Journal of Information Security and Applications 38 (2018) 40–49

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

Network layer attacks and countermeasures in cognitive radio networks: A survey

Mounia Bouabdellah[a,b,*], Naima Kaabouch[b], Faissal El Bouanani[a], Hussain Ben-Azza[c]

[a] ENSIAS, Mohammed V University, Rabat, Morocco
[b] Department of Electrical Engineering, University of North Dakota, Grand Forks ND, USA
[c] ENSAM, Moulay Ismail University, Meknes, Morocco

ARTICLE INFO

Article history:

Keywords:
Cognitive radio
Security
Network layer

ABSTRACT

Spectrum scarcity is the principal motivation behind the development of cognitive radio. This technology introduces new functionalities at the physical, medium access control, and network layers of the TCP/IP protocol stack. These functionalities can be subject to new security threats. Most of the existing works in cognitive radio focused on the security issues in both the physical and medium access control layers. However, threats related to the network layer have not been studied despite its importance in establishing communication between different users in cognitive radio networks. In this paper, we classify and give an overview of attacks that target the network layer functionalities of cognitive radio networks. We discuss the existing detection techniques and countermeasures and highlight the main security challenges for such networks.

1. Introduction

Cognitive radio (CR) is a promising technology that aims to solve the problem of spectrum scarcity. This technology allows an opportunistic use of the spectrum where unlicensed users called secondary users, SUs, can transmit in licensed bands without causing harmful interference to licensed users called primary users, PUs [1–3]. Communication between nodes in cognitive radio networks (CRN) uses the TCP/IP protocol stack with additional functions in the physical and medium access control (MAC) layers. Fig. 1 shows the CR layers that have been modified to allow a dynamic access to the radio spectrum. The CR physical layer new functionalities include spectrum sensing and data transmission [3]. The MAC layer new functionalities are spectrum sensing, spectrum decision, spectrum sharing, and spectrum mobility [4]. The functionalities of the network layer are similar to traditional wireless networks the only difference is that the routing function is affected by the spectrum availability [5].

A number of papers related to security in CRN have been published [6–27]. For instance, the authors of [6–15] described the physical-layer attacks in CRN, including primary user emulation, objective function, overlapping secondary user, and jamming attacks. The authors of [16–25] gave an overview of attacks targeting the MAC layer such as the control channel saturation, control channel jamming, and spectrum sensing data falsification attacks. However, attacks targeting the network layer have received insufficient attention [26,27]. Moreover, these papers discuss only the attacks that are similar to those in traditional wireless networks and they focus only on the attacks targeting the routing function. Furthermore, the discussed attacks do not take into consideration the specifications of the cognitive radio network.

The network layer in CRN allows establishing a communication between remote nodes. The nodes participating in the data packet forwarding from source to destination are required to release the used channel as soon as a PU activity is detected on that channel. Thus, these new specifications give the opportunity to new security threats.

This article provides a comprehensive survey of attacks targeting the network layer in CRN. The classification of these attacks is performed based on the network layer functionalities. Some of these attacks can be launched only in CRN and others are similar to those that target the traditional wireless networks. This article explains how these attacks can be perpetrated in CRN by exploiting the characteristics of such networks. To the best of our knowledge, this is the first work that focuses on the attacks targeting the network layer in CRN.

The remainder of this paper is organized as follows. In section II, we provide an overview of the network layer functionalities in CRN. In section III, we classify attacks targeting the CR network layer based on its different functionalities. In section IV, we describe the detection techniques and countermeasures to mitigate

* Corresponding author.
E-mail address: mounia_bouabdellah@um5.ac.ma (M. Bouabdellah).

https://doi.org/10.1016/j.jisa.2017.11.010
2214-2126/

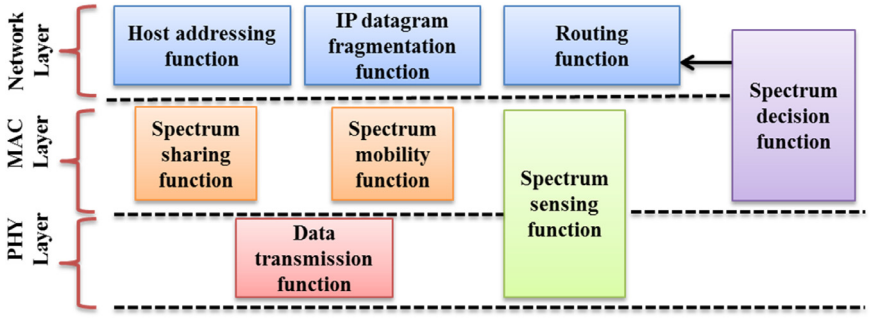

Fig. 1. Functions of physical, MAC, and network layers in CRN.

these attacks. In section V, we compare the attacks in terms of impacts; we also provide a comparison of the existing detection techniques and countermeasures to counter each attack. In section VI, we describe the challenges to secure the network layer functionalities. Finally, we end with a brief conclusion.

2. Network layer functionalities of cognitive radio systems

Communication between CRN nodes is established by executing the functions provided by the network layer. These functions include host addressing, IP datagram fragmentation, and routing of data packets from a source node to a destination node by using multi-hop routing protocols [26].

Host addressing is the first executed network layer function that assigns a unique logical address to CRN nodes. The common protocol used to perform the host addressing is the internet protocol (IP) which consists of two versions: the IPv4 and the IPv6 [27]. The proliferation of mobile devices introduced an exhaustion of IPv4 addresses which are of 32 bits. The IPv6 was proposed to solve this limitation of IPv4 by using 128-bit address [28]. In addition, IPv6 provides additional features such as stateless address auto-configuration [28], which allows nodes to automatically generate an IPv6 address by using the neighbor discovery protocol [28].

The IP datagram fragmentation function allows a packet that exceeds the maximum transmission unit to be divided into small fragments and sent through different transmission media [29]. Once the intended destination node receives all fragments, it starts the reassembly process. The fragmentation in IPv6 is performed by a sub-layer located between the network and MAC layers [30].

The routing function uses three processes: path determination, data packet forwarding, and route maintenance [31]. The first process determines a route from source to destination according to some specific metrics such as end-to-end delay and throughput. The second process allows data packets forwarding from source to destination through a selected path while the third process monitors the status of the established route.

The main difference between the routing protocols in traditional wireless networks and those in CRN is that the CR-based routing protocols must take into consideration the spectrum availability, the channel used by each SU, and the activity of PUs to select the best route toward a specific destination. According to [6], CR routing protocols can be classified into three classes: routing with spectrum decision, routing with joint spectrum decision and PU awareness, and routing with joint spectrum decision and reconfigurability. In the first category, the spectrum and path selection are performed jointly. The second class consists of selecting the route that avoids the regions known to have high PU activity. The third class of CR routing protocols has the ability to recover from changes in the spectrum caused by PU activity.

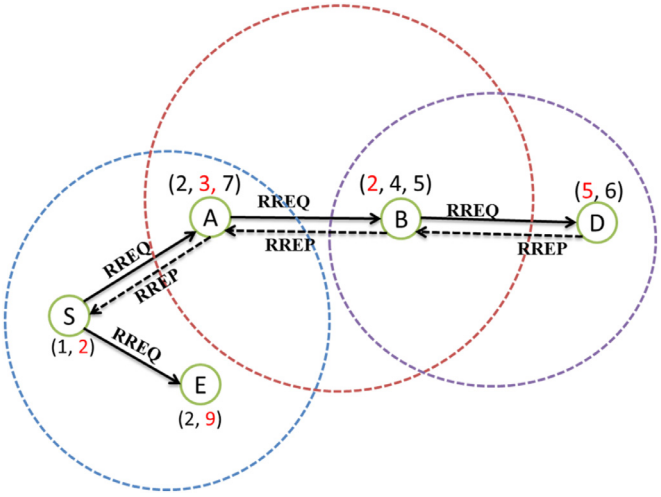

Fig. 2. Example of a CR routing protocol with spectrum decision.

Fig. 2 shows an example of a CR routing protocol with spectrum decision. Each CR node has a set of available channels and uses one of these channels. For instance, the available channels of node A are (2, 3, 7) and the channel being used is 3. When the source node S wants to send data packets to the destination node D it starts the process of path determination by broadcasting a route request (RREQ) packet. The source node S inserts its spectrum-related information in RREQ packets. When the intermediate nodes A and B forward the RREQ packets, they also include their own spectrum-related information. Once the destination node D receives the RREQ packets it decides on the channel to be used for data transfer on the selected path and inserts the information about the chosen channel in the route reply (RREP) packet. This packet is sent back to the source node through nodes B and A. Once these intermediates SUs receive the RREP, they assign the channel to themselves based on the information contained in the RREP. Once the route from source node S to destination node D is established the data packets forwarding begin using the selected path and the chosen channel in this path.

In CRN, communicating with a switching node is complicated, since this node switches channels frequently to support multiple flows on different channels. Thus, sending packets to a switching node can fail if this node is listening to another channel. To address this issue some CR routing protocols use leave/join messages to inform switching nodes' about the working channels. Before switching to a new channel, a switching node broadcasts a leave message on the current channel. After switching to a new channel, this node broadcasts a join message on the new channel. When an SU receives a leave message from a switching node, it does not send packets to this node before receiving the join message from it [23].