A Novel Trust Algorithm for Cognitive Radio ad-hoc Networks

Raghav Gaur
Michigan State University
East Lansing, USA
gaurragh@msu.edu

Katherine Perry
Michigan State University
East Lansing, USA
perryk12@msu.edu

Nathan Woods
Michigan State University
East Lansing, USA
woodsna1@msu.edu

***Abstract*— Cognitive radios (CRs) have great potential to reduce network congestion on unlicensed radio frequencies. Applying CR to mobile ad-hoc networks (MANET) introduces a solution to radio interference for mobile networks. Our group proposes a new trust algorithm to address spectrum sensing data falsification (SSDF) security concerns in MANET-CR. In this document, we introduce MANET-CR, present an extensive review of related work, and propose a project which will address key limitations of current MANET-CR research.**

Keywords—cognitive radio, decentralized, consensus, security, spectrum, falsification

I. Introduction

Digitization, only after the agricultural revolution and invention of the printing press, has been the single most transformative event in human history. The past 20 years have seen demand for stable and safe internet access increase rapidly and at an increasing rate. This growth has been curbed by the reality that not all areas that demand internet access have the infrastructure (or capital to create and maintain said infrastructure) needed for such access. Mobile ad hoc networks with cognitive radios (MANET-CRs) allow us to create flexible and powerful networks where such infrastructure does not exist or is not economically viable. Research into this area is important as it can potentially allow for more widespread, safe connection between mobile devices.

These networks, while powerful, are still susceptible to attack and exploitation by malicious users. While certain schemes have been put forth to handle this, many of these schemes are not proactive. New research, however, has yielded more robust methods of security — such as Punishment Schemes (PS) and Decentralized Schemes (DS). We will be directing our project to investigate these schemes. Such investigation is important as by combining these two schemes, we can overcome their individual limitations and yield a single, more robust scheme that facilitates the safe use of MANET-CRs.

II. Background

A. MANET – CR

A Mobile Ad Hoc Network (MANET) is a wireless, unfixed (continuously self – reconfiguring, dynamic topology), and scalable network of mobile devices. As each constituent device moves toward or away from one another in the network, links between devices are broken and new ones are formed ad hoc – spontaneously. This allows for the MANET to easily reconfigure itself and for it to be formed without infrastructure (such as cell towers, MicroCells, etc.). Subsequently MANETs are an economical and straightforward solution for when data must be shared between parties but a traditional network is unavailable.

Delving into greater detail, each device (or node) in a MANET is identical, serving as both a host and a router. This allows for messages between two devices on the network, if they are out of range from one another, to utilize multi-hop routing in order to interact. [1]

There exists, however, one important caveat that must be taken into consideration when making such extensive use of mobile devices — mobile devices are only allowed to use certain frequencies which are becoming increasingly congested. Certain services, such as streaming music or videos through the internet, require substantially more bandwidth than what is readily available. Cognitive Radio (CR) breaks down this barrier faced by mobile devices by allowing such devices to utilize frequencies typically reserved for other services such as television. Here the word “radio” refers to any form of wireless communication. Cognitive radios are said to be “cognitive” as they are able to “understand” different forms of radios such as a wireless network made up of satellites, televisions, mobile phones, etc. which, through it, are able to work in tandem with one another. [2]

MANET-CRs, then, are MANETs which have access to the full spectrum of frequencies via the use of cognitive radios. [1][2]

B. Punishment Schemes

Traditionally, the detection of malicious users in a network has been based on the location of said users and the likelihood of an attack. This method, while it is not without merit, is not a proactive approach to securing an MANET-CR system.

To address this, Li et al. proposed a punishment scheme (PS) in their 2014 paper “Security Management Based on Trust Determination in Cognitive Radio Networks”. [3]

The PS collects data about users on a local network via infrastructure referred to as a cluster header. These cluster headers send said data to fusion centers (FC) which compute cognitive trust values (CTV) for each user on the network. These values are, as the name suggests, a measure of how likely a user is to engage in malicious activities. As the CTV decreases for a user, they face increasingly harsh punitive consequences until their access to a network is ultimately cut off. Likewise, the reverse is true.

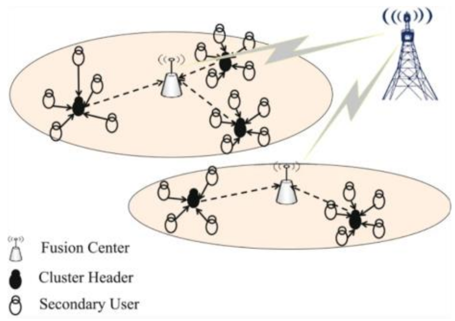

Fig. 1. Fusion center and cluster header architecture.

C. Decentralized Schemes and SSDFs

While PS are an improvement over the more traditional methods of malicious user detection, they undo one of the main strengths of a MANET-CR. That is, PS are less flexible and generally require stable infrastructure. Decentralized schemes reintroduce the flexibility lost with PS and if used in conjunction, can allow for on the fly MANET-CR networks to combat attacks such as SSDFs.

A spectrum sensing data falsification (SSDF) attack is the most frequently used method to disrupt a network. This attack consists of a malicious user distributing false information about the primary user's presence on a channel.

III. Related Work

Many studies have addressed mitigation of SSDF attacks in centralized cognitive radio networks (CRN). Most rely on extensive computation conducted on a fusion center (FC), central servers responsible for allocating available spectra to the network. Our survey of existing work includes several studies of centralized networks. Despite differences in architecture, many security concepts for CRN are similar between centralized and decentralized networks. Two key components in SSDF management are malicious device (MD) detection and trust determination.

A. Centralized Networks

Hyder et al. [4] utilize clustering to group malicious devices and honest cognitive users (CU). This clustering approach is effective for identifying MD without comparison to a global decision value for the channel's availability, but requires a FC with stored data about each CU to run the machine learning algorithm. Its effectiveness is reduced by the inherent limitations of clustering, including identifying the number of clusters to use.

Galeazzi et al. [5] move a step toward a decentralized trust algorithm for identifying MD, with each CU maintaining and updating trustworthiness information about its neighbors. Their proposed algorithm uses a FC to evaluate trustworthiness of each node and assign resources. This proposal may more accurately identify MD, but will not apply in situations where a FC is impractical. Additionally, this paper assesses performance only when MD falsely report the opposite of reality. More advanced SSDF attacks are not considered.

Li et al. [3] develop a new approach of security management based on trust determination in which cognitive trust value is based on authentication, interaction, configuration, trust value collection, storage and update, and punishment. This approach depends on a FC capable of running demanding software and managing the connection of each CU.

Chen et al. [6] apply a novel approach to mitigation of SSDF attacks using a joint spectrum sensing and resource allocation algorithm. This study combines advances in MD detection and punishment. This approach is extremely effective when MD can be accurately detected, because it cuts off unreliable nodes from usage of the available spectrum. MD identification relies on comparison of each CU's local decision to the global decision of a FC.

Biswas et al. [7] present a novel trust algorithm in which the confidence of the global decision is incorporated in the trust weighting for each iteration. This is a new approach which results in less penalty for suspected MD when the FC is unsure of the PU presence.

B. Decentralized Networks

The effectiveness of SSDF attacks is amplified in MANET-CR, which rely on peer-to-peer spectrum sensing data sharing without a FC. The next group of studies specifically considers security in decentralized architectures.

Yu et al. [8] present a framework for consensus-based decision making in MANET-CR utilizing advances in bio-based consensus research. Their algorithm is effective in networks with moderate interconnectivity, but does not address situations with high or low interconnectivity. In each iteration, a static number of reports are ignored.

Feng et al. [9] introduce a Distributed Trust Evaluation (DTE) scheme for MANET-CR which relies on neighbor help to evaluate trustworthiness of CU. Temporary fusion centers (TFC) are dynamically elected by the MANET-CR, simplifying routing and spectrum assignment. This approach is limited by the computational abilities of the TFC, which may become overloaded as the system grows.

Sivakumaran, Alfa, and Maharaj [10] assess the performance of a decentralized CRN using the Neyman-Pearson Belief Propagation (NPBP) algorithm to perform spectrum sensing. They find this algorithm to be extremely vulnerable to false-alarm SSDF attacks. The algorithm includes no tracking of CU trustworthiness over time, and thus is unable to identify MD.

Ngomane, Velempini, and Dlamini [11] present a decision-making algorithm combining a modified z-test with the q out of m rule for determining the presence of a Primary User (PU) in MANET-CR. This algorithm proves effective for small networks, but as the number of CU increases, many false alarms are reported.

Taggu and Marchang [12] combine a Hidden Markov Model and robust Machine Learning algorithms to classify MU and normal SU. These algorithms operate on a central FC accessed via a common control channel. The algorithm performs well even with many attackers, but is computationally expensive. This approach also relies on accurately predicting the behaviors of attackers to generate a synthetic dataset that mimics reality.

The current body of work in MANET-CR security research is fairly comprehensive, but leaves room for improvement. Many of the existing decentralized algorithms are simplistic, and usually don't have any sort of trust history for the nodes in the network. Centralized networks often rely on computationally expensive algorithms or lots of data. They cannot be applied to situations where a static FC does not exist, and don't extend well to networks made up of highly mobile devices such as autonomous vehicles.

IV. Proposal

We will contribute a novel trust algorithm to reduce the impact of SSDF attacks on Cognitive Radio Networks. To create this trust algorithm, we will apply a punishment scheme to a distributed approach. This scheme must be lightweight, and run with minimal computing power in a sensor network. We will adopt and adapt the punishment scheme of the paper "Security management based on trust determination in cognitive radio networks" by Li et al. [3] in which greedy, malicious, and malfunctioning users were punished differently by the FC. In our scheme, we will focus on data falsification attacks, and punish Selfish SSDF, Interference SSDF, and Confusing SSDF differently, scaling punishment by severity of the offense.

Additionally, we move a step further than Yu in 2009 [8], Biswas in 2020 [7], and Galeazzi et al. in 2021 [5] toward a decentralized trust algorithm by eliminating the need for a Fusion Center. Instead of secondary users reporting about their neighbors' reputations to an FC, which then fuses data and assigns available resources, we propose applying a lightweight tri-message synchronization method for sensor networks [13]. Instead of the time synchronization that has already been implemented using this approach, we modify the tri-message approach to trust synchronization. This accomplishes a system of peer monitoring to determine a consensus of trust values. Input from highly trusted users will be weighted more heavily in order to prevent malicious users from overtaking the trust system for their own benefit. In terms of allocating available channel resources, we aim to implement an innate distributed priority rule which allows secondary users with higher cognitive trust values to use available resources first. The punishment scheme will be realized by peer secondary users decrementing the trust value of a user engaging in SSDF attacks.

This combination of an optimized punishment scheme and a more fully distributed model has not yet been explored. In the centralized scheme research, the limitation was the need for a Fusion Center which limits the capacity for distribution of the algorithm. [3] is limited by lack of punishment optimization, along with requiring expensive computing resources at the FC. Through our proposal of a lightweight distributed trust algorithm, we address those weaknesses.

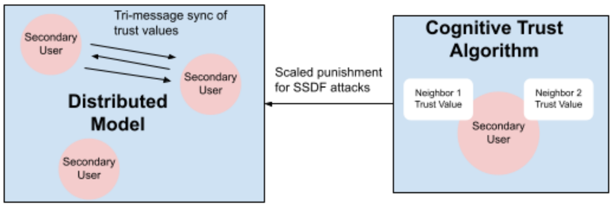

Fig. 2. Illustration of proposed network.

References

[1] LearnEveryone. (n.d.). What is Manet - Mobile Adhoc Network. www.youtube.com. Retrieved February 24, 2022, from https://www.youtube.com/watch?v=fqP_BdFvyUQ&ab_channel=LearnEveryone.

[2] Nokia Research. (n.d.). Nokia Research Center presents Cognitive Radio. Nokia Research Presents. Retrieved February 25, 2022, from https://www.youtube.com/watch?v=20wqZZaXG9o&ab_channel=JarkkoSaunamaki.

[3] Li, J., Feng, Z., Wei, Z. et al. Security management based on trust determination in cognitive radio networks. EURASIP J. Adv. Signal Process. 2014, 48 (2014). https://doi.org/10.1186/1687-6180-2014-48

[4] C. S. Hyder, B. Grebur, L. Xiao and M. Ellison, "ARC: Adaptive Reputation based Clustering Against Spectrum Sensing Data Falsification Attacks," in IEEE Transactions on Mobile Computing, vol. 13, no. 8, pp. 1707-1719, Aug. 2014, doi: 10.1109/TMC.2013.26.

[5] A. Galeazzi, L. Badia, S. -C. Chang and F. Gringoli, "Reputation-Based Spectrum Data Fusion against Falsification Attacks in Cognitive Networks," 2021 19th Mediterranean Communication and Computer Networking Conference (MedComNet), 2021, pp. 1-8, doi: 10.1109/MedComNet52149.2021.9501276.

[6] H. Chen, M. Zhou, L. Xie, K. Wang and J. Li, "Joint Spectrum Sensing and Resource Allocation Scheme in Cognitive Radio Networks with Spectrum Sensing Data Falsification Attack," in IEEE Transactions on Vehicular Technology, vol. 65, no. 11, pp. 9181-9191, Nov. 2016, doi: 10.1109/TVT.2016.2520983.

[7] R. Biswas, J. Wu, X. Du and Y. Yang, "Mitigation of the spectrum sensing data falsifying attack in cognitive radio networks," Cyber-Physical Systems, vol. 202, pp. 159-178, doi: 10.1080/23335777.2020.1811387

[8] F. R. Yu, H. Tang, M. Huang, Z. Li and P. C. Mason, "Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios," MILCOM 2009 - 2009 IEEE Military Communications Conference, 2009, pp. 1-7, doi: 10.1109/MILCOM.2009.5379832.

[9] J. Feng, X. Du, G. Zhang and W. Shi, "Securing multi-channel selection using distributed trust in cognitive radio ad hoc networks," in Ad Hoc Networks, vol. 61, pp. 85-94, 2017, https://doi.org/10.1016/j.adhoc.2017.03.009

[10] A. Sivakumaran, A. S. Alfa and B. T. Maharaj, "An Empirical Analysis of the Effect of Malicious Users in Decentralised Cognitive Radio Networks," 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), 2019, pp. 1-5, doi: 10.1109/VTCSpring.2019.8746414.

[11] I. Ngomane, M. Velempini and S. V. Dlamini, "The detection of the spectrum sensing data falsification attack in cognitive radio ad hoc networks," 2018 Conference on Information Communications Technology and Society (ICTAS), 2018, pp. 1-5, doi: 10.1109/ICTAS.2018.8368742.

[12] A. Taggu and N. Marchang, "Detecting Byzantine attacks in Cognitive Radio Networks : A two-layered approach using Hidden Markov Model and machine learning," Pervasive and Mobile Computing, vol. 77, 2021, https://doi.org/10.1016/j.pmcj.2021.101461

[13] Tian, Jiang, Liu, Wang "Tri-Message: A Lightweight Time Synchronization Protocol for High Latency and Resource-Constrained Networks," 2009 IEEE International Conference on Communications, 2009, pp. 1-5, doi: 10.1109/ICC.2009.5199544

[14] Vasiliou, Alexandros & Economides, Anastasios. (2007). Mobile collaborative learning using multicast MANETs. IJMC. 5. 423-444. 10.1504/IJMC.2007.012789.