Journal of Network and Computer Applications 61 (2016) 133–141

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Null-frequency jamming of a proactive routing protocol in wireless mesh networks

Shruti Lall *, B.T.J. Maharaj, P.A. Jansen van Vuuren

Department of Electrical, Electronic and Computer Engineering, University of Pretoria, South Africa

ARTICLE INFO

Article history:
Received 5 December 2014
Received in revised form
10 October 2015
Accepted 20 October 2015
Available online 4 November 2015

Keywords:
Null-frequency
Optimised link state routing
Proactive routing
Wireless jamming
Wireless mesh networks

ABSTRACT

Disrupting network communication of adversarial networks is of increasing interest and importance. The use of jamming devices is a viable method for disabling the communication capabilities of enemy networks. This paper proposes a jamming technique which targets the periodic nature of the routing protocol residing in the network layer. The technique is based on the concept of null-frequency jamming which refers to periodic attacks targeting specific protocol period/frequency of operation. The effects of this jamming technique are investigated in stack, half-diamond, full-diamond, full-mesh and random topologies employing the optimised link state routing protocol. OMNeT++ 4.3 was chosen as the network simulation platform in which to conduct the investigations. It was found that when jamming at the 2 s null-period for a length of 0.5 s, there was a substantial drop in overall network performance. This technique was then compared to constant, deceptive and random jamming techniques and was shown to outperform the techniques in terms of the energy expended by the wireless nodes in the networks.

© 2015 Elsevier Ltd. All rights reserved.

1. Introduction

Wireless networks are gaining widespread use and popularity because of their progressive increase in affordability and convenience. Owing to the improved facilitation of communication and data transfer, wireless networks are being deployed in numerous modalities, ranging from wireless local area networks (WLANs) to mesh and sensor networks (Xu et al., 2005). Wireless networks are often seen as a more attractive option to their wired network counterpart due to their increased mobility, expandability, cost efficiency and ease of integration. As a result of the need for mobility, data is broadcast using radio technology, which implies that any receiver in range will be able to, not only listen in on the transmission, but manipulate or alter the ongoing transmission. Wireless mesh networks (WMNs) are networks which consist of peer-to-peer wireless mobile node interconnections that collectively form an intelligent, large-scale and broadband wireless network. The shared and easy to access medium, while being the most beneficial characteristic of WMNs, makes it extremely easy for an adversary to launch an attack. Consequently, jamming attacks are most effective in these networks. Jamming is defined to be any activity that seeks to deny service to legitimate users by generating signals, noise or malicious packets in an effort to disrupt communication services (Prasad and Thuente, 2011). The device that transmits jamming pulses, signals and packets to disrupt the service is known as a jammer or a jamming node. Wireless network jamming has essential military application for disrupting enemy battlefield communication services (Commander et al., 2007). It is therefore pertinent that the jamming scheme is energy efficient and difficult to detect in order to ensure their longevity. Although security and energy efficiency are two research areas that have largely been addressed as separate entities, it is important to consider and propose energy-aware attack schemes that jointly address energy efficiency and the impact of the attack (Palmieri et al., 2015). A jamming attack is classified as being effective when it is energy efficient, has a low probability of being detected and has a high level of undesirable impact on network operation. There are a number of different types of jamming attacks namely, *constant jamming*, *deceptive jamming*, *random jamming*, *reactive jamming*, and *scheduled jamming* (Xing and Wang, 2006).

Constant jamming is the simplest kind of jamming attack in that it continually transmits an interference signal, in order to degrade the capacity of the wireless channel (Xing and Wang, 2006). It disregards the protocols in the physical and link layers of the nodes. The main disadvantage of constant jammers is that the energy consumption is excessive, as it continually transmits high-power noise. This causes significant interference which prevents the reliable delivery of data packets on the channel (Altman et al., 2009). *Deceptive jamming* is an attack in which the jammers continually inject legitimate packets with valid headers into the

* Corresponding author.
E-mail addresses: shruti.lall11@gmail.com (S. Lall), sunil.maharaj@up.ac.za (B.T.J. Maharaj), pieter.jansenvanvuuren@up.ac.za (P.A.J.v. Vuuren).

http://dx.doi.org/10.1016/j.jnca.2015.10.009
1084-8045/© 2015 Elsevier Ltd. All rights reserved.

channel. As a result, the receiving node thinks that it is receiving a legitimate packet and will therefore be restricted to the receiving mode. As with *constant jamming*, *deceptive jamming* is a continuous jamming attack and as such, it expends a large amount of energy to continually send out these packets. In addition, continuous jammers are easy to detect as a result of the constant presence of these high-power interference signals. There are numerous studies detailing methods on how to mitigate these types of attacks. Examples include the use of spread spectrum communications (Belouchrani and Amin, 2000) and spatial retreats (Wood et al., 2004) to aid in mitigation as well as mitigation through the localisation and removal of the jamming nodes (Proano and Lazos, 2004).

Random jamming addresses the large energy expenditure of *constant* and *deceptive jamming* by alternating the jammer between sleep mode and jamming mode. The random jammer performs the attack for a random period after which it shuts down for an arbitrary amount of time before continuing the attack. However, *random jamming* attacks are not as effective in degrading the performance of the network as continuous jamming attacks (Wang and Wyglinski, 2011). *Reactive jamming* involves listening to the network transmissions, deciphering the packets and reacting to the subsequent network state (Xing and Wang, 2006). This type of attack proves to be more difficult to implement than other attacks as it requires the ability to decode the packet information and react accordingly with malicious intent. The primary advantage of a reactive jammer is that it is more difficult to detect, however, it does not conserve any more energy than continuous jammers as it constantly needs to listen to the channel. Scheduled jammers send out bursts of jamming packets for a specific period of time, based on a predefined schedule (Balakrishnan et al., 2012). This type of attack does not require packet decoding capabilities or reactive intelligence. It is also significantly more energy efficient than both continuous and reactive jammers. The effectiveness of this attack depends on the pre-set schedule of the jamming packet bursts. This aims to target the timer-based operation of the protocols implemented in the physical layer, transport layer or network layer of the wireless nodes.

A large portion of the work done on jamming in wireless networks focuses on jamming at the physical and link layers (Ahmed and Huang, 2009). This includes the use of intelligent jammers that exploit link layer protocol rules (Gupta et al., 2002; Muogilim et al., 2011; Kim et al., 2013; Avelara et al., 2014; Xu and Saadawi, 2002). There have been several studies of protocol-aware jamming attacks on the link layer, while fewer studies focused on the network layer (Jae-Joon and Jaesung, 2013). One of the main reasons for the lack of sufficient study on network layer jamming strategies is the notion that a routing protocol can effectively construct alternate routes. This implies that the routing protocol can exclude routes involving the jamming nodes, and thus, provide reliable data delivery defeating the purpose of the jamming attack (Jae-Joon and Jaesung, 2013). However, certain vulnerabilities of routing protocols, resulting from the use of internal states and timers for network coordination, can be exploited and used to increase the efficiency of the jamming nodes. Jamming at the network layer includes sending extra control or data packets to degrade network performance as was presented in Desilva and Boppana (2005) where a malicious node constantly initiates route discovery requests but ignores any replies to them. A jamming node can also act as the originator of a large number of junk data packets, which are then injected into a path and result in resource deprivation of intermediate routing nodes (Gu et al., 2005). An added advantage of the network layer based jamming scheme is that energy-saving techniques and methods, which are largely targeted for higher layers, such as the transport and network layer, can be easily adopted to increase the energy efficiency of the proposed jamming attack (Oulmahdi et al., 2014; Ricciardi et al., 2015).

Balakrishnan et al. (2012) have investigated null-frequency jamming (NFJ) in wireless ad hoc networks employing a reactive routing protocol, namely, the dynamic source routing (DSR) protocol. The investigation proposed by Balakrishnan et al. is based on the concept of low-rate DoS attacks targeted at transmission control protocol (TCP) flows, named shrew attacks, which were proposed by Kuzmanovic (2006). NFJ is a scheduled jammer which targets the periodic operation of the routing protocol residing in the network layer. It is energy efficient and difficult to detect as a result of the short, infrequent, low-power jamming pulses broadcast by the jammer.

The jamming technique proposed in this paper is unique with respect to the approach and method used to implement the NFJ. The effectiveness of the proposed technique is investigated in WMNs employing a proactive routing protocol. NFJ has only previously been tested in wireless ad hoc networks which employed a reactive routing protocol as shown in Balakrishnan et al. (2012). Furthermore, the effectiveness of the jamming technique presented in this paper is demonstrated by analysing not only the overall throughput of the network, but also the energy expended by the jamming nodes, thereby enhancing the uniqueness of this paper. In addition, this paper reports on the probability of detecting the jamming nodes in comparison to other jamming techniques namely, *constant jamming*, *random jamming* and *deceptive jamming*.

In summary, this paper investigates the effectiveness of NFJ targeting the proactive optimized link state routing (OLSR) protocol for various WMN topologies namely, stack, half-diamond, full-diamond, random, and full-mesh topologies. OLSR is an optimisation of a pure link state protocol and makes use of multipoint relaying technology to efficiently and economically disseminate control information throughout the network. It is therefore well suited for large and dense wireless mesh networks (Jacquet and Muhlethaler, 2001). The effects of changing several parameters pertaining to the jamming technique are analysed in terms of network performance. A comparison of the NFJ to constant, deceptive and random jamming techniques is also presented.

2. Method

The proposed jamming technique targets the OLSR protocol in order to prevent the reception and transmission of protocol control packets from neighbouring nodes. The control packets that are targeted are the neighbour discovery packets, or the *Hello* packets. As a result, incomplete topological information is distributed throughout the network. This then facilitates the propagation of partial routing tables amongst the nodes in the network. Due to the fact that not all routes are available, packets are dropped and a significant degradation in network communication is observed. It is important to note that this jamming technique can potentially be applied to any periodic routing protocol in which the protocol specific neighbour discovery packets are targeted. Examples of period routing protocols include the Routing Information Protocol (RIP), Internet Gateway Routing Protocol (IGRP), and Exterior Gateway Protocol (EGP). The Ad-hoc On-Demand Distance Vector (AODV) protocol and variations thereof share some common characteristics with proactive routing protocols and can also be targeted by this jamming attack (Ong et al., 2011).

2.1. Objective

The objective of this work is to propose and investigate a jamming technique that is energy efficient, has a low probability of

Download English Version:

https://daneshyari.com/en/article/459707

Download Persian Version:

https://daneshyari.com/article/459707

Daneshyari.com