Applied Soft Computing 38 (2016) 469–476

Contents lists available at ScienceDirect

Applied Soft Computing

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

A routing defense mechanism using evolutionary game theory for Delay Tolerant Networks

Hang Guo [a], Xingwei Wang [b,*], Hui Cheng [c], Min Huang [a]

[a] College of Information Science and Engineering, Northeastern University, Shenyang, China
[b] College of Software, Northeastern University, Shenyang, China
[c] School of Computing and Mathematical Sciences, Liverpool John Moores University, Liverpool, UK

ARTICLE INFO

Article history:
Received 12 April 2015
Received in revised form
12 September 2015
Accepted 7 October 2015
Available online 17 October 2015

Keywords:
Delay Tolerant Networks
Evolutionary game
Routing attack
Routing security
Evolutionary strategy stable

ABSTRACT

Delay Tolerant Networks (DTNs) often suffer from intermittent disruption due to factors such as mobility and energy. Though lots of routing algorithms in DTNs have been proposed in the last few years, the routing security problems have not attracted enough attention. DTNs are still facing the threats from different kinds of routing attacks. In this paper, a general purpose defense mechanism is proposed against various routing attacks on DTNs. The defense mechanism is based on the routing path information acquired from the forwarded messages and the acknowledgment (ACK), and it is suitable for different routing schemes. Evolutionary game theory is applied with the defense mechanism to analyze and facilitate the strategy changes of the nodes in the networks. Simulation results show that the proposed evolutionary game theory based defense scheme can achieve high average delivery ratio, low network overhead and low average transmission delay in various routing attack scenarios. By introducing the game theory, the networks can avoid being attacked and provide normal transmission service. The networks can reach evolutionary strategy stable (ESS) under special conditions after evolution. The initial parameters will affect the convergence speed and the final ESS, but the initial ratio of the nodes choosing different strategies can only affect the game process.

1. Introduction

Delay Tolerant Networks (DTNs) [1] are designed to cope with the challenging conditions in the restricted networks with sparse density, intermittent disruption and limited energy. DTNs can be used in military, industry, transport, monitor, deep space communication and other challenging networks environments [2]. The messages are relayed hop by hop by means of the store-carry-forward mechanism. Importantly, routing is the main challenge in DTNs, and the routing techniques in traditional networks cannot work effectively in DTNs since it is extremely difficult to determine the potential end to end path toward the destination [3].

The unique features of DTNs result in unique security challenges [4]. DTNs have features such as multiple hops, self-organization, and no central administration. However, in most cases DTNs are deployed in the open environment, and security problems are tough issues. The security threats of DTNs are different from those of traditional wireless networks because of the unique features, so the traditional methods to deal with network security threats are not necessarily effective and alterations need to be made [5]. As shown in Fig. 1, there are different types of DTNs security problems, and they should be sufficiently considered in different network layers. In the physical layer, the main problems are wireless communication jamming and nodes being compromised. In the link layer, the main problems are collision and wireless resource allocation. In the routing layer, the main problems are the routing attacks and routing security. The various routing attack countermeasures are discussed in this paper.

Packets in DTNs are opportunistically routed toward the destination, making them robust against simple attacks such as packet dropping attacks [6]. However there are still some routing attack methods in DTNs. The primary attack methods include wormhole attack, blackhole attack, greed attack, tampering attack and so on. These routing attacks will severely affect the network performance [7]. In this paper, a general solution to deal with routing attacks in DTNs is proposed. First, a proactive defense mechanism is established based on the routing path information and the ACK information. Then, the evolutionary game theory is introduced with the defense mechanism to solve the routing attack problems in DTNs.

* Corresponding author.
E-mail addresses: guohang0001@126.com (H. Guo), wangxw@mail.neu.edu.cn (X. Wang), h.cheng@ljmu.ac.uk (H. Cheng), mhuang@mail.neu.edu.cn (M. Huang).

http://dx.doi.org/10.1016/j.asoc.2015.10.019
1568-4946/

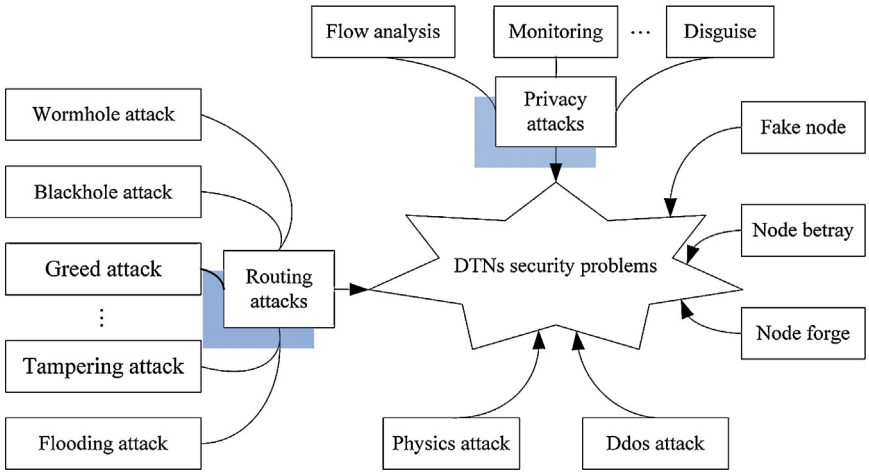

Fig. 1. A summary of security problems in DTNs.

The rest of this paper is structured as follows. Section 2 outlines the current state of routing security in DTNs. In Section 3, the defense mechanism is proposed and different strategies of nodes are analyzed in the evolutionary game system. The simulation results under various scenarios are presented in Section 4, followed by the conclusions and future work in the last section.

2. Related works

The current research on DTNs mostly focuses on routing algorithms [8], and the routing security problems have not attracted enough attention. There are mainly two ways to cope with the routing attacks in DTNs. One is to use different methods to detect malicious nodes and isolate them, and the other is to use incentive mechanism to encourage all the nodes to participate in the information transmission. Recently the game theory has also been used in the DTNs routing security filed.

The methods to detect malicious nodes in DTNs include probabilistic detection, ferry-based detection, reputation-based detection and reference-based detection and so on. The probabilistic misbehavior detection scheme proposed in [9] uses the trusted authority to collect every node's routing credentials periodically and judge the node's behavior through the information analysis. An intrusion detection system which utilizes the correlation of delivery probability between the nodes is proposed in [10] to mitigate flood attack in DTNs. A message-ferry-based detection method reported in [11] considers some dependable mobile nodes exist in the network, and these dependable nodes collect the history delivery information of the nodes they encounter, and then the malicious nodes can be distinguished according to the information. Ren et al. [12] take the node's transitivity into consideration and propose a mutual correlation detection scheme. This method can update the transfer probability between the nodes and improve the detection accuracy. Because the ferry-based detection methods need to use dependable nodes as ferry nodes, this will lead to extra cost. Meanwhile the efficiency of these methods will decrease in the sparse networks environment. A secure reputation-based dynamic window scheme is proposed in [13]. In this scheme, if one node wants to estimate another node's reputation, it should firstly gather all other neighbor nodes' evaluations to this node, and then do the estimation. During the process of routing, the nodes with high reputation will be chosen as relay nodes. Here the reputation can be global or local. The global case will need reliable hardware to spread the reputation, and the local case does not need the support of the hardware. Nagrath et al. [14] design a secure reputation based algorithm that handles flooding attack in distributive and transitive manner, in which it is assumed that the malicious node can flood the network with bogus nodes but is not capable of generating genuine messages. Guo et al. [15] propose a misbehavior detection system based on encounter record-based reputation system to protect the security of the hybrid networks. A reference-based method using encounter tickets is proposed in [16] and a reference-based method using packet exchange recording is proposed in [17]. Saha et al. [18] propose a table-based strategy to record network history and use this information to detect discrepancies in the behavior of nodes, followed by elimination of those detected as malicious. In these reference-based DTNs routing algorithms, if one node wants to provide relay service, it should firstly send its reference value to surrounding neighborhood nodes to certify that the node has taken part in the delivery of messages.

The incentive mechanism can improve the performance of DTNs by means of punishment or incentive. Upendra et al. [19] apply the tit-for-tat (TFT) strategy to DTNs. In the scheme, node *A* will forward messages for node *B* if node *B* has forwarded messages for node *A* and vice versa. Based on the TFT strategy, an incentive-aware routing protocol is proposed which can make the selfish nodes' benefit obey the TFT restriction. Zhu et al. [20] propose a secure credit-based incentive scheme, which uses virtual currency consisting of several layers of information to pay and reward the node that forwards messages in DTNs. The information of virtual currency contains the source node and destination node, the service needed, and the credit value obtained by forwarding the message. The authors subsequently further improve this scheme by permitting relay node to transfer and distribute the virtual currency. Lu et al. [21] propose a practical incentive protocol for DTNs which contains a fair incentive model. The source node will add incentive information to the to-be-sent message to encourage the selfish nodes to forward the message. If the message successfully reaches the destination node, all relay nodes will receive reward from the source node. If the message transmission fails, the relay nodes participating in the forward will achieve the reputation from the trusted agency.

Game theory has been mainly studied and applied in economics, politics and sociology, which has recently emerged as a useful tool in analyzing modern wireless networks since it provides analytical tools to model interactions among entities with conflicting interests that compete for the limited network resources. There is a survey on the game theory used in wireless sensor networks (WSNs) to achieve a tradeoff between maximizing the network lifetime and providing the required service [22]. An active