Information Sciences 220 (2013) 580–602

Contents lists available at SciVerse ScienceDirect

Information Sciences

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

Energy-aware and self-adaptive anomaly detection scheme based on network tomography in mobile ad hoc networks

Wei Wang [a,b], Huiran Wang [a], Beizhan Wang [c,*], Yaping Wang [d], Jiajun Wang [c]

[a] School of Computer Science, Xi'an Polytechnic University, Xi'an 710048, China
[b] Ministry of Education Key Laboratory for Intelligent Network and Network Security, State Key Lab for Manufacturing Systems Engineering, Xi'an Jiaotong University, Xi'an 710049, China
[c] School of Software, Xiamen University, Xiamen 361005, China
[d] Department of Industrial and Systems Engineering, Texas A&M University, TX 77843, USA

ARTICLE INFO

Article history:
Received 28 June 2010
Received in revised form 11 June 2012
Accepted 21 July 2012
Available online 1 August 2012

Keywords:
Mobile ad hoc network
Anomaly detection
Link delay
Self-organizing Map

ABSTRACT

Anomaly detection is indispensable for satisfying security services in mobile ad hoc network (MANET) applications. Often, however, a highly secure mechanism consumes a large amount of network resources, resulting in network performance degradation. To shift intrusion detection from existing security-centric design approaches to network performance centric design schemes, this paper presents a framework for designing an energy-aware and self-adaptive anomaly detection scheme for resource constrained MANETs. The scheme uses network tomography, a new technique for studying internal link performance based solely on end-to-end measurements. With the support of a module comprising a novel spatial-time model to identify the MANET topology, an energy-aware algorithm to sponsor system service, a method based on the expectation maximum to infer delay distribution, and a Self-organizing Map (SOM) neural network solution to profile link activity, the proposed system is capable of detecting link anomalies and localizing malicious nodes. Consequently, the proposed scheme offers a trade-off between overall network security and network performance, without causing any heavy network overload. Moreover, it provides an additional approach to monitor the spatial-time behavior of MANETs, including network topology, link performance and network security. The effectiveness of the proposed schemes is verified through extensive experiments.

1. Introduction

Mobile ad hoc networking (MANET), which does not rely on any existing communication infrastructure, has become an exciting and important technology in recent years. Though applications of MANETs include mobile computing, search and rescue, and disaster recovery, the problem of securing MANETs is still in its infancy [7]. Compared with a fixed network, a MANET is more vulnerable due to its exclusive characteristics, such as open medium, dynamic topology, resource constraints, and lack of centralized management point [49]. Inevitably, a variety of attacks have targeted the network layer, such as Wormhole and Byzantine attacks, and these have been identified and studied in the literature [17]. In these attacks, attackers inject themselves onto the path between the source and destination, thereby controlling the network traffic flow. For example, traffic packets may be forwarded to a non-optimal path, which could result in significant delay. Consequently, the attackers are able to introduce severe network congestion and performance degradation.

* Corresponding author.
E-mail addresses: wangbz@xmu.edu.cn, wangbeizhan@gmail.com (B. Wang).

0020-0255/$ - see front matter © 2012 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.ins.2012.07.036

Hitherto, much research effort such as [25], has focused on MANET intrusion detection. However, most of these studies have relied on cooperation with full coverage of network nodes to detect anomalous behavior. This may inevitably come at an unacceptable cost of high overhead [39]. Moreover, the existing proposals mainly address the security vigor of the design and largely ignore the network performance aspect [57]. These solutions may be highly secure, but their actual performance when deployed in real networks is uncertain [4]. The reason for this is that a highly secure mechanism inevitably consumes a large amount of system resources, which in turn may unintentionally degrade network performance (such as delay and throughput) and even cause Denial of Service (DoS) attacks [13]. This means that we are currently facing a difficult dilemma: on the one hand, extensive security services are indispensable for most MANET applications with inherent security vulnerabilities; on the other hand, with limited scarce resources, MANET system is incapable of supporting the integration of a large number of possible or necessary security measures.

In the light of all these considerations, new intrusion detection schemes (IDS) need to be found to balance security and MANET performance. While this is extremely challenging, it appears that many intrusions can be detected by the abnormal traffic patterns they have generated [18]. In particular, the ability to isolate the performance of localized portions of the network could be useful in detecting attacks, as network performance deteriorates significantly during such attacks. For example, the rapid increases in the correlation of delay behavior in local network neighborhoods can be indicative of DoS attacks. Through online monitoring of delay or loss behavior, a rapid identification of the source of an attack becomes much more feasible. Accordingly, a novel intrusion detection scheme that localizes pathological network performance to individual links or sub networks would be most useful as an early warning in an anomaly detection system.

Network tomography (NT) [48,24] is a new technique proposed for inferring network internal link performance information from end-to-end (E2E) measurements. Compared with the traditional direct measurement [2] which is expensive and even impractical for MANETs, NT minimizes the measurement overhead and provides a new direction for solving the anomaly intrusion detection problem [47]. Using the inferred performance information, we can characterize and monitor the network performance over time, detect anomalies in the network, and ensure compliance with service-level agreements [34].

In this work, our main focus is shifted from the existing security-centric design approach to a wireless link performance centric design scheme. A novel energy-aware and self-adaptive anomaly detection scheme based on network tomography is proposed. By combining anomaly detection with inference techniques, a new framework is constructed. For this system, we propose a novel spatial-time model to identify the MANET topology and an energy-aware algorithm to sponsor system services. Furthermore, to monitor the internal link delay over the identified topology, we develop a method based on the Expectation Maximum (EM) [54] to infer delay distribution. Finally, a Self-organizing Map (SOM) neural network solution [23] is used to profile link activity, detect link anomalies, and localize malicious nodes. Note that our system employs a fully distributed, multi-agent framework which provides detection adaptation to achieve a tradeoff between security and network performance. To the best of our knowledge, we are the first to introduce NT technology into MANETs anomaly detection.

A preliminary study has been carried out using the NS2 network simulator [61] to simulate network scenarios with 20 and 50 nodes, respectively. The simulation results show that the proposed system is a promising and desirable scheme for detecting anomaly link performance information and localizing the anomaly nodes hidden in a MANET. The rest of this paper is organized as follows. Section 2 reviews some of the related work on intrusion detection and NT. Section 3 formulates the spatial-time network topology model and security models, while Section 4 discusses the proposed system in detail. Section 5 analyzes the overhead and applicability of our system, and Section 6 discusses the simulation evaluation using NS2. Conclusions are presented in Section 7.

2. Related work

In this section, we present a state-of-the-art survey on intrusion detection for MANETs and review related work on NT.

2.1. A state-of-the-art survey on intrusion detection for MANETs

Due to the vulnerabilities of MANETs, there is a strong need for intrusion detection as a frontline security research area. Intrusion detection is defined as a method for identifying any sequence of actions that attempts to compromise the integrity, confidentiality, or availability of a resource [27].

Generally, according to the intrusion detection procedure used in security systems, IDS may be classified as signature-based detection, anomaly-based detection and specification-based detection [1]. Signature-based detection compares known attack signatures with current system activities. It may display low false positive rates, but does not perform well at detecting previously unknown attacks. Anomaly-based detection profiles the symptoms of normal behaviors of the system. It detects intrusions as anomalies, i.e. deviations from established normal behaviors. Compared with signature-based detection, anomaly-based detection may detect previously unknown attacks, but may exhibit high rates of false positives. In specification-based detection, the correct behaviors of the system are manually abstracted and crafted as security specifications, which are compared with the actual behavior of the system. It can provide detection of known and unknown attacks with lower false positive rate, but manual development of specifications can be very time consuming. So far the specification-based detection has been applied to privileged programs, applications, and several network protocols.