Computers, Materials & Continua
DOI: 10.32604/cmc.2022.026972
Article

Tech Science Press

Secure Irrigation System for Olive Orchards Using Internet of Things

Ayman Massaoudi*, Abdelwahed Berguiga and Ahlem Harchay

Department of Computer Science, College of Science and Arts in Gurayat, Jouf University, Sakakah, Saudi Arabia
*Corresponding Author: Ayman Massaoudi. Email: ahmassaaoudi@ju.edu.sa
Received: 07 January 2022; Accepted: 02 March 2022

Abstract: Smart irrigation system, also referred as precision irrigation system, is an attractive solution to save the limited water resources as well as to improve crop productivity and quality. In this work, by using Internet of things (IoT), we aim to design a smart irrigation system for olive groves. In such IoT system, a huge number of low-power and low-complexity devices (sensors, actuators) are interconnected. Thus, a great challenge is to satisfy the increasing demands in terms of spectral efficiency. Moreover, securing the IoT system is also a critical challenge, since several types of cybersecurity threats may pose. In this paper, we address these issues through the application of the massive multiple-input multiple-output (M-MIMO) technology. Indeed, M-MIMO is a key technology of the fifth generation (5G) networks and has the potential to improve spectral efficiency as well as the physical layer security. Specifically, by exploiting the available M-MIMO channel degrees of freedom, we propose a physical layer security scheme based on artificial noise (AN) to prevent eavesdropping. Numerical results demonstrate that our proposed scheme outperforms traditional ones in terms of spectral efficiency and secrecy rate.

Keywords: Smart farming; olive; IoT; massive MIMO; spectral efficiency; security

1 Introduction

According to the Guinness Book of Records, the Jouf region, in Kingdom of Saudi Arabia (KSA), is the largest olive farm in the world. Specifically, there are nearly 52,000 acres of olive groves and more than 5 million olive trees in Jouf region. This large quantity of olive trees requires the provision of a significant amount of water in order to obtain the maximum productivity and better quality. However, most of the KSA regions suffer from a desert climate, with very low precipitation and severe temperature fluctuations between day and night. Moreover, the use of traditional irrigation systems not only consumes a lot of farmers time and effort (farmers must remain present during the irrigation process), but also can leads to over or under irrigation problem. Consequently, it is necessary to design a new irrigation system for olive trees based on modern technology in order to improve the productivity of olive while reducing water consumption.

Recently, smart irrigation system (also referred as precision irrigation system) is considered as a key solution to save the limited water resources as well as to improve crop productivity and quality [1–11]. Indeed, the application of Internet of things (IoT) allows prediction of olive tree's needs (according to the sensed environmental parameters from the soil or the climate), and provides optimal decisions to the farmers about possible things to do, in real time [6]. Although several IoT based irrigation systems have been introduced in literature [1–11], there are several challenges that still need to be tackled [12–14].

First, since the use of wiring communication between various nodes is very expensive, the existing works adopted wireless solution, such as Bluetooth, ZigBee, IEEE 802.15.4 standard, LoRaWAN (Low Rate Wide Area Networks), etc. However, these technologies are not effective and do not satisfy the increasing demands in terms of spectral efficiency of the IoT based irrigation system. Indeed, in such system, a huge number of low-power and low-complexity sensors and actuators are interconnected.

Second, another challenge identified with smart irrigation systems using wireless technologies is the topology of the olive orchards that makes wireless signals susceptible to attenuation and results in non line of sight (NLoS) environment.

Third, the deployment of smart communication technologies and IoT raise the vulnerabilities and cybersecurity threats. Particularly, in IoT irrigation system various threats may exist: privacy threats, vulnerable software, eavesdropping attacks, DoS (denial of service) attacks, MITM (man in the middle) attack, etc. [15,16]. Therefore, protecting the IoT systems from cyber-attacks is a very important issue that was widely considered by researchers in many existing works (see for example [12,15,16] and references therein). In these studies, many security and privacy solutions were proposed, such as privacy preserving [15], authentication, access control, data integrity (using blockchain [16]), cryptography (as example elliptic curve cryptography in [17]), key management, intrusion detection system (IDS) [18], etc. Nevertheless, these proposed security schemes require high computational complexity, while dealing with limited resources devices (in terms of energy, memory, storage, and computing capability). As result, such solutions are not suitable for practical implementation.

In this work, we aim to address the aforementioned challenges and issues. To this end, we propose a smart and secure olive irrigation system through the application of the massive multiple-input multiple-output (M-MIMO) technology [19,20]. Indeed, this technology represents a keystone of the fifth generation (5G) and has the potential to improve spectral efficiency as well as the physical layer security [21,22]. Specifically, by exploiting the available M-MIMO channel degrees of freedom, we propose a physical layer security scheme based on artificial noise (AN) [23–25] to prevent eavesdropping.

The remaining sections of the paper are organized as follows. In Section 2, we provide a survey of recent state of the art on smart irrigation systems. We describe our proposed IoT-based irrigation system using the massive MIMO technology in Section 3. In the fourth Section, we evaluate the performance of our system using Monte Carlo simulation. In the last Section, we conclude the paper.

2 Recent State of the Art

2.1 IoT-Based Irrigation Systems

In literature, several IoT-based irrigation systems have been introduced. This section summarizes existing works. In [6], authors considered a hedgerow olive orchard in Spain. They developed an automated irrigation system by using soil mapping and distant sensing techniques. The proposed

system in [6] is based on regulated deficit irrigation strategies (RDI). However, in [6] all sensors were connected to a data logger via cable. Therefore, the distance between the various nodes of the irrigation system is restricted by the maximum possible cable distance in order to preserve a good quality of the electrical signal. Note that there are other several drawbacks when using wired sensors: lack of mobility, deployment costs, cable damage and scalability.

In [4], a peach orchard is considered. Brun-Laguna et al. deployed the Time-Slotted Channel Hopping (TSCH) technology in a wireless meshed sensor network. TSCH technology interconnects the sensors (or actuators) to the gateway (the edge node). Notice that other technologies were also considered in other researches [1,2,5,7,10], such as Bluetooth, ZigBee, IEEE 802.15.4 standard, LoRaWAN (Low Rate Wide Area Networks), etc. In LoRaWAN technology less energy can be consumed, whereas ZigBee and TSCH provide a more reliable upstream/downstream. To ensure communication between the edge node (gateway) and the public/private Cloud, cellular network like GPRS (General Packet Radio Service), GSM (Global System for Mobile Communications), 3G (Third Generation), 4G (Fourth Generation), 5G and WiFi (Wireless Fidelity) were deployed. In [10], the deployment of an IoT based irrigation system, called AgriSens, was presented. The deployed irrigation system provided a real-time and dynamic irrigation process since the diverse crop growth stages are considered. In [10], GPRS and ZigBee ensure data transmission. In [2], wireless sensor network (WSN) is adopted and authors proposed a precision irrigation system using GPRS technology. Nevertheless, the irrigation threshold is a pre-set static for diverse crop growth stages, which do not guarantee water saving. In [1], authors proposed a distributed WSN based irrigation system for the arid as well as the semi arid regions. Additionally, the communication protocol between the base station and the sensor nodes is Bluetooth. Thus, the system of [1] do not support high scalability and therefore it cannot be deployed in practice. In [7], Krishnan et al. proposed a smart irrigation system based on GSM technology. The farmer can follow the task's statuses (e.g., temperature, humidity and soil moisture) via acknowledgement messages sent by the system. Authors proposed to use Fuzzy logic controller in order to compute input parameters and to produce outputs of motor status. Queté et al. [5] considered a smart IoT irrigation system wherein the LoRaWAN media access control (MAC) protocol is deployed. The performance and scalability tradeoffs of LoRaWAN technology were studied in [5] for diverse conditions (LoRaWAN spreading factor; distance between sensors and gateway; number of sensors (sensor density). The results in [5] showed a significant delay increase with the sensor density as well as the spreading factor. The paper of [8] described the designing of an IoT based irrigation system for urban as well as rural farmers. Authors in [8] employ the MQTT (Message Queuing Telemetry Transport) protocol. In [9] Bhoi et al. used machine learning (ML) and internet of things to deploy a smart irrigation system in Raipur, India. In order to save water usage with minimum human assistance, several ML-based regression and classification models were used in [9]. Authors had integrated the forecasted weather data in order to ensure the robustness of their system.

2.2 Addressing Security Issues in IoT Systems

The deployment of smart communication technologies and IoT raise the vulnerabilities and cybersecurity threats. Therefore, protecting the IoT systems from intruders is a very important issue that was widely considered by researchers in many existing works (see for example [12,16] and references therein). In particular, Gupta et al. presented in [15] a study on security and privacy of IoT systems for precision agriculture. The work of [15] outlined a multi-layered architecture suitable to the smart farming context and highlighted various cyber-attack scenarios. In [16], Yang et al. presented a survey on smart farming and discussed the security challenges. They considered the following security

and privacy solutions: privacy preserving [15], authentication, access control, data integrity (using blockchain [16]), cryptography (as example elliptic curve cryptography in [17]), key management, intrusion detection system [18], etc. Additionally, other supplementary experiments based on solar insecticidal lamps IoT were done. In [12], García et al. presented a survey that summarizes the current researches concerning smart irrigation systems. They discussed the challenges and the best practices for the deployment of sensor based irrigation systems. In [17], the authors designed a security mechanism for industrial IoT environment. Ali et al. proposed a secure industrial IoT scheme based on HECC (hyper elliptic curve cryptography). The purpose of work in [17] is to improve security of an industrial IoT environment with reduced computational complexity. In [18], Berguiga et al. considered an IoT based healthcare system. Authors developed a secure scheme using intrusion detection system. The proposed scheme protect the healthcare system against DoS attacks caused by TCP SYN flooding attacker nodes.

3 Massive MIMO for IoT-Based Irrigation System

In this study, we propose to adopt the massive MIMO technology to deploy a smart and secure irrigation system for olive orchards. For this purpose, we design an IoT based architecture that ensure the interconnection of sensors and actuators to a base station (acting as wireless gateway to the remote processing server). In the sequel, we will elaborate our proposed system in detail.

3.1 Network Model

In this subsection, we describe the network model adopted in the present work. As illustrated in Fig. 1, we divide the olive orchards into L cells. Each cell operates separately using one base station (BS). The l-th BS ($1 \leq l \leq L$) is equipped with M_l antennas ($M_l \gg 1$) and communicates with K_l single antenna sensor-actuator nodes (SANs). The SANs are geographically distributed in the cell. Precisely, we deploy beside each olive tree a node responsible for sensing different environmental parameters (provided by the soil or the climate) and acting accordingly. Each BS forwards the sensed data to a remote processing server. This server compares the gathered information to the predefined threshold values. For any deviation from the threshold, the remote processing server will send, via the corresponding base station, a signal to the actuator for the purpose to activate the solenoid valve that irrigates the olive tree (without the physical presence of the farmer). Additionally, through the Internet, the farmers can visualize the information and running activities of the olive orchard instantly in real time.

In uplink transmission (from the SANs to the BS) for a given cell, the received signal at the BS, $\boldsymbol{y}^{\mathrm{UL}} \in \mathbb{C}^{M_l}$, is modeled as:

$$\boldsymbol{y}^{\mathrm{UL}} = \sum_{l=1}^{L} \sum_{k=1}^{K_l} \boldsymbol{h}_{lk} \boldsymbol{s}_{lk} + \boldsymbol{n}, \tag{1}$$

where:

- We omit the index of the cell for convenience.
- h_{lk} is the channel between the SAN and the BS. We assume that the channel vector is independent and identically distributed (i.i.d.) complex Gaussian samples of a random variable with zero mean and unit variance.
- $s_{lk} \sim \mathcal{N}_{\mathbb{C}}(0, p_{lk})$ denotes the signal from the SAN to the BS, where $p_{lk} = \mathrm{E}\left\{|s_{lk}|^2\right\}$ is the power of the transmitted signal, where $\mathrm{E}\{\boldsymbol{x}\}$ represents the expectation of a random variable x.

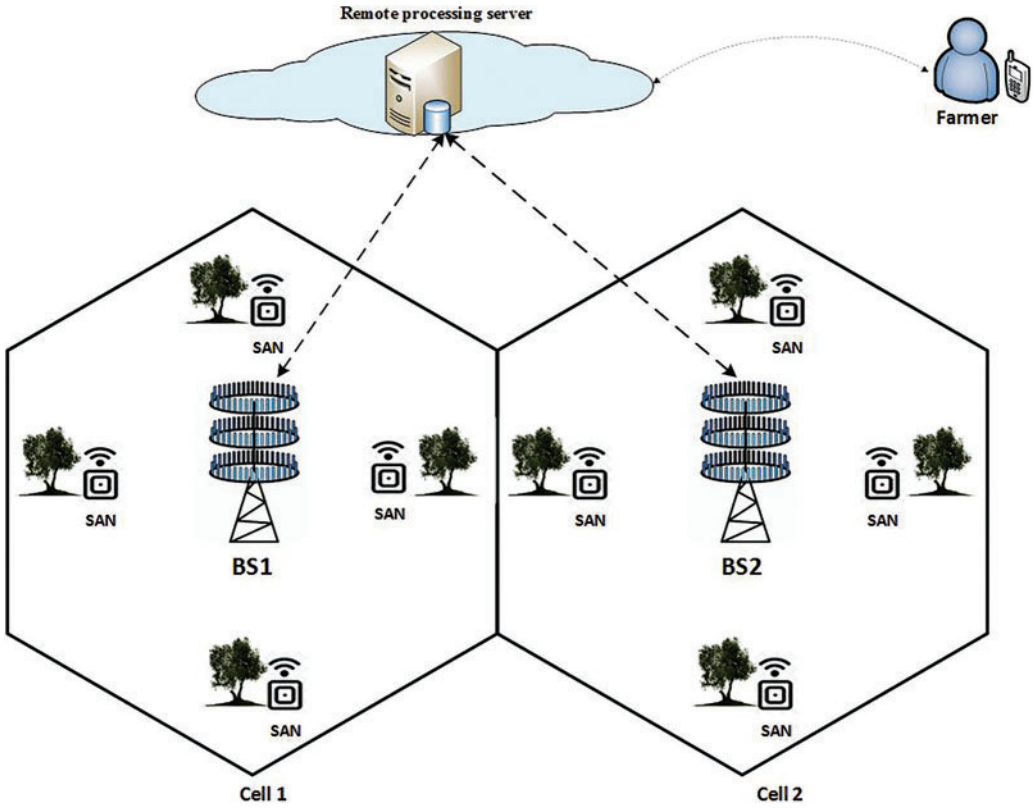

Figure 1: Proposed network model

- $\boldsymbol{n} \sim \mathcal{N}_{\mathbb{C}}\left(0, \sigma_{UL}^2 \boldsymbol{I}_{M_l}\right)$ is the independent additive white noise with zero mean and variance equal to σ_{UL}^2.

Similarly, in downlink transmission (from the BS to the k-th SAN, $1 \leq k \leq K_l$ and $1 \leq l \leq L$), the received signal at the k-th SAN, $\boldsymbol{y}_k^{\mathrm{DL}} \in \mathbb{C}$, is modeled as:

$$\boldsymbol{y}_k^{\mathrm{DL}} = \sum_{l=1}^{L} \sum_{i=1}^{K_l} (\mathbf{h}_{lk})^{\mathrm{H}} \boldsymbol{w}_{li} \boldsymbol{x}_{li} + \boldsymbol{n}_k, \tag{2}$$

where:

- $\mathbf{h}_{lk}$ denotes the channel between the BS and the k-th SAN. We assume that the channel vector is independent and identically distributed (i.i.d.) complex Gaussian samples of a random variable with zero mean and unit variance.
- $w_{lk} \in \mathbb{C}^{M_l}$ represents the transmit precoding vector (beamforming). This beam complies $\mathrm{E}\left\{\|w_{lk}\|^2\right\} = 1$.
- $x_{lk} \sim \mathcal{N}_{\mathbb{C}}(0, \rho_{lk})$ denotes the data signal intended for the k-th SAN in the l-th cell and ρ_{lk} is the signal power.
- $\boldsymbol{n}_k \sim \mathcal{N}_{\mathbb{C}}(0, \sigma_{DL}^2)$ is independent additive white noise with zero mean and variance σ_{DL}^2.

In this paper, we assume that the time division duplex (TDD) mode is used and perfect channel state information (CSI) of all channels is available at the BS. In this case, only uplink pilot signals

are required and no feedback is needed. Indeed, the BS carry out the channel estimation by using the uplink pilot transmission from each SAN.

3.2 Spectral Efficiency of the IoT System

Spectral efficiency (SE) of an encoding (or decoding) scheme can be defined as the average number of bits of information that it can reliably transmit over the channel under consideration [21]. We will now study the spectral efficiency that our proposed irrigation system based on massive MIMO can achieve. To this end, we consider the multi-cell minimum mean-squared error (M-MMSE) combining, as well as the maximum ratio (MR) combining.

The uplink SE of the channel between the k-th SAN and the l-th BS ($1 \leq k \leq K_l$ and $1 \leq l \leq L$), denoted $\mathbf{SE}_{kl}^{\mathrm{UL}}$, can be expressed as:

$$\mathbf{SE}_{kl}^{\mathrm{UL}} = \frac{\boldsymbol{\tau}_u}{\boldsymbol{\tau}_c} \mathrm{E}\left\{\log_2\left(1 + \mathbf{SINR}_{kl}^{\mathrm{UL}}\right)\right\}, \tag{3}$$

where

- τ_u represents the uplink data samples per coherence block.
- $\tau_c = \mathrm{B}_c\mathrm{T}_c$ denotes the number of samples per coherence block (T_c is the channel coherence time and is the channel coherence bandwidth).
- $\mathrm{SINR}_{kl}^{\mathrm{UL}}$ denotes the uplink signal to interference plus noise ratio (SINR) from the k-th SAN in the l-th cell.

Similarly, the downlink SE of the channel between the l-th BS and the k-th SAN (where $1 \leq l \leq L$ and $1 \leq k \leq K_l$), denoted $\mathbf{SE}_{lk}^{\mathrm{DL}}$, can be expressed as:

$$\mathbf{SE}_{lk}^{\mathrm{DL}} = \frac{\boldsymbol{\tau}_d}{\boldsymbol{\tau}_c} \mathrm{E}\left\{\log_2\left(1 + \mathbf{SINR}_{lk}^{\mathrm{DL}}\right)\right\}, \tag{4}$$

where

- τ_d represents the downlink data samples per coherence block. We notice that $\tau_c = \tau_u + \tau_d + \tau_p$, where $\boldsymbol{\tau}_p$ denotes the number of samples allocated for pilots per coherence block.
- $\mathrm{SINR}_{lk}^{\mathrm{DL}}$ denotes the dowlink signal to interference plus noise ratio (SINR) of the k-th SAN in the l-th cell.

3.3 AN-Based Secure Olive Irrigation System

In IoT networks, particularly IoT irrigation system, various threats may pose: privacy threats, vulnerable software, denial-of-service (DoS) attacks, man-in-the-middle attack, eavesdropping attacks, etc. [12]. In this section, we address the eavesdropping issue of the proposed olive irrigation system. Specifically, by exploiting the available massive MIMO channel degrees of freedom, we propose a physical layer security scheme based on artificial noise (AN). We assume that one eavesdropper is located within the cell. The key idea behind AN is that the BS transmits artificial noise in order to contaminate the received signal at the eavesdropper [23]. Consequently, the received signals at the eavesdropper can be expressed as follows:

$$\boldsymbol{y}_{\mathbf{e}} = \sum_{l=1}^{L} \sum_{i=1}^{K_l} (\mathbf{h}_e)^{\mathrm{H}} \boldsymbol{w}_{li} \boldsymbol{x}_{li} + (\mathbf{h}_e)^{\mathrm{H}} \boldsymbol{x}_{\mathrm{AN}} + \boldsymbol{n}_e, \tag{5}$$

where

- h_e represents channel between the BS and the eavesdropper. We assume that the channel vector is independent and identically distributed (i.i.d.) complex Gaussian samples of a random variable with zero mean and unit variance.
- $x_{\mathbf{AN}}$ is the artificial noise vector.
- $n_e \sim \mathcal{N}_{\mathbb{C}}\left(0, \sigma_e^2\right)$ is independent additive white noise with zero mean and variance σ_e^2.

The achievable secrecy sum rate for the k-th node is given by:

$$\boldsymbol{R}_k^{\text{secrecy}} = (\boldsymbol{R}_k - \boldsymbol{R}_e), \tag{6}$$

where R_k (respectively R_e) denotes the ergodic rate of the k-th SAN (of the eavesdropper).

The next section provides the simulation results of the proposed smart irrigation systems.

4 Performance Validation

In this section, we propose to validate the performance of our proposed system using Monte Carlo Simulation in MATLAB. We assume equal transmit power per SAN in both uplink and downlink. Without loss of generality, we assume also that the number of BS antennas (respectively the number of SANs) is the same in all cells (i.e., $M_l = M$ and $K_l = K$, for $1 \leq l \leq L$). We consider two propagation models: the line of sight (LoS) propagation and the non line of sight (NLoS) propagation. We give the simulation parameters in Tab. 1.

Table 1: Simulation parameters

Parameters	Value
Number of cells (L)	15
SNR	0 dB
Uplink data samples per coherence block	90
Number of samples per coherence block	200
Downlink data samples per coherence block	90

Fig. 2 shows the average uplink sum spectral efficiency (SE) of the studied system as function of the number of antennas at the BS, M. The number of SANs per cell is chosen K = 25. In this figure, we consider the MR and the M-MMSE combining for the LoS (Red curves) and NLoS (Blue curves) channel models. As expected, the sum spectral efficiency increases linearly with M for all considered cases since the spatial diversity increases.

Fig. 2 illustrates the average uplink sum spectral efficiency (SE) of the IoT system *vs.* the number of SANs per cell, K. The number antennas at the BS is fixed to $M = 100$. As in Fig. 2, we consider also the MR and the M-MMSE combining for different channel models (LoS and NLoS). In Fig. 3, it can be seen that the sum spectral efficiency of the system increases linearly with K for all considered cases since the multi users diversity increases.

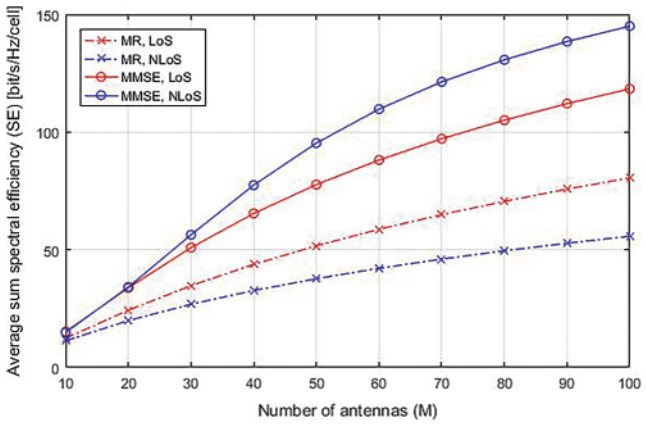

Figure 2: Uplink sum spectral efficiency in term of the number of base station (BS) antennas, $\boldsymbol{M}$, for two channel models, maximum ratio (MR) combiner, multi cell minimum mean-squared error (M-MMSE) combiner and number of sensor-actuator nodes (SANs) per cell, $\boldsymbol{K} = 25$

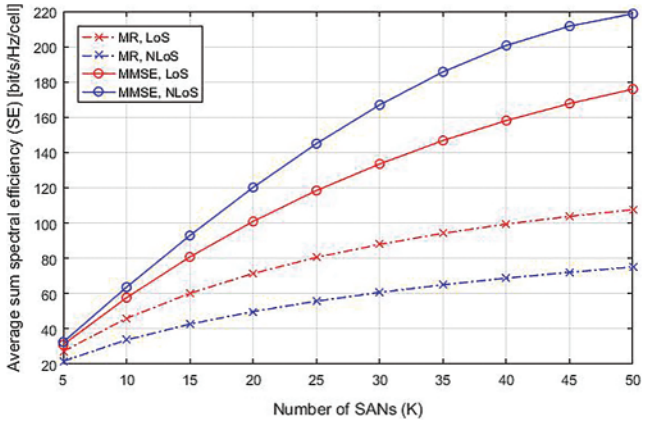

Figure 3: Uplink sum spectral efficiency in term of $\boldsymbol{K}$ (the number of SANs per cell), for two channel models, MR combiner, multi cell MMSE combiner and number of BS antennas $\boldsymbol{M} = 100$

Moreover, from both Figs. 2 and 3, one can see that the M-MMSE combining outperforms the MR combining. This can be explained by the fact that the multi-cell MMSE combiner prevents interferences better than the MR one. In addition, if we consider the maximum ration combiner, we notice that the spectral efficiency of our IoT system is significantly higher for the situation of line of sight propagation. However, if we consider the multi-cell MMSE combiner, we get the contrary performances. We can explain the obtained result as follow: in the NLoS situation, each SAN is influenced by interference caused by several SANs, however, in the LoS situation only a small number of SANs having close angles and causing intense interference. Since the resulted interference is suppressed, as with multi cell MMSE combiner, the spectral efficiency is higher in the NLoS situation.

We plot in Fig. 4, the average uplink sum spectral efficiency (SE) of the proposed irrigation system in term of the BS antennas to SANs ratio, M/K. In this figure, we consider the M-MMSE combining scheme for both channel models (LoS and NLoS). We can notice that the sum spectral efficiency grows linearly with the BS antennas to SANs ratio M/K. Indeed, when the number of BS antennas M increases proportionally to K ($M/K \gg 1$), the inter-user interference (that increases with K) is

suppressed. Notice that the case when $M/K = 1$ represents the traditional scheme adopted in the literature. We can clearly deduce that our proposed scheme ($M/K \gg 1$) outperforms the traditional one ($M/K = 1$). In fact, for the LoS case when $M/K = 4$ we obtain a 300% gain in spectral efficiency as compared to the traditional scheme. Moreover, as previously mentioned, the SE of the irrigation system is considerably low in the line of sight situation when using the M-MMSE combiner.

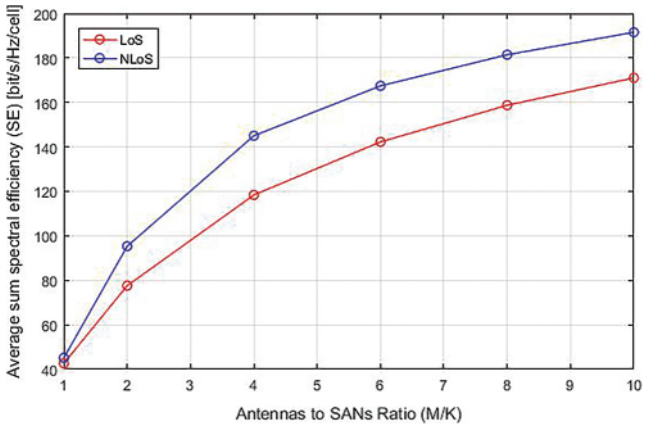

Figure 4: Average uplink sum spectral efficiency in term of the BS antennas to SANs ratio, $\boldsymbol{M/K}$, for the M-MMSE combining scheme and different channel models

We notice that, for simplicity, we provide (in Figs. 2–4) only the results of uplink spectral efficiency since the downlink spectral efficiency in our case study is very similar to the uplink spectral efficiency (especially when $M \gg 1$).

In Fig. 5, we plot the secrecy sum rate for the k-th SAN in term of the signal to noise ratio (SNR). The figure shows that the secrecy performance of the irrigation system is enhanced the use of artificial noise, especially when the SNR is greater than 10 dB.

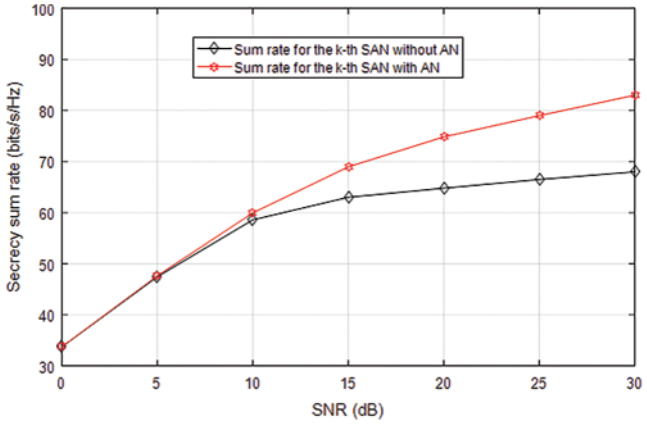

Figure 5: Achievable secrecy sum rate for the $\boldsymbol{k}$-th SAN in term of the signal to noise ratio (SNR)

5 Conclusions

In this work, we considered the problems of spectral efficiency and security in IoT-based irrigation systems for Olive Orchards in the Jouf region, KSA. We proposed the application of the massive MIMO technology. Indeed, this technology represents a keystone of the fifth generation (5G) and has the potential to improve spectral efficiency as well as the physical layer security. Specifically, we proposed to deploy under each olive tree a node responsible for sensing different environmental parameters (provided by the soil or the climate) and acting accordingly. The sensed data are forwarded to a remote processing server. This server compares the gathered information to the predefined threshold values. For any deviation from the threshold, the remote processing server will send, via the corresponding base station, a signal to the actuator for the purpose to activate the solenoid valve that irrigates the olive tree. Additionally, by exploiting the available M-MIMO channel degrees of freedom, we deployed a physical layer security scheme based on artificial noise (AN) to prevent eavesdropping. Numerical results demonstrated that our proposed scheme outperforms traditional ones in terms of spectral efficiency and secrecy rate.

In future work, we aim to address the problem of power allocation in order to optimize the proposed IoT-based irrigation system.

Acknowledgement: The authors extend their appreciation to the Deanship of Scientific Research at Jouf University for funding this work through research Grant No: (DSR-2021-02-0107).

Funding Statement: Our work was supported by the Deanship of Scientific Research (DSR) at Jouf University, Sakakah, Kingdom of Saudi Arabia under the Grant No: (DSR-2021-02-0107). The URL to sponsors' website: https://www.ju.edu.sa/en/administrations/deanships/deanship-of-scientific-research/home/.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Y. Kim, R. G. Evans and W. M. Iversen, "Remote sensing and control of an irrigation system using a distributed wireless sensor network," *IEEE Transactions on Instrumentation and Measurement*, vol. 57, no. 7, pp. 1379–1387, 2008.

[2] J. Gutiérrez, J. F. Villa-Medina, A. Nieto-Garibay and M. Á. Porta-Gándara, "Automated irrigation system using a wireless sensor network and GPRS module," *IEEE Transactions on Instrumentation and Measurement*, vol. 63, no. 1, pp. 166–176, 2014.

[3] Z. Zhang, P. Li, S. Zhao, Z. Lv, F. Du *et al.,* "An adaptive vision navigation algorithm in agricultural IoT system for smart agricultural robots," *Computers, Materials & Continua*, vol. 66, no. 1, pp. 1043–1056, 2021.

[4] K. Brun-Laguna, A. L. Diedrichs, D. Dujovne, R. Leone, X. Vilajosana *et al.,* "(Not so) intuitive results from a smart agriculture low-lower wireless mesh deployment," in *Proc. CHANTS*, New York, NY, USA, pp. 25–30, 2016.

[5] B. Queté, A. Heideker, I. Zyrianoff, D. Ottolini, J. H. Kleinschmidt *et al.,* "Understanding the tradeoffs of LoRaWAN for IoT-based smart irrigation," in *Proc. MetroAgriFor*, Trento, Italy, pp. 73–77, 2020.

[6] S. Millán, C. Campillo, J. Casadesús, J. M. Pérez-Rodríguez and M. H. Prieto, "Automatic irrigation scheduling on a hedgerow olive orchard using an algorithm of water balance readjusted with soil moisture sensors," *Sensors*, vol. 20, no. 9, pp. 2526, 2020.

[7] R. S. Krishnan, E. G. Julie, Y. H. Robinson, S. Raja, R. Kumar *et al.,* "Fuzzy logic based smart irrigation system using internet of things," *Journal of Cleaner Production*, vol. 252, pp. 119902, 2020.

[8] L. Raju K. and V. Vijayaraghavan, "IoT and cloud hinged smart irrigation system for urban and rural farmers employing MQTT protocol," in *Proc. ICDCS*, Coimbatore, India, pp. 71–75, 2020.
[9] A. Bhoi, R. P. Nayak, S. K. Bhoi and S. Sethi, "Automated precision irrigation system using machine learning and IoT," *Intelligent Systems*, vol. 185, pp. 275–282, 2021.
[10] S. K. Roy, S. Misra, N. S. Raghuwanshi and S. K. Das, "AgriSens: IoT-based dynamic irrigation scheduling system for water management of irrigated crops," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 5023–5030, 2021.
[11] P. Suresh, R. H. Aswathy, S. Arumugam, A. A. Albraikan, F. N. Al-Wesabi *et al.,* "IoT with evolutionary algorithm based deep learning for smart irrigation system," *Computers, Materials & Continua*, vol. 71, no. 1, pp. 1713–1728, 2022.
[12] L. García, L. Parra, J. M. Jimenez, J. Lloret and P. Lorenz, "IoT-based smart irrigation systems: An overview on the recent trends on sensors and IoT systems for irrigation in precision agriculture," *Sensors*, vol. 20, no. 4, pp. 1042, 2020.
[13] W. Tao, L. Zhao, G. Wang and R. Liang, "Review of the internet of things communication technologies in smart agriculture and challenges," *Computers and Electronics in Agriculture*, vol. 189, pp. 106352, 2021.
[14] B. B. Sinha and R. Dhanalakshmi, "Recent advancements and challenges of internet of things in smart agriculture: A survey," *Future Generation Computer Systems*, vol. 126, pp. 169–184, 2022.
[15] M. Gupta, M. Abdelsalam, S. Khorsandroo and S. Mittal, "Security and privacy in smart farming: Challenges and opportunities," *IEEE Access*, vol. 8, pp. 34564–34584, 2020.
[16] X. Yang, L. Shu, J. Chen, M. A. Ferrag, J. Wu *et al.,* "A survey on smart agriculture: Development modes, technologies, and security and privacy challenges," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 2, pp. 273–302, 2021.
[17] U. Ali, M. Y. I. Idris, J. Frnda, M. N. B. Ayub, R. Alroobaea *et al.,* "Hyper elliptic curve based certificateless signcryption scheme for secure IIoT communications," *Computers, Materials & Continua*, vol. 71, no. 2, pp. 2515–2532, 2022.
[18] A. Berguiga and A. Harchay, "An IoT-based intrusion detection system approach for TCP SYN attacks," *Computers, Materials & Continua*, vol. 71, no. 2, pp. 3839–3851, 2022.
[19] T. L. Marzetta, "Noncooperative cellular wireless with unlimited numbers of base station antennas," *IEEE Transactions on Wireless Communications*, vol. 9, no. 11, pp. 3590–3600, 2010.
[20] E. Björnson, J. Hoydis and L. Sanguinetti, "Massive MIMO networks: Spectral, energy, and hardware efficiency," *Foundations and Trends in Signal Processing*, vol. 11, no. 3–4, pp. 154–655, 2017.
[21] E. Björnson, E. G. Larsson and M. Debbah, "Massive MIMO for maximal spectral efficiency: How many users and pilots should be allocated?," *IEEE Transactions on Wireless Communications*, vol. 15, no. 2, pp. 1293–1308, 2016.
[22] A. S. Bana, E. Carvalho, B. Soret, T. Abrão, J. C. Marinello *et al.,* "Massive MIMO for internet of things (IoT) connectivity," *Physical Communication*, vol. 37, pp. 100859, 2019.
[23] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, 2008.
[24] A. Qu, X. Zhang, K. An, G. Zheng and S. Chatzinotas, "Secure transmission in massive MIMO system with specular component-based beamforming and artificial noise over ricean fading channel," *IEEE Wireless Communications Letters*, vol. 10, no. 11, pp. 2479–2483, 2021.
[25] Y. Qian, F. Ye and H. H. Chen, "Security in 5G wireless networks," *IEEE Security in Wireless Communication Networks*, vol. 14, pp. 279–310, 2022.