opinion

iMedPub Journals
www.imedpub.com

American Journal of Computer Science and Information Technology
ISSN 2349-3917

2022
Vol.10 No.10:001

Enhance the Wireless Network Security by Reinforcement Learning

K Shitharth*

Department of Computer Science and Engineering, Kebri Dehar University, Kebri Dehar, Ethiopia

***Corresponding author:** K Shitharth, Department of Computer Science and Engineering, Kebri Dehar University, Kebri Dehar, Ethiopia Email: Shitharthroy@yahoo.com

Received date: September 02, 2022, Manuscript No. IPACSIT-22-15210; **Editor assigned date:** September 05, 2022, PreQC No. IPACSIT-22-15210 (PQ); **Reviewed date:** September 12, 2022, QC No IPACSIT-22-15210; **Revised date:** September 20, 2022, Manuscript No. IPACSIT-22-15210(R); **Published date:** October 03, 2022, DOI: 10.36648/ 2349-3917.10.10.1

Citation: Shitharth K (2022) Enhance the Wireless Network Security by Reinforcement Learning. Am J Compt Sci Inform Technol Vol. 10 Iss No. 10:001.

Description

Shadowing, path loss, and fading are just a few of the channel impairments that can occur in wireless networks. The direct transmission between the sender and the receiver may not achieve an acceptable signal quality because of shadowing, path loss, and fading. Because it can take a different route to the destination, cooperative communication has provided appealing solutions in that scenario. Through cooperative spatial diversity, cooperative communication improves the channel's stability. New security requirements and challenges have emerged as a result of recent advancements in the cellular network. Power efficiency, reliability, and spectral efficiency can all be improved by cooperative communications; however, eavesdroppers frequently target it. As a result, the research's goal is to improve the secrecy capacity of wireless networks with moving cooperative communication devices because of the need for secure wireless mobile networks. Reinforcement learning, which learns the transmit parameters in response to the interaction of the transmitter, receiver, relay-node, and eavesdropper devices, is the organizing principle of the method that has been proposed to improve the security of wireless networks. The simulation results have demonstrated that the proposed method has increased the legitimate receiver's level of secrecy.

Objectives of the Next Generation of Wireless Networks

Between the sender and the receiver, cooperative communication introduces a relay node, an intermediate device. The broadcast nature of wireless communication, which enhances spectral efficiency, applies to cooperative communication; improves power proficiency and builds the correspondence dependability. Due to the multiple links between the sender-relay node and relay node-receiver in cooperative communication, the eavesdropper has a better chance of gaining access to the information. As a result, the communication is vulnerable to cyberattacks in which the adversary ultimately aims to destroy, delay, or steal the transmitted data. The signal in wireless networks travels from a source to a destination *via* Radio Frequency (RF). Mobility is supported by wireless communication, which may have made wireless communication the most appealing option. Wireless networks can now transmit a lot of data with good coverage thanks to 4G. The cutting edge remote organization objectives incorporate super thick arrangement which gives huge throughput as indicated by the 5G prerequisites. The low-power and large-scale connections that can accommodate a large number of terminals are the other objectives of the next-generation wireless network. Cooperative communication is necessary for the extremely dense deployment, high traffic, low power consumption, and large-scale connections. Eavesdroppers, on the other hand, have the ability to exploit information obtained either directly from the sender or from the relay node, making the cooperative mobile communication method susceptible to eavesdropping. Another crucial requirement for the future network is high reliability and low latency. This is anticipated to provide millisecond end-to-end delay and reliability guarantees for safety-critical applications like industrial controls and vehicle networking. Therefore, the objectives of the next generation of wireless networks include not only networks with increased bandwidth but also services of a higher quality.

A Novel Physical-Layer Security Strategy

Relay nodes, also known as two-hop communications, are now used in wireless communication to send signals to receivers together and evaluated a secure network with minimal routing energy. Cooperative jamming has been used in to make cooperative communication-based networks more secretive, but this method has required more power and required more computation. The physical layer security has been investigated and has achieved a higher level of secrecy. However, the scenario that has been investigated was on a fixed device that does not take advantage of the significance of the wireless network. A novel physical-layer security strategy that generates a key independent of channel variations has been utilized in a study. However, despite the relatively low level of secrecy, this still adds to the computational complexity. New security requirements and difficulties have emerged recently as a result of wireless networks. Shadowing, path loss, and fading are difficult barriers to cellular communication in wireless networks. These issues can be partially resolved through cooperative communication. Cooperative communication also improves reliability, power efficiency, and spectral efficiency; however, it is

highly vulnerable to security issues. As a result, in order to boost wireless networks' capacity for secrecy, this paper suggests using reinforcement learning. The results of the simulations show that the proposed method is ideal for increasing the secrecy capacity of mobile wireless networks.