Ad Hoc Networks 21 (2014) 18–41

Contents lists available at ScienceDirect

Ad Hoc Networks

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

Traffic-and-resource-aware intrusion detection in wireless mesh networks ☆

Amin Hassanzadeh, Ala Altaweel, Radu Stoleru *

Department of Computer Science and Engineering, Texas A&M University, United States

ARTICLE INFO

Article history:
Received 29 July 2013
Received in revised form 21 March 2014
Accepted 21 April 2014
Available online 5 May 2014

Keywords:
Wireless mesh network
Intrusion detection
Optimal monitoring
Traffic awareness
Resource constraints
Integer linear program

ABSTRACT

As the interest in Wireless Mesh Networks (WMN), as an infrastructureless wireless network, grows, security issues, especially intrusion detection, become of paramount importance. The diversity in hardware along with a variety of WMN applications, have resulted in WMN with different network characteristics (e.g., resource levels, system and security models, etc.). Consequently, different intrusion detection mechanisms have been proposed by the research community. Recently, the community has proposed several monitoring techniques for intrusion detection where each considers different assumptions and presents a different problem formulation for optimal monitoring. This article proposes a taxonomy that categorizes existing solutions in this research area and identifies the similarities and differences in their optimal monitoring problem formulations. We then concentrate on two classes of monitoring techniques for intrusion detection in WMN: *Traffic Agnostic and Resourceful* and *Traffic Aware and Resourceful* and present centralized and distributed algorithms for solving optimal monitoring problem in these networks. Through extensive simulations and a real implementation, we demonstrate the effects of different network characteristics on the problem formulation and consequently the performance (e.g., intrusion detection rate and resource consumption) of proposed solutions for optimal monitoring in WMN.

1. Introduction

Wireless Mesh Networks (WMN) has emerged as self-managing networks that provide Internet, intranet, and other networking services to fixed and mobile clients using a multi-hop multi-path wireless infrastructure [2–4]. The number of deployments of WMN is continuously increasing as they are suitable for many application domains such as disaster response [5–9], rural IT services [10–14], environmental monitoring [15–17] and many others, as surveyed in [4]. Because of the intrinsic sharing of the wireless medium and the emerging information security threats, security has become one of the most critical issues WMN deployments face today.

Although *Intrusion prevention* methodologies, e.g., encryption protocols, public key infrastructure (PKI), etc., are known as the first line of defense in wireless networks, this may not be enough in mission critical scenarios that require strictly secure communication. It has been argued [18] that regardless of the number of intrusion prevention strategies used in a network, some vulnerabilities can always be found to allow intruders passing the first line of defense. For example, an unauthorized client physically located in the WMN coverage area, but not associated to a WMN access point, can launch attacks against WMN communication links, e.g., Jamming attacks. To address the issues of intrusion prevention, one of the most effective

☆ An earlier version of this article appeared in ADHOC-NOW 2011 [1].

* Corresponding author. Tel.: +1 979 862 8349.
E-mail addresses: hassanzadeh@cse.tamu.edu (A. Hassanzadeh), altaweel@cse.tamu.edu (A. Altaweel), stoleru@cse.tamu.edu (R. Stoleru).

http://dx.doi.org/10.1016/j.adhoc.2014.04.009
1570-8705/

ideas proposed was to add layers of additional security tools, e.g., *intrusion detection systems* (IDS), that take appropriate actions when the network is perceived to be under attack. Simply adopting IDS from wired networks is challenging because WMN lack: (a) single vantage points where traffic can be analyzed, which is typical in wired networks (e.g., a gateway or router in a corporate network); (b) the *hardware resources*(e.g., CPU and RAM) available to wired networks; and (c) the practically *unlimited energy* for powering WMN hardware.

The lack of concentration points where network traffic can be analyzed has been investigated mainly in the context of MANET and sensor networks. There, IDS were completely decentralized, and an intrusion detection agent was placed on each node [18]. These solutions were very inefficient since nodes in the network would execute intrusion detection in a redundant manner (e.g., a multi-hop stream was analyzed multiple times) thus consuming both hardware resources (that could be allocated to other network functions) and energy. These identified inefficiencies have triggered significant research on *optimal monitoring* for intrusion detection. The optimal monitoring has been typically solved by selecting a few nodes (called monitoring nodes) that execute IDS [21,25–27]. The research has shown that these solutions suffer from high false negative rates if the hardware resources are not sufficient for executing complete IDS functions [19,28]. Consequently, "cooperative monitoring" has been proposed, where nodes are assigned with few distinct IDS functions for local intrusion detection and exchange information for cooperative intrusion detection [29–37]. Cooperative monitoring for intrusion detection has proven viable in scenarios where network traffic is not significant, e.g., sensor networks, but it is problematic in networks with significant traffic [4,11,38,39] as expected in WMN. Consequently, in this paper we investigate non-cooperative approaches for IDS in WMN.

Recently, it was proposed that knowledge about network traffic (i.e., traffic-awareness) be used for optimal monitoring for intrusion detection [24,40]. The traffic awareness is particularly helpful in networks with significant constraints on hardware resources (designated herein as resourceless). Some WMN may fall in this category and can benefit from such solutions [40]. Other WMN have wireless routers with more hardware capabilities (designated herein as resourceful), that can be dedicated to performing full IDS functions [7,16,22]. We hypothesize that traffic awareness can also be helpful for resourceful WMN.

To better understand the space of solutions for intrusion detection in WMN, we propose a taxonomy, presented in Table 1. This taxonomy allows us to identify gaps in existing solution-dedicated space and validate our aforementioned hypothesis. As shown, our taxonomy is based on the hardware resources available to WMN nodes (i.e., Resourceless and Resourceful) and based on Traffic Awareness (i.e., Traffic Aware and Traffic Agnostic). It is important to observe that our taxonomy addresses IDS architectural issues and not intrusion detection engine specific issues (e.g., if the IDS engine is Snort or Bro or some other one). *Traffic Agnostic and Resourceless* solutions (e.g., OpenLIDS [19] and DogoIDS [20]) use lightweight IDS for resource-constrained WMN devices, but they can only detect a limited number of attacks (they have higher false alarm rates). *Traffic Aware and Resourceless* solutions (e.g., PRIDE [24,40] and TRAM [23]) assume that security administrators have the traffic information and distribute reduced IDS tasks to monitoring nodes in the network, thus using fewer hardware resources while still achieving high detection rates. *Traffic Agnostic and Resourceful* solutions (e.g., [21,22]) assume resourceful WMN devices (so called specialized monitoring nodes in [22]) that are able to perform complete IDS configurations and tolerate IDS computational load.

Table 1
Taxonomy for traffic and resource aware intrusion detection in WMN.

	Hardware resources	
	Resourceless	Resourceful
Traffic awareness		
Traffic Agnostic	OpenLIDS [19], DogoIDS [20]	[21,22], EEMON
Traffic Aware	TRAM [23], PRIDE [24]	TRAIN

In this article, we identify that the *node coverage* approach of existing IDS for WMN is problematic for some network security attacks (Section 3 shows that *link coverage* provides higher intrusion detection rate than node coverage). Additionally, using our taxonomy, we observe that no solution was proposed for intrusion detection in Traffic Aware and Resourceful WMN. Consequently, we present the EEMON design, an IDS for Traffic Agnostic and Resourceful WMN that monitors links instead of nodes. EEMON also considers the limited energy of WMN nodes. This article also introduces TRAIN, an IDS for Traffic Aware and Resourceful WMN that monitors traffic paths and also takes into account the limited energy of WMN nodes. More precisely, our contributions are as follows:

- We present similarities and differences in state-of-art-art formulations for optimal monitoring problem, based on our proposed taxonomy.
- We formulate a novel optimal monitoring node selection problem (Weighted Monitoring Coverage (WMC)) for Traffic Agnostic and Resourceful WMN whereby monitoring nodes are responsible for monitoring wireless links and not individual neighbor nodes. We show that WMC is NP-hard.
- We formulate a novel optimal monitoring node selection problem (Path Monitoring Problem (PMP)) for Traffic Aware and Resourceful WMN, in which monitor nodes are responsible for monitoring traffic paths.
- We propose a protocol (EEMON) for solving WMC and a protocol (TRAIN) for solving PMP.
- We provide analysis of algorithms used in EEMON and TRAIN to illustrate the tradeoff of time and message complexities for intrusion detection rate.
- Through extensive simulations, we evaluate the performance of TRAIN and EEMON for intrusion detection rates and energy consumption in battery-powered WMN.