Performance evaluation of cooperative mobile communication security using reinforcement learning

Gebrehiwet Gebrekrstos Lema\textsuperscript{a,}\textsuperscript{*}, Kiros Siyoum Weldemichael \textsuperscript{b}, Leake Enqay Weldemariam \textsuperscript{c}

\textsuperscript{a} School of Electrical and Computer Engineering, Mekelle University, Ethiopia
\textsuperscript{b} Mekelle Institute of Technology, Mekelle University, Ethiopia
\textsuperscript{c} Tigray Institute of Policy Studies, Mekelle, Ethiopia

ARTICLE INFO

Keywords:
Energy efficiency
Mobile network security
Reinforcement learning

ABSTRACT

In wireless networks, there are many channel impairments including shadowing, path loss, and fading. Due to the shadowing, path loss, and fading, the direct transmission between the sender and the receiver may not attain acceptable signal quality. In that case, the cooperative communication has shown attractive solutions because it can use an alternate route to the destination. Cooperative communication increases the stability of the channel by cooperative spatial diversity. Quite recently, the advancement in the cellular network has resulted in new security requirements and challenges. Cooperative communications can increase spectral efficiency, power efficiency, and reliability; however, it is often vulnerable to eavesdroppers. Hence, inspired by the need for safe wireless mobile networks, the objective of the research is to increase the secrecy capacity of the wireless networks when there are moving cooperative communication devices. The technique proposed to enhance the wireless network security is organized by reinforcement learning which learns the transmit parameters according to the interaction of the transmitter, receiver, relay-node, and the eavesdropper devices. The simulation results have shown that the proposed technique has enhanced the secrecy level of the legitimate receiver.

1. Introduction

Cooperative communication introduces an intermediate device (relay node) between the sender and the receiver. As cooperative communication applies, the broadcast nature of the wireless communication which improves spectral efficiency; enhances power efficiency and increases the communication reliability. In cooperative communication, due to the multiple links between the sender-relay node and relay node-receiver, the eavesdropper gets a better chance to access the information and hence the communication is vulnerable to cyber-attacks in which the enemy aims ultimately destroying, delaying, or stealing the transmitted information.

Wireless networks [1] make use of the Radio Frequency (RF) to transmit the signal from a source to a destination. Wireless communication support mobility [2] and perhaps this made the wireless communication attractive, by far. The 4G has enabled wireless networks to carry high data transmission and good coverage performance. The next-generation wireless network goals include ultra-dense deployment [3] which provides enormous throughput as specified by the 5G requirements. The other next-generation wireless network goals are the low-power and large-scale connections in which a large number of terminals can be deployed. The ultra-dense deployment, high traffic, low-power consumption, and large-scale connections are possible with cooperative communication. However, the cooperative mobile communication technique is vulnerable to eavesdroppers as the eavesdropper can exploit the information either directly from the sender or from the relay node.

The low latency and high reliability are also another stringent future network requirement. This is expected to provide millisecond end-to-end delay and reliability guarantees high demand for safety, such as vehicle networking and industrial controls. Hence, the next-generation wireless network goals are not only networks with wider bandwidth but also the advanced quality of services.

With the advancement of wireless communication, relay nodes (i.e., two-hop communications) are used to cooperatively transmit their signals to their receivers, [4]. A secure network, with minimum routing energy, has evaluated [5], and [6]. In [7], cooperative jamming has applied to enhance the secrecy capacity of cooperative communication-based networks, but this technique has faced both elevated power consumption and increased computational complexity.
The physical layer security is investigated and achieved better secrecy level [8], however, the scenario it has investigated was on a fixed device that doesn’t exploit the wireless network significance. A research [9], has applied a new physical-layer security approach that generates a key independent of channel variations. However, this still increases the computational complexity in addition to the insignificant secrecy level.

Quite recently (2018) [10,11], physical layer-based security techniques have shown attractive solutions. However, though the physical-layer network security issues have attracted many researchers they haven’t applied multiple solutions together to enhance the secrecy capacity and the machine learning for enhancing secrecy is not exploited. Though several researches are conducted on the physical layer network authentication using machine learning [12, 13, 14, 15], there was not much concern given on enhancing the secrecy using the channel impairment parameters. Authors [16], have tried to enhance the security of wireless sensor networks by detecting and then counteracting the denial of service attacks. However, the research didn’t discuss more on enhancing the signal at the legitimate user while lowering the SNR at the eavesdropper terminal.

For easier mobility communication, wireless communication network has become a crucial part of life. For effective wireless communication, there are many emerging wireless technologies including millimeter-wave communications, machine-type communications and physical layer wireless security [17], and [18]. Besides, machine learning has made wireless communication designs easy, [19, 20, 21]. The cooperative-jamming [22] and cooperative-relay [23] techniques are also evaluated to enhance wireless network security issues. The significance and design issues of the physical layer-based network security are also briefly discussed [24], and [25].

In physical layer security, rather than relying on the fact that the eavesdropper has no access to the keys and it has limited processing power to perform attacks against the encryption algorithms themselves, the goal is to minimize the ability of the eavesdropper to retrieve information (encrypted or not) from the channel used by the transmitter and the receiver. This way, messages can be transmitted confidentially without using an encryption key. This can enhance the security of the secret keys by providing an additional layer of obfuscation to the Hellman key exchange process. This and other system-related issues, such as key agreement, cross-layer design, authentication, etc. are discussed in [26]. The characteristics of the physical medium make it such that any receiver, legitimate or otherwise, hears a different version of the waveforms being transmitted. Confidentiality of data can be obtained by exploiting this difference to hide the transmission from unintended receivers. This is fundamentally different from the cryptographic assumption. In cryptography, the eavesdropper hears the same information as the receiver but it cannot decrypt it without a key.

The maximal rate at which information can be transmitted reliably subject to an information-theoretic secrecy requirement is called secrecy capacity [27]. Physical layer security, making sure that no information is leaked to the eavesdropper, is an addition (not an alternative) to existing security schemes. Whereas securing information at the physical layer is not so problematic in wired communication systems, since access to the physical cables is comparably hard to obtain incompunguously, implementing physical layer security in wireless communication systems can provide increased confidence with respect to the securing of data. The research potential of this area has remained relatively untapped even though the fundamental idea dates back nearly thirty years ago [28]. In recent years, owing to an increased understanding of the complex theory involved and to the technological advances, there has been a surge in interest in physical layer security in the research community.

The functionality of each layer is well-defined. Each layer is supported by the layer below it [29]. This modular architecture makes technical solutions portable from one system to the next without a complete system redesign. Wired and wireless communication systems function in the same way except at the two lower layers which deal with information transfer over the medium: data-link and physical. The data link layer is required to define the wireless-specific issues.

Research [30], that decides the transmit power according to the transmission state, in which the receiver applies learning to choose whether to change its location to resist strong jamming based on the previous transmission performance. Though it sounds good to enhance the secrecy without knowing the channel model, changing the direction of the beam and transmit power is reliable than changing once location. On the other hand, the impact of different numbers of transceivers on end-to-end multi-hop outage probability is evaluated [31], however, obtaining the closed-loop equation has more assumptions and simplicities than the non-linear learning capability.

The secrecy outage probability and average secrecy capacity are also evaluated under high and low power conditions, [32]. However, the mobility and channel variability scenarios are not well explored. The impact of imperfect channel state information is evaluated in underlay cooperative cognitive networks and it has shown that the relative position of the eavesdropper significantly affects the secrecy capacity [33], however, it doesn’t show any solid securing mechanism.

In general, though the physical-layer security method has attracted customers all over the world, the advancement in the features and functionalities of mobile wireless communication resulted in new secrecy requirements and challenges. In spite of the cooperative communication’s qualities including improving the spectral efficiency, enhancing power efficiency, and increased reliability, as the eavesdropper can exploit the information either directly from the sender or from the relay node, and hence the cooperative mobile communication technique is vulnerable to eavesdroppers. The security issue even gets worsens when the unauthorized user and the sender and receiver are mobile in nature. The so-far researches didn’t exploit the reinforcement learning significances under mobile user conditions. Therefore, this paper focuses on evaluating the mobile network security performance using reinforcement learning.

The proposed model consists of the sender, relay, eavesdropper, and receiver. Assuming the sender cannot directly transmit to the destination, the relay node can receive the sender’s signal and re-transmit it to the receiver. In both phases, the eavesdropper can receive the signal and hence the intercepting probability is more.

As it is shown in Figure 1, the eavesdropper can be in the coverage range of both the sender and the relay. Of course, the eavesdropper can also receive from only either of the transmitters (sender and relay). In general, the physical-layer network security is an emerging research area that discovers the likelihood of attaining consistent signal transmission. This is possible if the eavesdropper node is made to receive almost zero information. In this paper, this is realized by exploiting the time-varying of the wireless channel including path loss, shadowing, and fading.

2. System model

The technique proposed to enhance the wireless network security is organized by machine learning which manages the transmit power according to the interaction of the transmitter, receiver, relay-node, and the eavesdropper devices. The power is controlled in a manner that creates

![Figure 1. Cooperatively communicating devices under the presence of eavesdropper.](image-url)
weak SNR at the eavesdropper and stronger signal at the legitimate receiver. Moreover, other techniques that don’t use machine learning is also applied to compare the amount of enhancement achieved using the proposed technique. In general, the technique proposed to achieve better wireless network security is characterized by cheaper system complexity and better energy efficiency. For the analysis and machine learning, the Matlab is used as a simulation tool. The machine learning methods including supervised, unsupervised, semi-supervised, and reinforcement learning change patterns into knowledge. In this paper, due to the unavailability of existed training datasets, reinforcement learning is used. The objective of the learning is to infer an outcome, from online or offline experiences.

In the Reinforcement Learning (RL), there is an agent that interacts with the external world, and instead of being taught by datasets. The RL learns by exploring the environment and utilizing the collected knowledge. RL easily enables cognitive choices, including logical decision-making, planning, and scheduling. For this reason, this paper is based on RL.

Figure 2 indicates how the machine learning-based security enhancement works in the wireless environment. Basically, the wireless environment is affected by shadowing, path loss, fast or slow fading, mobility of the devices including speed and direction of all the participating devices. The proposed learning algorithm is q-learning. The utility and cost evaluation is the objective function that is planned to achieve mainly in this paper. The action is the appropriate task that the algorithm should do to achieve the best objective function. The ADC and DAC are the analogs to digital converter and digital to analog converter, respectively. The RF Tx/Rx is the radio frequency/carrier transmitter and receiver, respectively.

Therefore, in this paper, the physical-layer security mechanism is proposed to achieve an acceptable security level while still, the computational complexity is very simple. In the physical layer security techniques, even if the unauthorized devices are equipped with power computational devices, secure communications are possible. The reinforcement learning focuses on disciplined learning with the machine is given a set of actions, end values, and parameters.

The proposed system model consists of the sender, relay, eavesdropper, and receiver, as shown in Figure 3. The channel between each device is a Rayleigh fading channels.

The information is expected to be received by the destination without actually received by the eavesdropper. However, due to the nature of the transmission, the eavesdropper may be able to listen the signal both at the first phase (sender to relay) and second phase (relay to destination). The wiretap channel is the channel where the eavesdropper can access the signal and the main channel is the channel where the legitimate user collects the signal. The wiretap channel is the channel we want to eliminate or reduce the signal distribution while the main channel is the channel we want to maximize the signal to increase the secrecy capacity.

The proposed system is modeled using the Gaussian wiretap channel, with the source of the information sends $X_i$, the receiver accepts $Y_{B,i}$, and the eavesdropper receives $Y_{E,j}$ as:

$$Y_{B,i} = h_{B}X_i + N_{B,i}$$  \hspace{1cm} (1)

$$Y_{E,j} = h_{E}X_i + N_{E,j}$$

$h_{B}$ & $h_{E}$ are, respectively, the channel gains of the sender-destination and sender-eavesdropper. $N_{B,i}$ & $N_{E,j}$ are AWGNs additive white Gaussian noises with zero means $\delta_{B}$ & $\delta_{E}$, respectively.

With an average transmit-power of $P$, the secrecy capacity ($C_S$) of the channel is:

$$C_S = \frac{1}{2} \log \left( 1 + \frac{P|h_{B}|^2}{\delta_{B}^2} \right) - \frac{1}{2} \log \left( 1 + \frac{P|h_{E}|^2}{\delta_{E}^2} \right)$$

(2)

The $C_S$ is main channel’s Shannon-capacity minus eavesdropper channel’s Shannon-capacity. Hence, safe communication is achievable if the legitimate receiver has better channel than the eavesdropper’s channel:

$$\frac{|h_{B}|^2}{\delta_{B}^2} > \frac{|h_{E}|^2}{\delta_{E}^2}$$

(3)

The channel connecting the devices represented as when the sending device $i$ and the receiving device $j$, (represented as $h_i$), $i, j \in \{s, r, d, e\}$. The devices communicate in a half-duplex which either transmits or receives at a time. The message is transmitted in two phases: (i) when the sender transmits the message and the relay node receives it (ii) when the relay node transmits the signal to the legitimate destination. In both phases, the eavesdropper can listen and receive the message.

The fading coefficients of the channels are constant while transmitting the message at a phase. However, the channel can change independently and randomly from one message to another message. It is also assumed that there is no direct communication between the source and the destination.
$y_u = \frac{P_r |h_{sr}|^2}{\sigma^2}$ and $y_u = \frac{P_r |h_{sr}|^2}{\sigma^2}$, respectively. (4)

$P_y$ is the source transmit-power and $\sigma^2$ is variance of AWGN. The $h_{sr}$ is zero mean complex Gaussian random variable, and $\gamma_{sr}$ is exponentially distributed. Then, Cumulative Density Function (CDF) of $\gamma_{sr}$ is:

$$P_{ysr}(y) = 1 - e^{-\frac{y}{\gamma_{sr}}}$$

(5)

In the second phase of the transmission, the instantaneous received SNRs at the destination of the legitimate receiver and the eavesdropper are:

$$y_{sr} = \frac{P_r |h_{sr}|^2}{\sigma^2}$$

(6)

Where $P_r$ is the relay node transmit power.

Again, the CDF of the $y_{sr}$ is expressed as:

$$P_{y_{sr}}(y) = 1 - e^{-\frac{y}{\gamma_{sr}}}$$

(7)

### 2.1. Performance measurements

#### A. Secrecy capacity

Secrecy capacity is the maximum secure transmission rate from the source to the legitimate destination given while the eavesdropper is trying to receive the information:

$$C_s = |C_r - C_e| +$$

(8)

Where

$C_r$ is the secrecy capacities of the legitimate user and $C_e$ is the capacity collected by the eavesdropper receiver.

The secrecy capacity of the legitimate user in the second phase of the cooperative communication is:

$$C_s = \frac{1}{2} \min \{\log z(1+y_u), \log z(1+y_e)\}$$

(9)

The 1/2 term is used as the transmission is carried out in two phase. Considering the worst case, the Maximum Ratio Combining (MRC) is used at the eavesdropper; the capacity at the eavesdropper is:

$$C_e = \frac{1}{2} \log z(1+y_e + y_r)$$

(10)

Introducing the parameters:

$$y_e = y_u + y_r$$

and $y_r = \frac{1}{2} \min \{y_e, y_{sr}\}$.

(11)

This can also be further simplified also simplify $y_{sr} = \frac{1}{1+y_r}$.

Hence, the total secrecy capacity of the cooperative communication is:

$$C_s = \frac{1}{2} \log z(1+y_r) + \frac{1}{2} \log z(y_s)$$

(12)

#### B. Existence of Secrecy Capacity

The probability of secrecy capacity, the legitimate channel-capacity is greater than the eavesdropper channel-capacity. Mathematically,

$$P_s[Cs > 0] = P_r \left[ 1 + \gamma_r > 1 \right]$$

$$= P_r [\gamma_s > 1]$$

$$= 1 - P_{y_{sr}}(y)$$

Here, the $P_{y_{sr}}(y)$ is the CDF of $\gamma_{sr}$

$$P_{y_{sr}}(y) = 1 - \theta \left[ \frac{1}{\beta y_s + \frac{1}{y_s}} \right] \left[ \frac{1}{\beta y_e + \frac{1}{y_e}} \right] e^{\beta y_{sr}}$$

(14)

Where $\beta$ and $\theta$ are:

$$\beta = \frac{1}{\gamma_{sr}} + \frac{1}{y_{sr}}$$

and $\theta = \frac{1}{\gamma_{sr}} + \frac{1}{y_{sr}}$

#### C. Secure Outage Probability

Secure outage probability is the instantaneous secrecy capacity that is less than an objective secrecy rate:

$$P_{out}(R_s) = Pr(C_s < R_s)$$

(15)

Here, $R_s$ is the target secrecy rate. Now, applying the total probability theorem:

$$P_{out}(R_s) = Pr[Cs < R_s|y_T > y_0]Pr[y_T > y_0] + Pr[Cs < R_s|y_T \leq y_0]Pr[y_T \leq y_0]$$

(16)

Where $Pr[y_T \leq y_0] = 1 - Pr[C_s > 0]$.

$R_s > 0$ then $Pr[C_s < R_s|y_T \leq y_0] = 1$

$$P_{out}(C_s) = Pr[C_s < R_s|Cs > 0]Pr[Cs > 0] + Pr[Cs \leq 0]$$

$$P_{out}(C_s) = Pr[1 < y_s < 2^{R_s}] + Pr[y_s < 1]$$

(17)

The outage probability during the $k$th slot is given by:

$$Outage\ probability\ (P_{out}) = Pr(C_k < R_s)$$

Where $R_s$ is the end-to-end target rate.
\[ y_n = 2^{K^{Rs}} - 1, \text{ taking } k = 2 \]

The outage probability in multi-hop is:

\[ \text{Pout} = \Pr(\min(C_k) < R_s) \]

\[ \text{Pout} = 1 - \prod_{k=1}^{K} \]

### 2.2. Reinforcement learning

Though RL has many components, it has two main components called the agent and the environment. The environment comprises states and the agent is the RL algorithm that acts on the environment. The environment sends a state to the agent that acts on it. Then, the environment sends a pair of next state and reward back to the agent, as shown in Figure 4(a). The loop keeps going on until either the environment ends up with its states or the required objective function has attained its goal.

Parameters definition, Figure 4(b):

- Action \((A_0)\): they are the possible acts the agent can do
- State \((S_{t+1})\): this is the situation of the actual world.
- Reward \((R_{t+1})\): this is the feedback of the environment on each state by each action.
- Q-value \((Q(s, a))\): this is the long-term return of the current state \(s\) by using the action \(a\).

In the Q-learning-based RL, the agent learns from the interactions with the environment. The agent a sequence of:

\(s_0, a_0, r_1, s_1, a_1, r_2, s_2, a_2, r_3, \ldots\)

The agent at a state \(s_0\) with an action of \(a_0\) yields reward \(r_1\). Similarly, \(s_1\) with \(a_1\) yields \(r_2\), etc.
In q-learning, the agent sustains Q-table \( Q(S, A) \). Where \( S \) stands for set of states and \( A \) stands for set of actions. RL agent uses the following equation to fill its table:

\[
Q(s, a) \leftarrow (1-\alpha) Q(s, a) + \alpha (r + \gamma \max_a Q(s', a')).
\]

In this paper, \( \alpha \) is fixed for simplicity.

When the q-learning agent starts the learning, it doesn't have any knowledge. It doesn't know if a particular action results in a positive or negative reward. Coming to this paper, initially, the algorithm doesn't know if a particular Transmit power (Tx P level) provides better secrecy capacity or bad secrecy capacity. Therefore, the q-values of every state-action pair are initialized with zero (i.e. no prior knowledge). When the q-learning starts iterating, the table starts filling rewards for the pair of state-action combinations. The secrecy capacity of the proposed wireless network is represented by the reward. Hence, better reward means better secrecy capacity. The secrecy capacity is also the utility function of this algorithm. In other words, the effort is to find the best secrecy capacity of the link while every device is freely moving in the coverage range of the study area.

To start the q-learning, the horizontal axis of the table represents the list of actions, and the vertical axis represents the list of states.

**Steps 1.** Initialize the Q-table
The n columns (actions) and m rows (states) the values. In this paper, the transmit powers of all the transmitters are mapped for the actions and the set of positions of the devices is mapped for the states.

**Steps 2.** Perform any action
All the actions (thousands of transmit power levels) stars acting on each state (movements of the interacting devices, sender, eavesdropper, relay, and destination). Then the observation is recorded on the table which acts as a database for later reference.

**Steps 3.** Evaluation
The collective result of the state-action pairs is evaluated for its reward. More specifically, the secrecy capacity of each transmits power is evaluated at each device movement and interaction. Then, it fills the table using a New Q \( (s, a) \) equation:

\[
\text{New}Q(s, a) = Q(s, a) + \alpha [R(s, a) + \gamma \max_a Q(s', a') - Q(s, a)]
\]
Where $\alpha$ is learning rate, fixed to 0.2. $R(s,a)$ is the reward at that state using that action. $Q(s,a)$ is the current Q-value. The $\max Q(s',a')$ is the maximum expected future-reward given the new states’ and all possible actions at the new state.

In general, the agent is the Q-learning algorithm itself. The reward is the secrecy capacity of the wireless network. The set of actions includes the Tx power of the sender and Tx power of the relay. Similarly, the states can be positions and movements of the interacting devices. For such decisions the SNR formulated in this paper is evaluated at the receiver and the performance of the design is evaluated using secrecy capacity enhancement. Since, the received SNR is a result of the sender, eavesdropper, relay and destination movement and location, path loss, fading and shadowing, the interaction of every devices is investigated using the machine learning. The environment is, in general, composed of different influences of the wireless network including sender, eavesdropper, relay, sender and destination movement and location, path loss, fading and shadowing.

Simplified summary of the Q-learning algorithm:

1. Set the gamma parameter (set to)
2. Initialize Q table to zero (no value is zero by default)
3. For each episode:
   - Select a random initial state (say any position of the devices)
   - Do until all states finished
   - Select one action that acts on a certain state (all possible powers for each devices position)
   - Using this one action, apply on all of the following states (with each action evaluate all the possible devices positions that may happen in the future)
   - Evaluate the best q-value using all of the actions acting on the states (the best secrecy calculated at each action-state couples)
   - Compute: $Q(s, a) = R(s, a) + \gamma \max_{a'} Q(s', a')$ (the formula for filling the Q-value table)
   - Set the next state as the current state (update states and continue evaluating the state action)
   - End Do
   - End For

This indicates that the transition from the algorithm’s parameters to the proposed research parameters. Since a reward (R) is the combination of the output of state and action, the best reward is chosen for further analysis (i.e. the best reward is the best secrecy).

3. Results and discussions

In modern networks, the security concern has become increasingly significant concerns in wireless networks. As a solution, the physical layer-based security resolution has emerged as an attractive approach for performing secure transmission that is feasible for the 4G networks. Regarding the identification of the devices, this research assumes all the locations of the devices are already known relative to the relay and destination.

The noise variance is the noise distribution in the receiver. This is the assumption where the receiver accommodates this level of noise. The noise can come from the internal capacity of the transmitter-receiver equipment, from the environment and from the receiver circuitry. The -60 dBm is chosen in this research as many researches suggests for the wireless networks. The Sender receiver separation is chosen from 10 m to 550 m because if the transmitter-receiver is below 10m separation then

![Figure 9. Secrecy capacity enhancement at different SNRs.](image)

![Figure 10. Performance evaluation of secrecy capacity using reinforcement learning.](image)
they are together and no need this type of wireless transmission for the communication. Due to the chosen power limit, the maximum coverage of the transmission is assumed 550m. The transmit power variation is taken from -5 to 35 dBm. This power is the power of both the relay and the sender devices. Shadowing is the tendency of the opposition of the signal from smoothly going to the destination. As many standards researches use it, this paper assumes a log-normal shadowing standard deviation of 8 dB for all links.

A) Effect of relay node movement on the secrecy capacity

As can be shown in Figure 5, the secrecy capacity is significantly affected by the relay position relative to the transmitter and receiver (assuming the eavesdropper is located at a certain fixed position). The best secrecy capacity is attained when the relay is in the middle of the receiver and transmitter. This middle relay position is evaluated when the distance between the sender and relay, sender and eavesdropper, relay and eavesdropper, and relay and receiver is 100 m in the 3D scenario. The “relay close to the receiver” is evaluated when the relay is located 125m far from the transmitter and 75m far from the receiver. Similarly, the “relay close to the transmitter” is taken when the relay is 75m from the transmitter and 125m from the receiver. The “relay very close to the receiver” is evaluated when the relay is located 150m far from the transmitter and 50m far from the receiver. Similarly, the “relay very close to the transmitter” is taken when the relay is 50m from the transmitter and 150m from the receiver.

In general, the position of the relay significantly affects the secrecy capacity without modifying the position of the eavesdropper. In reality, however, all the devices are mobile. They can move at any time to any position. Hence, neither a single power allocation nor fixed transmission budget design can result in the best possible secrecy capacity.

Figures 6 and 7 indicates the received SNR levels at the legitimate user and eavesdropper when the relay is at the middle and when the relay is close to the transmitter, respectively. This confirms that better SNR is achievable at the legitimate user when the location of the relay is in the middle. At this position of the relay, the legitimate user exploits much better than the eavesdropper. However, when the relay moves to either (transmitter or receiver) directions of the devices, the secrecy capacity decreases.

Besides, better SNR of the legitimate user depends on the relative positions of the devices. Hence, a dynamic live channel investigation can only tell us the best transmission parameters design that results in the best secrecy capacity. That is why this paper proposes reinforcement learning to solve the mobility problems on the secrecy capacity.

B) Effect of total transmit power on secrecy capacity

Figure 8 indicates that increasing the total transmit power increases the secrecy capacity. This confirms the possibility of increasing the secrecy capacity of the legitimate receiver without any cryptographic key. However, practically, we can’t have unlimited power which indicates that increasing the transmit power violates energy efficiency.

It is not also surprising that the secrecy decreases when the relay node is moving away from the sender because the path loss is increasing while still, the eavesdropper closes the transmitter. It is also logical that the secrecy capacity increases when the eavesdropper is moving away from the sender. This is because the eavesdropper faces more difficulties in intercepting the message. Similarly, when the eavesdropper moves closer to the transmitter than the relay, the eavesdropper get better chance of the channel conditions relative to the legitimate receiver. This concludes that increasing the power can not be a solution when the devices are mobile.

Figure 9 indicates that the secrecy capacity can be easily increased when the SNR level is increased. Therefore, this result verifies that increasing the SNR at the legitimate receiver is one technique that can be used for increasing the secrecy capacity. However, increasing the SNR is not an easy task as we may also increase the SNR of the eavesdropper.

C) Secrecy capacity performance evaluation using reinforcement learning

Without affecting the positions of the other devices, the relay device is made to move freely. For every position of the relay, the transmit power of the relay and transmitter devices is learned using reinforcement learning. By receiving the feedback from the channel (reward), the transmit power of the transmitters is varied (actions) for each position of the relay (states). Figure 9 indicates that reinforcement learning has further increased the secrecy capacity.

The reinforcement learning also selects the appropriate minimum possible power (to sustain the energy efficiency) while enhancing the secrecy capacity. Unlike without reinforcement learning, the reinforcement learning adaptively selects the best transmit power while all the devices are moving randomly within the network coverage.

From Figure 10, we can deduce that when the separation of sender and relay is too large, the reinforcement learning method has almost no

![Figure 11](image-url). Performance evaluation of secrecy outage probability of the proposed solution.
effect on the confidentiality enhancement. This is true because when the separation of the sender and the relay is too large, the probability of the eavesdropper is closer to the sender than the relay node increases. If the eavesdropper gets sufficient signal while the relay node is not, then there is a high probability that working on the transmitters’ power could result in a limited solution.

As it is shown in Figure 11, the secrecy outage probability increases with the capacity per Hertz (i.e. the spectral efficiency). The increase in the secrecy outage probability has slowed by the proposed solution and hence the reinforcement learning is ideal for increasing secrecy capacity.

4. Conclusion

Recently, wireless network has resulted in new security requirements and challenges. In wireless networks, the shadowing, path loss, and fading are challenging obstructions of cellular communication. Cooperative communication solves these problems to some extent. The cooperative communication also increases the spectral efficiency, power efficiency, and reliability, but it is highly exposed to security problems. Hence, this paper proposes reinforcement learning to increase the secrecy capacity of wireless networks. The simulation results have confirmed that the proposed technique is ideal for increasing the secrecy capacity of the wireless networks under mobile devices.

Declarations

Author contribution statement
Gebrehiwet Gebrekristos Lema: Conceived and designed the experiments; Performed the experiments; Wrote the paper.
Kiros Siyoum Weldemichael: Analyzed and interpreted the data.
Leake Enqay Weldemariam: Contributed reagents, materials, analysis tools or data.

Funding statement
This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Data availability statement
Data will be made available on request

Declaration of interests statement
The authors declare no conflict of interest.

Additional information
No additional information is available for this paper.

References
[1] Piyush Gupta, Panganamala R. Kumar, The capacity of wireless networks, IEEE Trans. Inf. Theor. 2 (2000) 388–404.
[2] Mario Alves, Eduardo Tovar, Real-time communications over wired/wireless PROFIBUS networks supporting inter-cell mobility, Comput. Network. 51 (11) (2007) 2994–3012.
[3] Xiaohu Ge, et al., 5G Ultra-dense Cellular Networks, IEEE Wireless Communications, 2016.
[4] A. Sheikholeslami, D. Goekcel, H. Pi Shepherd, D. Towsley, Physical layer security from inter-session interference in large wireless networks, in: Proc. IEEE INFOCOM, Orlando, FL, USA, 2012, pp. 1179–1187.
[5] M. Ghaderi, D. Goekcel, A. Orda, M. Dehghan, Efficient wireless security through jamming, coding and routing, in: Proc. 10th IEEE Int. Conf. Sensing, Commun., Netw. (SECON), New Orleans, USA, 2013, pp. 505–513.
[6] Majid Ghaderi et al., Minimum energy routing and jamming to thwart wireless network eavesdroppers, IEEE Trans. Mobile Comput. 14 (7) (2015) 1433–1448.
[7] J. Huang, A.L. Svindland, Cooperative jamming for secure communications in mimo relay networks, IEEE Trans. Signal Process. 59 (10) (Oct. 2011) 4871–4884.
[8] Elham Nosrati, Xinbin Wang, Arash Kababbazoumen, Secrecy capacity enhancement in two-hop DF relaying systems in the presence of eavesdropper, in: 2015 IEEE International Conference on Communications (ICC), IEEE, 2015.
[9] Shyamnath Gollakota, Dina Katabi, Physical layer wireless security made fast and channel independent, in: 2011 Proceedings IEEE INFOCOM, IEEE, 2011.
[10] Li Sun, Qinghe Du, A review of physical layer security techniques for internet of things: challenges and solutions, Entropy 20 (10) (2018) 730.
[11] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.K. Wong, X. Gao, A survey of physical layer security techniques for 5G wireless networks and challenges ahead, IEEE J. Sel. Areas Commun. 36 (4) (2018) 679–695.
[12] Zhijin Qin et al., Deep Learning in Physical layer Communications, arXiv preprint arXiv:1807.11713, 2018.
[13] Songlin Chen et al., Physical-layer channel authentication for 5G via machine learning algorithm, Wireless Commun. Mobile Comput. (2018) 2018.
[14] Ning Wang et al., Physical-layer authentication based on extreme learning machine, IEEE Commun. Lett. 21 (7) (2017) 1557–1560.
[15] He Fang, Xinbin Wang, Lajos Hanzo, Learning-aided physical layer authentication as an intelligent process, IEEE Trans. Commun. 67 (3) (2019) 2260–2273.
[16] A. Serafet al., Security enhancement in wireless sensor networks using machine learning, in: 2012 IEEE 14th International Conference on High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems, IEEE, 2012.
[17] N. Yang, L. Wang, G. Geraci, M. Elkashlan, Safeguarding 5G wireless communication networks using physical layer security, Commun. Mag. IEEE 53 (4) (2015) 20–27.
[18] Jose Sánchez, Vega David et al., Survey on physical layer security for 5G wireless networks, Annals of Telecommunications, 2020, pp. 1–20.
[19] E. S, B. L, G. C, Nonconvex online support vector machines, IEEE Trans. Pattern Anal. Mach. Intell. 33 (2) (2011) 368.
[20] Y. Chang, H. Liu, Semi-supervised classification algorithm based on the KNN, in: Proc. IEEE International Conference on Communication Software and Networks, 2011, pp. 9–12.
[21] K. Nettil, Y. Radhika, A novel method for minimizing loss of accuracy in naive bayes classifier, in: Proc. IEEE International Conference on Computational Intelligence and Computing Research, 2016, pp. 1–4.
[22] L. Tang, H. Chen, Q. Li, Social tie based cooperative jamming for physical layer security, IEEE Commun. Lett. 19 (10) (2015) 1790–1793.
[23] J. Li, A.P. Petropulu, S. Weber, On cooperative relaying schemes for wireless physical layer security, IEEE Trans. Signal Process. 59 (10) (2011) 4985–4997.
[24] Alfred O. Hero, Secure space-time communication, IEEE Trans. Inf. Theor. 49 (12) (December 2003) 3235–3249.
[25] Matthieu Bloch, Andrew Tangaraj, Steven W. McLaughlin, Jean-Marc Merolla, LDPC-based Gaussian key reconciliation, in: Proc. of the IEEE International Workshop on Information Theory, Punta del Este, Uruguay, March 2006.
[26] Y. Liang, V.H. Poor, Information theoretic security, Found. Trends® in Commum. Inf. Theory 5 (4) (Apr. 2008) 355–580.
[27] M. Bloch, J. Barros, Physical-Layer Security: From Information Theory to Security Engineering, Cambridge University Press, 2011.
[28] A.D. Wyner, The wiretap channel, Bell Syst. Tech. J. 24 (8) (Oct. 1975) 1385–1387.
[29] Y.W. Peter Hong, Pang-Chang Lan, C.-C.C. Jay Kuo, Enhancing physical-layer secrecy in multiantenna wireless systems: an overview of signal processing approaches, IEEE Signal Process. Mag. 30 (5) (2013) 29–40.
[30] Liang Xiao et al., Anti-jamming underwater transmission with mobility and learning, IEEE Commun. Lett. 22 (3) (2018) 542–545.
[31] Minh Nam Pham, On the secrecy outage probability and performance trade-off of the multi-hop cognitive relay networks, Telecommun. Syst. 73 (3) (2020) 349–358.
[32] Parag Singh, Chauhan, Sanjeev Kumar, Sanjay Kumar Soni, On the physical layer security over Beaulieu-Xie fading channel, AEU-Int. J. Electron. Commun. 113 (2020) 152940.
[33] Tan-Phuc Huynh et al., Secrecy outage probability of a NOMA scheme and impact imperfect channel state information in underlay cooperative cognitive networks, Sensors 20 (3) (2020) 895.