Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

Trust-based multi-hop cooperative spectrum sensing in cognitive radio networks

Adele Khalunezhad, Neda Moghim*, Behrouz Shahgholi Ghahfarokhi

Faculty of Computer Engineering, Department of Information Technology, University of Isfahan, Iran

ARTICLE INFO

Article history:

Keywords:
Cognitive radio
Multi-hop cooperative spectrum sensing
Data falsification attack
Trust and reputation management

ABSTRACT

Cooperative spectrum sensing is one of the solutions for cognitive radio networks, which can resolve the uncertainty of stand-alone spectrum sensing. It means that each secondary user senses defined spectrum bands for the unused spectrum detection and shares its sensing results with the others to improve the accuracy of spectrum sensing. Due to the presence of malicious secondary users and their fake sensing reports, various forms of attacks will be encountered that reduce the performance of cooperative spectrum sensing. Spectrum sensing data falsification attack (SSDF) is one of the attacks that some research works have been presented to defend against it, based on trust and reputation management (TRM). Previous works assume that all the secondary users are in the transmission range of each other and one-hop sensing reports are provided. However, multi-hop dissemination of sensing reports is a necessary scenario for the secondary users with limited energy sources and its security attacks are very challenging to be encountered. In this paper, a trust-based multi-hop cooperative spectrum sensing method is proposed to deal with SSDF attack. Simulation results show that this scheme improves spectrum sensing accuracy and reduces.

1. Introduction

With the rapid development of wireless communication technology and the huge demands for wireless applications, radio spectrum usage has increased significantly. Radio spectrum is divided into licensed and unlicensed bands. Since licensed bands are assigned statically, their spectrum utilization is sometimes low. Utilization of the licensed bands varies in the range of 15% to 85%, while the unlicensed bands often face congestion and spectrum scarcity [1]. Therefore, cognitive radio networks have emerged to improve the utilization of the radio resources and to resolve the spectrum scarcity problem. It allows wireless devices to access the unused licensed spectrum opportunistically, without causing any harmful interference for the licensed users. Licensed users are called Primary Users (PUs) and cognitive users that exploit the spectrum opportunistically are called Secondary Users (SUs) [2]. Spectrum sensing is a key process in cognitive radio networks in which various frequency bands are scanned for possible unused spectrum bands (spectrum holes). Cooperative Spectrum Sensing (CSS) is an efficient spectrum sensing scheme to improve the accuracy of sensing. CSS can enhance the sensing performance by exploiting the spatial diversity of the observations of the SUs, located in diverse locations. In CSS, SUs share their sensing data to make a joint decision with higher accuracy compared to the individually derived decisions [1–3].

However, such cooperation has inevitably laid SUs open to attacks [2,3]. A CSS action is often randomly established among SUs that are unknown to each other. This offers opportunities to the malicious SUs to launch Spectrum Sensing Data Falsification (SSDF) attack to mislead the spectrum decision of other SUs. Even few malicious SUs can significantly degrade the performance of CSS. Therefore, it is a challenging issue to encounter SSDF attacks in CSS [2,3].

Trust schemes are used by recent researchers to deal with the misbehaving users and to improve the accuracy level of the sensing data [3]. Trustworthiness of the SUs is evaluated according to their past behaviors and reported sensing results of a low trusted SU will have less impact on the final decision about the spectrum holes. Trust level of the SU is calculated based on the proximity of its reports to the final decision. However, most of the proposed trust schemes assume that all the SUs are able to sense the signal of all PUs and they are also in the transmission range of each other [3]. If all the SUs are not able to sense the signal of the primary users and if they are not in the transmission range of each other, sensing results should be reported in a multi-hop manner and the existing methods will not work well for such a scenario. In this paper, a new TRM scheme is proposed to deal with SSDF attack in

[*] Corresponding author.
E-mail address: n.moghim@eng.ui.ac.ir (N. Moghim).

https://doi.org/10.1016/j.jisa.2018.07.007
2214-2126/© 2018 Elsevier Ltd. All rights reserved.

multi-hop cooperative spectrum sensing scenario. In this scheme, each received sensing report is weighted based on two trust values, i.e., trust of the sensor node and trust of the multi-hop path between the sensing SU and the decision maker SU. Trust of the multi-hop path is evaluated based on the forwarding trusts of the SUs along the path.

The rest of the paper is organized as follows: Related work is reviewed in Section 2. System model and also the proposed scheme are presented in details in Section 3. Simulation results are given in Section 4. Finally, the paper is concluded in Section 5.

2. Related work

In Section 2.1, the methods that are used for the sensor nodes' trust calculation in cooperative spectrum sensing are explained. Furthermore, to calculate the multi-hop path trust value, trust methods utilized for the packet forwarding in multi-hop ad-hoc networks were considered that are represented in Section 2.2.

2.1. Trust methods in cooperative spectrum sensing

In [4], a Weighted Sequential Probability Ratio Test (WSPRT) scheme is proposed based on data gathering technique to identify malicious users. In this paper, fusion center compares final decision with the sensing results of the SUs. If they are the same as the final decision, reputation of the SUs will be increased and otherwise, the reputation will be decreased. Afterward, the reputation of SUs is used to make the final decision about spectrum holes. A weight is assigned to each SU regarding its reputation. Honest SUs gain more weight to be more effective in the final decision.

In [5], a user-centric misbehavior detection scheme is presented. SUs consider their own sensing results as the valid results and compare it to the sensing reports of the others. Malicious and honest SUs are determined based on the correlation difference of the results, which is calculated during the comparison.

In [6], dynamic witness selection scheme is presented based on clustering. This scheme is a protection mechanism for the collusive behavior of SUs and Beta reputation system [7] is used as the basis for the calculation of direct and indirect reputation. In his method, each SU determines the trustworthiness of the other SUs according to its local observations of their past cooperative spectrum sensing operations. Then, it sends its own sensing report along with the trustworthiness of its neighboring SUs to the fusion center (each SU may be a fusion center). Fusion center detects malicious and honest users by means of its direct and indirect reputation reports and via clustering. However, all SUs are assumed within each other's transmission range in this work.

In [8], a trust evaluation scheme is proposed via anomaly monitoring to identify malicious users. In this method, each node sends its own sensing results to its neighbors as a binary vector. Decision-maker SU predicts its neighbors' sensing report vector, considering its distance to the intended neighbors, its received signal strength and the calculated distance of the neighbors from the primary station. The predicted vector is compared to the neighbors' sensing results and the number of true/false reports is determined to update the trust coefficient of the neighboring nodes.

In [9], a secure distributed cooperative spectrum sensing strategy is proposed based on a dynamic reputation model. This strategy detects malicious users through reputation mechanism which is based on the subjective logic. A belief metric that is called the opinion is used to declare the SUs' reputation. Each neighbor user's opinion is specified based on the comparison of the final spectrum decision with the received sensing results from it. Then, reputation value of the SU is evaluated based on its current opinion value affected by the temporal distance of the past and current opinions.

In [10], a trust-based data fusion scheme is proposed based on mechanism design theory to detect malicious users and to encourage SUs to send true sensing reports. In this method, SUs send their sensing results accompanied by their sensing capability to the other users. Sensing capability is estimated by the false alarm and missed detection probabilities. Therefore, the closer each SU's sensing capability is to 1, the more confident is its sensing result. However, a malicious user may intentionally report a higher sensing capability to affect the final decision. Therefore, each SU keeps trust scores of the other SUs too. In the process of the final decision, if the decision maker has a high sensing capability, it will choose its own sensing result as the final decision; otherwise, it will use the sensing results of the users with higher sensing capabilities. Finally, trust scores will be updated by comparing the final decision with the sensing results of the SUs.

To the best of our knowledge and as it is shown in Table 1, the research works on distributed cooperative spectrum sensing have generally assumed one-hop network model [3]. It was assumed that all the SUs are in the transmission range of each other (an optimistic assumption). Therefore, they are able to detect malicious SUs simply. However, there are situations that SUs are not in the transmission range of each other and sensing reports should be transmitted in a multi-hop manner. Therefore, existing trust-based CSS methods are not efficient. In fact, current mechanisms have not considered the trust of the relay SUs, while malicious SUs may change sensing reports during relaying. Therefore, it is required to offer an appropriate trust-based mechanism for the distributed cooperative spectrum sensing by considering the trust of the relay SUs. For this purpose, secure routing methods in MANET that employ trust mechanisms will be studied in the next section.

2.2. Trust-based routing in MANETs

In this paper, the secondary users are assumed to be a MANET and so communicate in an ad-hoc manner. MANET is a self-configuring mobile network without any fixed infrastructure. As we assume to have a multi-hop cooperative spectrum sensing in such a MANET, nodes should operate as a router to forward the packets in the network. MANET is vulnerable to routing attacks [14] and nodes may intend to save their energy. Therefore, they do not cooperate in the packet transmission. To encounter such problem, trust and reputation management methods are used.

In [11], a cooperative routing scheme is proposed based on trust and energy management. Trust value of a neighboring node is evaluated by monitoring the node's behavior and regarding the successful and dropped packets ratio. If the successfully forwarded packets of a neighbor node are more than the dropped ones, direct trust value of the neighbor node will be increased. Otherwise, direct trust value will be decreased. Final trust value of each neighboring node is evaluated based on the weighted direct and indirect trust. Indirect trust is the average of the trust values reported by the other neighboring nodes about the evaluated neighbor node. Finally, trust value of the path is calculated based on the average trust value of the intermediate nodes along the path.

In [12], a trust-based routing scheme is proposed. First of all, a secure path is selected by sending an encrypted value to a specific destination. During encrypted data forwarding to the destination, each node evaluates neighboring nodes' trust value by monitoring their behavior. Trust value of the neighbors is calculated regarding the number of packets successfully sent/dropped by the evaluated node comparing to the number of packets sent by the evaluating node. Final trust value of the nodes is formed based on the average of their direct and indirect trust. If the neighboring node's trust value is less than a threshold value, the evaluating node should choose another trustworthy path.