling Chang

CNCERT/CC, Beijing, 100029, China

ARTICLE INFO

Article history:
Received 12 November 2012
Received in revised form 18 June 2013
Accepted 21 June 2013
Available online 26 June 2013

Keywords:
Trust model
QoS
Trust-based QoS routing
Trust degree
Link delay

ABSTRACT

In a mobile ad hoc network (MANET), the lack of a trusted infrastructure makes secure and reliable packet forwarding very challenging, especially for providing QoS guarantee for multimedia applications. In this paper, we firstly introduce the concept of trust and QoS metric estimation into establishing a trust-based QoS model. In this model, we estimate the trust degree between nodes from direct trust computation of direct observation and indirect trust computation by neighbors' recommendations. On the other hand, due to the NP-completeness of the multi-QoS constraints problem, we only take into account link delay as the QoS constraint requirement. Then, we design a trust-based QoS routing algorithm (called TQR) from the trade-off between trust degree and link delay. At last, by using NS2 we implement this algorithm based on AODV (Ad hoc On-demand Distance Vector). We compare its performance with AODV, Watchdog-DSR and QAODV. The simulation results show that TQR scheme can prevent attacks from malicious nodes and improve the security performance of the whole network, especially in terms of packet delivery ratio, average end-to-end delay, routing packet overhead and detection ratio of malicious nodes.

1. Introduction

Mobile ad hoc networks (MANETs), are temporary autonomous systems, where mobile nodes communicate with each other by wireless links and multi-hop forwarding, while the network topology, wireless channels and limited bandwidth are time-varying. Due to its flexibility, a MANET is attractive for applications, such as disaster relief, emergency operations, military service, maritime communications, vehicle networks, casual meetings, campus networks and robot networks. Similarly to conventional fixed networks, security of the ad hoc networks is considered from the attributes such as availability, confidentiality, integrity, authentication, non-repudiation, access control and usage control [1–3]. Security approaches used for the fixed networks are not feasible due to the salient characteristics of MANETs. So, it is necessary to design new security mechanisms to adapt to the special characteristics of MANETs.

To improve the security of MANETs, one natural idea is to develop trust establishment mechanisms that allow a node to evaluate trustworthiness of other nodes. To facilitate the implementation of this idea, various trust models and trusted routing protocols, which quantify trust relationships according to different security requirements, have been designed in the literatures [4,5]. Therefore, designing a mechanism that allows nodes to infer the trustworthiness of other nodes, especially of strangers, is necessary.

Recently, Quality of Service (QoS) for MANETs has received increased attention [6–13]. Traditional QoS routing requires not only finding a route from a source to a destination, but a route that satisfies end-to-end QoS requirements, often given

[*] Corresponding author. Tel.: +86 01082990156.
E-mail addresses: wbxyz@163.com, cxx@cert.org.cn (B. Wang).

1574-1192/$ – see front matter Crown Copyright © 2013 Published by Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.pmcj.2013.06.004

in terms of throughput, bandwidth, jitter or delay. However, security requirements are not taken into account in the QoS guarantee of the MANET environment. Security is a critical aspect of QoS routing in MANETs. To the best of our knowledge, little research efforts were made to address the trust issues with existing QoS routing and resist to malicious behaviors. In this paper, we introduce the definition of trust and QoS parameters estimation into a classic routing to enhance the security of networks. The proposed trust scheme obtains the trust degree between nodes from direct trust computation of direct observations and indirect trust computation by neighbors' recommendations to accelerate the establishment of trust in MANETs. In addition, due to the NP-completeness of the multi-QoS constraints problem, we only consider the link delay as the QoS constraint requirement for establishing trusted routing.

The main contributions of this paper are as follows: (1) A novel model for evaluating trust and satisfying QoS requirement is proposed. (2) An approach to incorporate QoS requirements and trust degree into a routing algorithm (called TQR) is designed. (3) The TQR into the classic AODV [14] is provided. Moreover, we present simulations demonstrating the effectiveness of the proposed routing scheme in selecting the more trusted nodes and least link delay, so as to defend against malicious attacks and meet the QoS requirements. The extensive results reveal the effects of maximum velocity, number of malicious nodes, trust update interval and simulation time on network performances.

The rest of the paper is organized as follows. We give an overview of related work in Section 2. Section 3 discusses the design of the trust-based QoS model, followed by a detailed description of a trust-based QoS routing algorithm in Section 4. Section 5 evaluates the algorithm with extensive simulation results and discusses different scenarios. Finally, Section 6 concludes the paper.

2. Related work

In this section, we briefly review the previous works on trust establishment and QoS schemes for MANETs.

2.1. Trust model

In recent years, there has been considerable interest in the topic of trust establishment for MANETs. In [15], Marchang N et al. propose a light-weight trust-based routing protocol. It is light-weight in the sense that the intrusion detection system (IDS) used for estimating the trust that one node has for another, which consumes limited computational resource. Moreover, it uses only local information thereby ensuring scalability to resist the black-hole attack and the gray-hole attack. In [16], Mawloud Omar et al. survey and classify the existing trust models that are based on public-key certificates proposed for ad hoc networks, and then discuss and compare them with respect to some relevant criteria. Also, the authors develop analysis and comparison among trust models using stochastic Petri nets in order to measure the performance of each one with what relates to the certification service availability. In [4], the authors present a detailed survey on various trust computing approaches that are geared towards MANETs, and highlight the summary and comparisons of these approaches. In addition, they analyze various works on trust dynamics including trust propagation, prediction and aggregation algorithms, the influence of network dynamics on trust dynamics and the impact of trust on security services. In [17], Huang Jing-Wei et al. propose a message security approach in MANETs that uses a trust-based AOMDV (Ad hoc On-demand Multipath Distance Vector) routing combined with soft-encryption, yielding a so-called T-AOMDV scheme. In [18], the authors propose a novel trust management scheme for improving routing reliability in wireless ad hoc networks. It is grounded on two classic autoregression models, namely autoregressive (AR) model and autoregressive with exogenous inputs (ARX) model. According to this scheme, a node periodically measures the packet forwarding ratio of its every neighbor as the trust observation about that neighbor. With an AR model being applied, the node only uses its own observations for prediction; with an ARX model, it also takes into account recommendations from other neighbors. In [19], the authors incorporate the concept of trust to ad hoc networks, build a simple trust model to evaluate neighbors' forwarding behavior and apply this model to opportunistic routing for ad hoc networks. A new trusted opportunistic forwarding model is proposed by choosing the trusted and highest priority candidate forwarder, then a trusted minimum cost routing algorithm (MCOR) is formally formulated. In [20], the authors propose a novel trusted route that considers communication reliability and path length for a reliable and feasible packet delivery in a MANET. They introduce the concept of attribute similarity in finding potentially friendly nodes among strangers, so security is inherently integrated into the routing protocol where nodes evaluate trust levels of others based on a set of attributes. In [5], the authors provide a survey of trust management schemes developed for MANETs and discuss generally accepted classifications, potential attacks, performance metrics, and trust metrics in MANETs. Finally, they discuss future research areas on trust management in MANETs based on the concept of social and cognitive networks. In [21], the authors state that using only a reputation-based trust framework gives only an incomplete partial solution for trust management. They propose an objective trust management framework (OTMF) for MANETs based on both direct and indirect information for reputation management and show the effectiveness of OTMF. This work uses the objective trust to refer to trust evaluated based on secondhand information. In [22], the authors introduce the concept of attribute similarity in finding potentially friendly nodes among strangers, so security is inherently integrated into the routing protocol where nodes evaluate trust levels of others based on a set of attributes. Unlike the fixed probability of dropping packets adopted in other routing mechanisms, the proposed new forwarding rule is designed based on the attribute similarity, and then the authors provide a recommended method in calculating the degree of similarity between