Available online at www.sciencedirect.com
ScienceDirect
Ad Hoc Networks 6 (2008) 508–523
Ad Hoc Networks
www.elsevier.com/locate/adhoc

Collaborative techniques for intrusion detection in mobile ad-hoc networks

Ningrinla Marchang [a], Raja Datta [b,*]

[a] Department of Computer Science and Engineering, North Eastern Regional Institute of Science and Technology, Nirjuli 791109, Arunachal Pradesh, India
[b] Department of Electronics and Electrical Communication Engineering, Indian Institute of Technology Kharagpur, Kharagpur 721302, West Bengal, India

Received 14 July 2006; received in revised form 16 January 2007; accepted 10 April 2007
Available online 24 April 2007

Abstract

In this paper, we present two intrusion detection techniques for mobile ad-hoc networks, which use collaborative efforts of nodes in a neighborhood to detect a malicious node in that neighborhood. The first technique is designed for detection of malicious nodes in a neighborhood of nodes in which each pair of nodes in the neighborhood are within radio range of each other. Such a neighborhood of nodes is known as a *clique* [12]. The second technique is designed for detection of malicious nodes in a neighborhood of nodes, in which each pair of nodes may not be in radio range of each other but where there is a node among them which has all the other nodes in its one-hop vicinity. This neighborhood is identical to a *cluster* as mentioned in [12]. Both techniques use message passing between the nodes. A node called the *monitor* node initiates the detection process. Based on the messages that it receives during the detection process, each node determines the nodes it suspects to be malicious and send votes to the *monitor* node. The *monitor* node upon inspecting the votes determines the malicious nodes from among the suspected nodes. Our intrusion detection system is independent of any routing protocol. We give the proof of correctness of the first algorithm, which shows that it correctly detects the malicious nodes always when there is no message loss. We also show with the help of simulations that both the algorithms give good performance even when there are message losses arising due to unreliable channel.

Keywords: MANET; Intrusion detection system (IDS); Malicious node; Security; Wireless network

1. Introduction

The proliferation of mobile devices such as laptops, PDAs and mobile phones have ushered in exciting applications such as virtual classrooms, rescue missions, virtual conferences, etc. Mobile ad-hoc Networking is a technology which makes all these applications a possibility anywhere. All that is required is for a group of mobile nodes to self-configure and form a network without the need of any fixed infrastructure or a centralized controlling authority. In this network, a mobile node behaves as a host and a router at the same time.

* Corresponding author. Tel.: +91 9474065905; fax: +91 3222 282264.
E-mail addresses: ningrinla@yahoo.co.in (N. Marchang), rajadatta@ece.iitkgp.ernet.in (R. Datta).

1570-8705/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.adhoc.2007.04.003

Thus, this technology makes a mobile node really mobile as compared to a conventional infrastructure-based mobile network, in which case a mobile node is constrained to work within a certain radius from the infrastructure. Also a mobile ad-hoc network (MANET) could be a cost-effective solution for providing communication in areas where setting up fixed infrastructures would be an impossible task due to geographical constraints or financial inviability. However, the downside of MANET is that it is difficult to ensure a secure communication within the network.

Providing security in mobile ad-hoc networks (MANET) is a prime concern due to the need of providing protected communication between mobile nodes in a hostile environment. Early research efforts on MANET assumed a friendly and co-operative environment, which may not apply in real-life scenarios (e.g., a MANET set up in a battlefield environment). Unlike in infrastructure-based wireless networks, the unique characteristics of MANETs such as open network architecture, shared wireless medium, stringent resource constraints and highly dynamic network topology pose new security challenges. Several schemes have been proposed for secure routing protocols, intrusion detection and response systems.

One way of securing a mobile ad-hoc network at the network layer is to secure the routing protocols such that all possible attacks are prevented. Several kinds of attacks, such as routing loop attack, black hole attack, gray hole attack, partitioning, etc. are given in detail by Hu et al. [1]. Some ways through, which these attacks can be carried out are, using modification of control message fields (e.g., modifying the hop count, modifying the sequence number, etc.) and using impersonation (e.g., forge messages by spoofing sender or destination addresses). Yang et al. proposed that security solutions for MANET should provide complete protocol protection spanning the entire protocol stack [2].

However, as far as we know, no secure routing protocol proposed in the literature so far takes care of all kinds of attacks. And if it were that a secure routing protocol would come up, which takes care of all known attacks, yet, one can never say when a different kind of attack which has not been envisaged before will suddenly raise its ugly head, exploiting the weaknesses in the ever-increasingly complex systems due to design and programming errors. This would require a modification of the secure routing protocol to be able to handle this new attack. In other words, one can never claim that a prevention mechanism is foolproof. Hence, the need arises for a second wall of defense: an intrusion detection system. The idea is that in the unfortunate event of a MANET being intruded, if there exists a system for detection of such an intrusion, it could be detected as early as possible, and the MANET could be saved before any extensive harm can be done, even if it cannot be avoided altogether. Research efforts are going on to develop Intrusion Detection Systems (IDS) to detect intrusion, identify the malicious nodes, and isolate them from the rest of the network. Further, the presence of a detection system will discourage malicious nodes from attempting intrusion in future. An analogy of an intrusion detection system would be security guards posted to secure a house. A trespasser could be detected by the security guards and handed over to the police. Moreover, it is likely that the trespasser will think twice before he attempts to break in again in future.

In this paper, we have presented algorithms for detection of malicious nodes that may intrude a MANET. The first algorithm, which we call ADCLI (Algorithm for Detection in a CLIque) is for detection of malicious nodes in a *clique*, whereas the second algorithm, which we call ADCLU (Algorithm for Detection in a CLUster) is for detecting malicious nodes in a *cluster*. In both the algorithms, we have used a message passing mechanism between the group of nodes, which enables each of the nodes to determine those nodes in the group that are suspected to be malicious. Finally, a voting method is used for detecting the malicious nodes from among the suspected nodes. We give the proof of correctness of the first algorithm and also show with the help of simulation that it gives good performance even when there is packet loss (due to packet collision, unreliable channel etc.) up to 6%. Through simulation, we also show that the second algorithm is efficient even for a network where packet loss may go up to 5%. Our intrusion detection algorithms are independent of any routing protocol. Most of the earlier detection systems in the literature require a considerable amount of packets to be buffered in the process of monitoring the neighbor's traffic, which accounts for a lot of overhead for a node. Our algorithm does not need to monitor packets meant for other nodes thereby reducing this overhead.

The rest of the paper is organized as follows: In Section 2 we discuss related works on intrusion