PLS Performance Analysis of a Hybrid NOMA-OMA based IoT System with Mobile Sensors

Hela Chamkhia[1], Aiman Erbad[2], Abdullah Al-Ali[1], Amr Mohamed[1], Ahmed Refaey[3], and Mohsen Guizani [1]
[1]Computer Science and Engineering, Qatar University, Qatar
[2]College of Science and Engineering, Hamad Bin Khalifa University, Qatar
[3]School of Engineering, The University of Guelph, ON, Canada

2022 IEEE Wireless Communications and Networking Conference (WCNC) | 978-1-6654-4266-4/22/$31.00 ©2022 IEEE | DOI: 10.1109/WCNC51071.2022.9771872

***Abstract*—With the advent of Internet of Things (IoT) systems, privacy and integrity of messages are becoming critical issues and are threatened, especially with mobile sensors. The broadcast nature of wireless communications increase information leakage in the presence of eavesdroppers. This paper proposes a hybrid Non-Orthogonal Multiple Access (NOMA)/Orthogonal Multiple Access (OMA)- based IoT systems to improve the data transmission security of moving sensors. We derive the Key Agreement Probability (KAP) expression of the proposed scheme, and we investigate the corresponding Secrecy Outage Probability (SOP) and the Average Bit Rate (ABR), when compared to pure NOMA and pure OMA transmission schemes. Simulation results are used to validate the derived expression and to evaluate the performance of the proposed scheme in terms of KAP, SOP, and ABR.**

***Index Terms*—Internet of Things, Channel-based Key Generation, NOMA, OMA, Physical layer Security.**

I. Introduction

WITH the rapid development of IoT smart devices, services, and applications, a large number of critical information is shared through mobile communication networks (such as 5G) [1], [2]. Faced with high latency, spectrum scarcity and a massive connectivity [3], [4], key technologies, such as millimeter wave, and multiple-input multiple-output (MIMO) [5], [6], have been used. Aligned with this, Non Orthogonal Multiple Access (NOMA) has been implemented to overcome the challenging future mobile communication network requirements and to potentially serve massive IoT systems [4]. In fact, NOMA techniques have the potential of using the same physical resources (time/ frequency/ code) by multiple users [7], [8], by harnessing superposition coding (SC) at the transmitters and successive interference cancellation (SIC) at the receivers [9], [10]. However, the broadcast nature of wireless communication impacts the communication security and increases the likelihood of information leakage in the presence of malicious eavesdroppers [7], [11]. Therefore, it is crucial to protect such sensitive data, and ensure confidentiality, integrity, and availability. Unlike, classic encryption-based techniques, where security establishment and key distribution are more complex [12], the physical layer key generation techniques offer complementary solution to encryption algorithms [13]–[15], by making use of the intrinsic properties of wireless channels. In fact, the channel reciprocity guarantees equivalent symmetric key, and the rich multi-path scattering environment offers uncorrelated channel measurements when eavesdroppers are located half-wavelength apart from legitimate nodes. Thus, eavesdroppers fail to extract key bits similar to those extracted by legitimate nodes. Besides, no infrastructure is required for key distribution and management.

Motivated by this, we propose a hybrid NOMA-OMA transmission scheme, where physical layer key generation is deployed, and latency-critical transmissions are considered. The contributions of the proposed work are summarized as follows:

- A Physical layer key generation based hybrid NOMA-OMA system is proposed to improve the security of IoT systems. First, mobile sensors perform key generation, and then based on the message urgency and the maximum estimated number of regular transmissions, the mode of transmission is decided.
- We provide the mathematical derivation of the Key Agreement Probability (KAP) between a given sensor and the access point. To the best of our knowledge, this is the first work to derive the analytical expression of the KAP with sensors' mobility.
- We present a comprehensive performance analysis of the Secrecy Outage Probability (SOP) and the Average bit Rate (ABR) in the presence of malicious eavesdroppers. Simulation results are compared with pure NOMA and pure OMA-based IoT systems.

The remainder of the paper is structured as follows. In Section II, the system model is introduced. Section III presents the proposed hybrid NOMA-OMA transmission scheme where channel-based key generation and users mobility are investigated. The derivation of the KAP expression is detailed in Section IV. In Section V, the numerical results are presented, where the performance of the proposed scheme is compared with that of pure NOMA and pure OMA, in terms of KAP, SOP, and ABR. The paper is finally concluded in Section VI.

II. System Model

With the rapid deployment of IoT healthcare, patients can upload their health data, such as blood pressure and heart rate, and hence get medical diagnosis and obtain professional healthcare advice [16]. Furthermore, with the increasing development of information technology, personnel medical devices acquired accuracy and portability, patients can receive an accurate medical diagnostic report everywhere and at anytime. Fig. 1 presents a general IoT-based healthcare

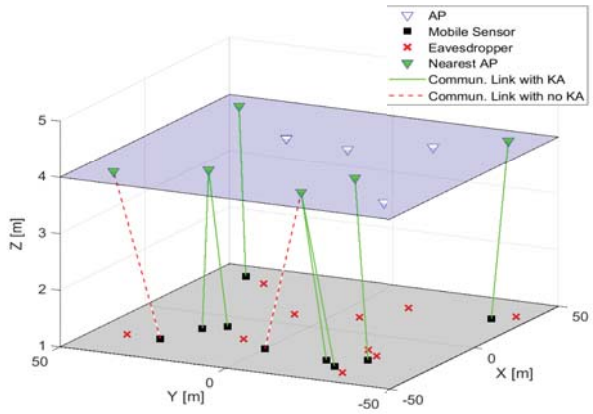

Fig. 1: System model.

system model, where Access Points (*APs*), Mobile Sensors (*MS*) and eavesdroppers are located in a 3-D space. The considered healthcare system model facilitates data collection and offers real-time transmissions. While the integration of sensors, wearable devices, and healthcare monitoring systems, is transforming the healthcare industry, massive connectivity becomes a major issue. Consequently, NOMA has been proposed as a promising solution that achieves better spectral utilization. In uplink NOMA, each near and far sensors are paired to simultaneously communicate the gathered information to the *AP*. We assume that the different links experience independent and identically distributed (i.i.d) Rayleigh fading subject to an additive white Gaussian noise (AWGN).

For data recovery, the SIC process is applied at the AP. In fact, the decoding starts with the near sensor message, by treating the low power received message of the far sensor as noise. Then, it performs SIC to remove the previously decoded high power received message, and be able to recover the far sensor message.

In addition to the use of NOMA technique, we propose a PLS-based scheme to enhance the considered system security and reliability, where a hybrid NOMA/OMA communication is possible. In the following section, we present the proposed hybrid NOMA-OMA based IoT system.

To evaluate the sensors mobility impact on the system performance, the classical random way point (RWP) model is adopted in this work [17]. The RWP model can be used to generate the movement trace of a given MS. For a given position, and a given movement period, the MS selects a random direction, and moves to the next position that is identified by the selected direction, movement period, and the MS speed.

III. Proposed Communication Scheme

In this section, we present the proposed communication scheme which takes into consideration the physical layer key generation, the hybrid NOMA/OMA access, and the mobility aspect of the sensors. The proposed scheme is based on the physical layer properties, where communicating parties can benefit from the channel reciprocity for equivalent symmetric key generation. Moreover, security is enhanced since no key exchange step is required [1], [18]. Based on that, we present in Fig. 2 the proposed scheme that consists of the following main steps:

- *Channel Probing:* First, the AP and each MS_i exchange synchronisation signals to estimate the physical layer characteristics [19], where the uplink (UL) and the downlink (DL) Channel State Information (CSI) real parts are considered in this work.
- *Quantization:* The quantization is the second step of the key generation process, where the estimated UL and DL CSI real parts that are denoted by CSI_{MS_i-AP} and CSI_{AP-MS_i}, respectively, are quantized to generate the corresponding bit streams. In this work, we have considered the adaptive quantization technique presented in [20]. As a result of the quantization, two vectors for each link are generated; the first vector contains the initial bit stream key_0, and the second vector represents the corresponding peak positions PV_0 of the estimated CSI.
- *Reconciliation:* The end users have to make sure that the generated keys are similar, as it is expected to have mismatching bit streams after performing the quantization due to the different noise levels, synchronisation errors, or possible quantization errors. The mismatches can be corrected in the reconciliation stage as follows: First, each MS_i should transmit its $PV0_{MS_i}$ vector to the AP. Then, the AP compares the received position vector with its own position vector and update the position vector by removing the nonexistent bits in both position vectors. The updated position vector $PV0_{MS_i}$ is then send to the mobile sensor. Afterwards, the AP and the mobile users have to confirm that the resulting keys at both sides are similar. Accordingly, the AP encrypts a randomly generated message R with its key and sends it to the MS_i. After receiving the encrypted message X, the MS_i decrypts it with its own key, increments the result by one, then encrypts it and sends the result back to the AP. The received message is decrypted at the AP and the result is compared with the message $R+1$. The generated keys are considered only when the messages in the AP are equal. On the contrary, the MS_i transmission depends on two counters. The first one is the regular transmission tentative number n, which allows the sensor to transmit if it exceeds the maximum number of tentative N_{max}. The second counter is the urgent transmission tentative number m, which allows the MS_i to transmit time-critical message if it exceeds the maximum number of urgent tentative M_{max}. Meanwhile, when neither the maximum regular tentative number nor the maximum urgent tentative number are met, and their was no successful key agreement between the AP and the MS_i, the user should restart the first step of channel probing as indicated in Fig. 2.
- *Privacy Amplification:* This process aims to increase the key randomness, by using SHA-2 for example. In

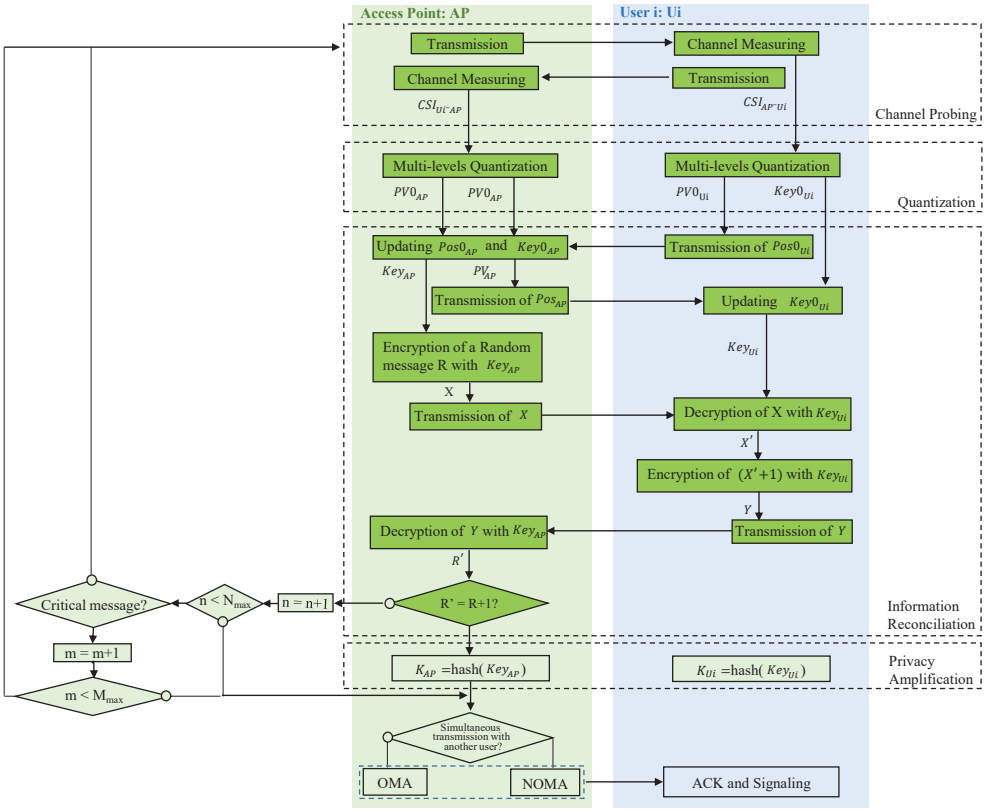

Fig. 2: Proposed Hybrid NOMA-OMA IoT Transmission Scheme.

fact, when the key reconciliation is performed, some bits are deduced from the initially generated key, when a mismatch is reported. Hence, privacy amplification ensures higher entropy.

Now, we need to decide which transmission mode will be performed based on the key generation process, as presented in Fig. 2. If both mobile sensors are transmitting (either with a generated key, or due to exceeding one of the maximum tentative numbers), the NOMA transmission will be selected. However, if only one of the users is transmitting, transmission will be selected. Finally, if both users are not transmitting, there will be no transmission.

IV. Performance Analysis

The proposed hybrid IoT transmission is mainly based on the key agreement procedure between the different mobile sensors and the corresponding APs. In order to evaluate the performance of our proposed scheme, we derive in this section the key agreement probability expression. In the simulation results, the secrecy outage probability and the average bit rate (ABR) are presented and compared with conventional pure OMA and pure NOMA transmissions.

The KAP is defined as the probability of the event, when a given sensor and its nearest AP have agreed on the generated secure key. The expression of this probability is related to the Bit Agreement Probability (BAP), which presents the probability that the communicating sides agreed on a given bit of the generated binary key. Mathematically, the BAP expression can be written as follows:

$$BAP = 1 - Pr\left\{\left((\hat{CSI}_{MS_i-AP} \geq L_0) \cap (\hat{CSI}_{AP-MS_i} \leq -L_0)\right) \cup \left((\hat{CSI}_{AP-MS_i} \geq L_0) \cap (\hat{CSI}_{MS_i-AP} \leq -L_0)\right)\right\} \quad (1)$$

where, L_0 is the minimum predefined quantization level, and $\hat{CSI}_{MS_i-AP}$ and $\hat{CSI}_{AP-MS_i}$ are the CSI estimates of the links $MS_i - AP$, and $AP - MS_i$, respectively, with the corresponding error $e_{MS_i-AP} = \hat{CSI}_{MS_i-AP} - CSI_{MS_i-AP}$, and $e_{AP-MS_i} = \hat{CSI}_{AP-MS_i} - CSI_{AP-MS_i}$. Accordingly, (1) can be rewritten as follows:

$$BAP = 1 - Pr\left\{\left(\left(e_{MS_i-AP} \geq \left[L_0 - CSI_{MS_i-AP}\right]\right) \cap \left(e_{AP-MS_i} \leq \left[-L_0 - CSI_{AP-MS_i}\right]\right)\right) \cup \left(\left(e_{AP-MS_i} \geq \left[L_0 - CSI_{AP-MS_i}\right]\right) \cap \left(e_{MS_i-AP} \leq \left[-L_0 - CSI_{MS_i-AP}\right]\right)\right)\right\}. \quad (2)$$

Given that e_{MS_i-AP} and e_{AP-MS_i} are two independent random variables, (2) can be expressed as follows:

$$BAP = 1 - \left\{ Pr\left\{ e_{MS_i-AP} \geq [L_0 - CSI] \right\} Pr\left\{ e_{AP-MS_i} \leq [-L_0 - CSI] \right\} + Pr\left\{ e_{AP-MS_i} \geq [L_0 - CSI] \right\} Pr\left\{ e_{MS_i-AP} \leq [-L_0 - CSI] \right\} \right\}. \quad (3)$$

Assuming that the different links experience symmetric i.i.d Rayleigh fading, the CSI PDF expression is given by:

$$f_{CSI}(x) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{x^2}{2\sigma^2} \right), \quad (4)$$

with, $\sigma^2 = A\ d_{AP-MS_i}^{-(\alpha+1)}$, where, d_{AP-MS_i} is the distance between MS_i and its nearest AP. This distance can be expressed as $\sqrt{r_i^2 + (H_{AP} - H_{MS_i})^2}$, with H_{AP} and H_{MS_i} are the heights of AP and MS_i, respectively. According to the proposed system model, the PDF expression is given by [2]:

$$f_{r_i}(r) = 2\pi r\ \lambda_{AP} \exp\left(-\pi r^2 \lambda_{AP} \right) \quad (5)$$

In addition, the error e_{MS_i-AP} and e_{AP-MS_i} are assumed to be random variables with the same PDF expression, given by:

$$f_{e_{MS_i-AP}}(y) = f_{e_{AP-MS_i}}(y) = \frac{1}{\sqrt{2\pi\sigma_e^2}} \exp\left(-\frac{y^2}{2\sigma_e^2} \right), \quad (6)$$

with, $\sigma_e^2 = \frac{P_N}{P_T}$, P_N is the noise power, and P_T is the transmit power. Consequently, the BAP expressed in (3) is derived as follows:

$$BAP = 1 - \int_{-\infty}^{+\infty} f_{r_i}(r) \int_{-\infty}^{+\infty} \left(\int_{L_0-x}^{+\infty} f_{e_{MS_i-AP}}(y)\ dy \int_0^{-L_0-x} f_{e_{AP-MS_i}}(z)\ dz - \int_{L_0-x}^{+\infty} f_{e_{AP-MS_i}}(z)\ dz \int_0^{-L_0-x} f_{e_{MS_i-AP}}(y)\ dy \right) f_{CSI}(x)\ dx\ dr, \quad (7)$$

As the errors have the same PDF expressions, (7) can be simplified to be

$$BAP = 1 - \int_{-\infty}^{+\infty} f_{r_i}(r) \int_{-\infty}^{+\infty} 2\ f_{CSI}(x) \times \left(\int_{L_0-x}^{+\infty} f_{e_{MS_i-AP}}(y)\ dy \int_0^{-L_0-x} f_{e_{MS_i-AP}}(z)\ dz \right) dx\ dr. \quad (8)$$

Now, by using the PDF expressions of the CSI, and e_{MS_i-AP}, the BAP can be evaluated as follows:

$$BAP = 1 - \int_{-\infty}^{+\infty} f_{r_i}(r) \int_{-\infty}^{+\infty} 2 \left(\int_{L_0-x}^{+\infty} \frac{1}{2\pi\sigma_e^2} \exp\left(-\frac{y^2}{2\sigma_e^2} \right) dy \times \int_0^{-L_0-x} \exp\left(-\frac{z^2}{2\sigma_e^2} \right) dz \right) \frac{1}{\sqrt{2\pi\sigma_x^2}} \exp\left(-\frac{x^2}{2\sigma_X^2} \right) dx\ dr. \quad (9)$$

After evaluating the integrals in (9), with respect to y and z, the BAP expression can be rewritten as follows:

$$BAP = 1 - \int_{-\infty}^{+\infty} f_{r_i}(r) \int_{-\infty}^{+\infty} \frac{1}{2} \left(\left[1 - \mathrm{erf}\left(\frac{L_0 - x}{\sqrt{2\sigma_e^2}} \right) \right] \times \left[1 + \mathrm{erf}\left(\frac{-L_0 - x}{\sqrt{2\sigma_e^2}} \right) \right] \right) \frac{1}{\sqrt{2\pi\sigma_x^2}} \exp\left(-\frac{x^2}{2\sigma_X^2} \right) dx\ dr. \quad (10)$$

where, $\mathrm{erf}(x)$ presents the error function. By using the expression (8.259.1) in [21], and after some simplifications, the BAP is expressed as:

$$BAP = \frac{1}{2} \int_{-\infty}^{+\infty} f_{r_i}(r) \left[1 + \mathrm{erf}\left(\frac{L_0}{\sqrt{2\sigma^2 + 2\sigma_e^2}} \right) - \mathrm{erf}\left(\frac{-L_0}{\sqrt{2\sigma^2 + 2\sigma_e^2}} \right) + \frac{1}{\sqrt{2\pi\sigma^2}} \times \int_{-\infty}^{+\infty} \mathrm{erf}\left(\frac{L_0 - x}{\sqrt{2\sigma_e^2}} \right) \mathrm{erf}\left(\frac{-L_0 - x}{\sqrt{2\sigma_e^2}} \right) \exp\left(-\frac{x^2}{2\sigma^2} \right) dx \right] dr \quad (11)$$

By using the expression (2.7.1.3) in [22], and after some simplifications, the approximate expression of (11) is given by:

$$BAP \approx \frac{1}{2} + \int_0^{\infty} f_{d_{AP-MS_i}}(r) \times \left[\mathrm{erf}\left(\frac{L_0}{\sqrt{2\sigma(r)^2 + 2\sigma_e^2}} \right) + \frac{1}{\pi} \mathrm{atan}\left(\frac{\sigma^2}{\sqrt{\sigma_e^4 + 2\sigma_e^2\sigma(r)^2}} \right) \right] dr \quad (12)$$

Finally, using the Laguerre theorem [10] yields the final BAP expression:

$$BAP \approx \frac{1}{2} + \sum_{k=1}^{N} w_k \left\{ \mathrm{erf}\left(\frac{L_0}{\sqrt{2\sigma_k^2 + 2\sigma_e^2}} \right) + \frac{1}{\pi} \mathrm{atan}\left(\frac{\sigma_k^2}{\sqrt{\sigma_e^4 + 2\sigma_e^2\sigma_k^2}} \right) \right\} \quad (13)$$

where,

$$\sigma_k^2 = A \left[\frac{3\sqrt{x_k^2 + (H_{AP} - H_{MS_i})^2}}{4\pi\lambda_{AP}} \right]^{-\frac{\alpha+1}{2}}. \quad (14)$$

with w_k and x_k that represent the k^{th} weights and roots of the Laguerre polynomial of order N. By using the approximate expression of BAP presented in (13), the KAP expression can be given as follows:

$$KAP = BAP^{KL_0}. \quad (15)$$

where KL_0 is the maximum key length.

V. Numerical Results and Discussions

In this section, we present the conducted numerical results to confirm the derived analytical expression and evaluate the performance of the proposed scheme. Without loss of generality, the simulation parameters are set to be as follows: The side-length of the considered environment is 100 m, $H_{AP} = 4$ m, $H_{MS} = 1$ m, the eavesdroppers' density $= 1e-4$ m^{-2}, the noise power is -110 dB, the secrecy rate threshold $= 0$, the maximum key length $KL_0 = 64$, $N_{max} = 20$, and $M_{max} = 10$.

Fig. 3 presents the instantaneous key agreement vs. time, with two different mobile speeds; a) 0.5 m/s, and b) 3 m/s. As shown in this figure, by increasing the mobile speed, the instantaneous key agreement variation increases. In fact, increasing the mobile speed increases the number of handover

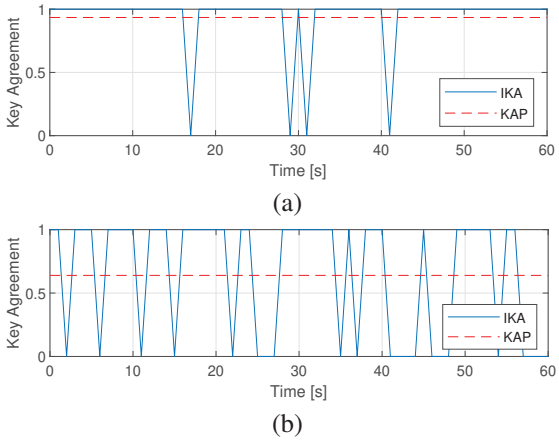

Fig. 3: Instantaneous key agreement (IKA) vs. time, with a) mobile speed = 0.5 m/s, and b) mobile speed = 3 m/s.

between the APs, and hence the probability of a key agreement change, for a given link, increases. However, with a low mobile speed, the handover is rare, and the communication channel is less selective in time. Also, it is shown that the KAP is high for the low speed, which is expected. In fact, for this example, the mobile sensor started with an instantaneous key agreement that remains stable most of the time, as the probability of the handover is low, and the channel is not very selective in time (due to the low mobile speed) to affect the generation of the secured key, and hence the key agreement.

The KAP vs. APs' density, with a mobile speed = 1.5 m/s, and different transmit powers is presented in Fig. 4. The figure confirms the accuracy of the derived KAP expression that fits well the simulation results for the different APs' densities and the transmit power levels. By increasing the APs' density and the transmit power, the KAP increases, which is expected. This is because the increase of these parameters enhance the link reliability between the nodes, which reduces the channel estimation error, and hence an improvement of the KAP can be observed.

In Fig. 5, the key agreement ratio vs. transmit power, with a mobile speed = 1.5 m/s, and different APs' density is

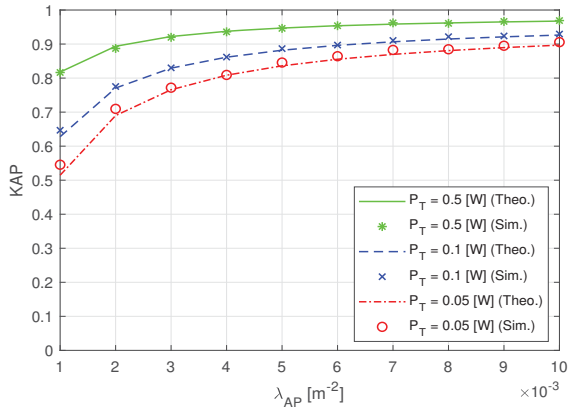

Fig. 4: Key agreement probability vs. APs' density, with a mobile speed = 1.5 m/s, and different transmit Powers.

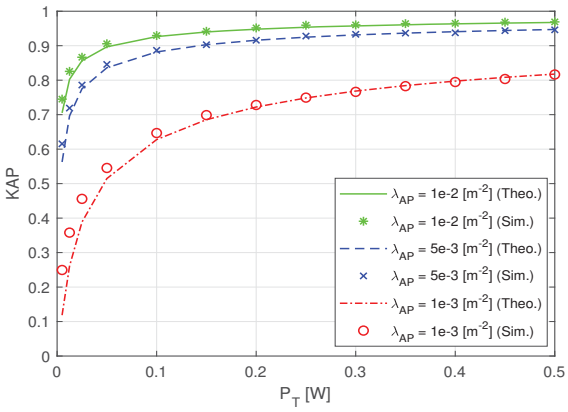

Fig. 5: Key agreement probability vs. Transmit Power, with a mobile speed = 1.5 m/s, and different APs' density

presented. From this figure, we can observe the major impact of the used number of APs on the KAP, when compared to the transmit power. As an example, with a low transmit power of 0.1 W, we can reach a KAP larger than 0.9, with a high APs' density, e.g. $\lambda_{AP} = 7.10^{-3}$ m^{-2}. However, with a low density, e.g. $\lambda_{AP} = 10^{-3}$ m^{-2}, the KAP can reach a maximum of 0.82 KAP, even with the use of high transmit power.

The SOP of the different considered transmission schemes vs. APs' density, with a mobile speed = 1.5 m/s, and a transmit power = 5 mW is presented in Fig. 6. As shown in this figure, the SOP decreases with the increased APs' density, with a better performance of the proposed scheme, when compared to that of the pure NOMA and OMA schemes. This is due to the fact that, increasing the APs' density, enhances the link reliability between the sensors and the corresponding APs, which results in enhancement of the legal link and the KAP, and hence an improvement of the proposed scheme SOP can be depicted. However, the other schemes benefit only from the enhancement of the legal link, as no PLS mechanism is considered. Moreover, the pure NOMA offers a better spectrum efficiency than the pure OMA, that is why the legal link efficiency and the corresponding SOP is better than the OMA scheme, where the available resources (spectrum/time) should be shared between the different sensors.

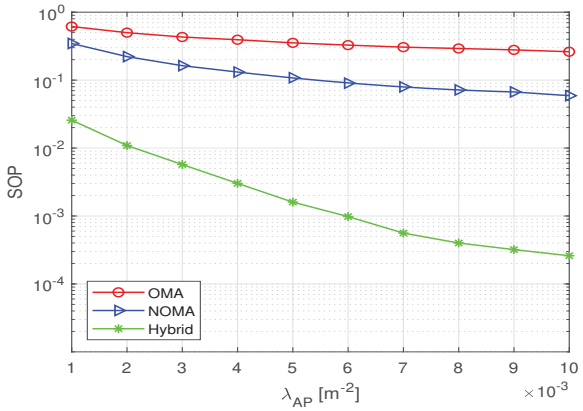

Fig. 6: SOP of the different transmission schemes vs. APs' density, with a mobile speed = 1.5 m/s, and a transmit power = 5 mW.

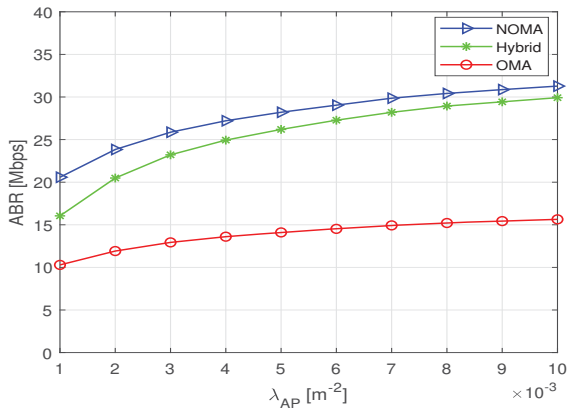

Fig. 7: Average bit rate vs. transmit power and APs' density, with a mobile speed = 1.5 m/s, a given frequency bandwidth = 2 [MHz], and a transmit power = 5 mW.

In Fig. 7, we present the average bit rate vs. transmit power and APs' density, with a mobile speed = 1.5 m/s, a given frequency bandwidth = 2 [MHz], and a transmit power = 5 mW. Different from the behaviour of the SOP, the proposed scheme outperforms the pure OMA scheme in terms of ABR, and offers a close performance to that of the pure NOMA. In fact, the pure NOMA is always transmitting via the whole available resources, without any security measure, which enhances the spectrum efficiency and hence the ABR. However, within the proposed scheme, the transmission is allowed only if a key agreement is done or a maximum number of transmission iterations is reached, which slightly reduces the corresponding ABR, with respect to the pure NOMA transmission.

VI. Conclusion

In this paper, we have presented PLS performance analysis of a proposed hybrid NOMA-OMA based IoT system with mobile sensors, using a realistic 3-D stochastic geometry model. The considered IoT system model and the proposed hybrid IoT system were described. KAP expression have been derived. Based on that, numerical results have been conducted to evaluate the performance of the proposed scheme when compared to the pure OMA and NOMA scheme, in terms of KAP, SOP, and ABR.

Acknowledgement

This publication was made possible by NPRP-Standard (NPRP-S) Thirteen (13th) Cycle grant # NPRP13S-0205-200265 from the Qatar National Research Fund (a member of Qatar Foundation). The findings herein reflect the work, and are solely the responsibility, of the authors.

References

[1] J. Liu, Q. Hu, R. Suny, X. Du, and M. Guizani, "A Physical Layer Security Scheme with Compressed Sensing in OFDM-based IoT Systems," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 2020, pp. 1–6.

[2] H. Chamkhia and A. Erbad and A. Al-Ali and A. Mohamed and A. Refaey and M. Guizani, "3-D Stochastic Geometry-based Modeling and Performance Analysis of Efficient Security Enhancement scheme for IoT Systems," *IEEE Internet of Things Journal*, pp. 1–1, 2021.

[3] Usman Mahmood Malik, Muhammad Awais Javed, Sherali Zeadally, and Saif ul Islam, "Energy efficient fog computing for 6g enabled massive iot: Recent trends and future opportunities," *IEEE Internet of Things Journal*, pp. 1–1, 2021.

[4] Xin Wan, Xu Zhu, Yufei Jiang, Yujie Liu, and Jiahe Zhao, "An interference alignment and ica-based semiblind dual-user downlink noma system for high-reliability low-latency iot," *IEEE Internet of Things Journal*, vol. 7, no. 11, pp. 10837–10851, 2020.

[5] Long Jiao, Ning Wang, Pu Wang, Amir Alipour-Fanid, Jie Tang, and Kai Zeng, "Physical layer key generation in 5g wireless networks," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 48–54, 2019.

[6] Y. Cao, N. Zhao, Y. Chen, M. Jin, Z. Ding, Y. Li, and F. R. Yu, "Secure Transmission via Beamforming Optimization for NOMA Networks," *IEEE Wireless Communications*, vol. 27, no. 1, pp. 193–199, 2020.

[7] Z. Xiang, W. Yang, Y. Cai, J. Xiong, Z. Ding, and Y. Song, "Secure Transmission in a NOMA-Assisted IoT Network With Diversified Communication Requirements," *IEEE Internet of Things Journal*, vol. 7, no. 11, pp. 11157–11169, 2020.

[8] Wali Ullah Khan, Ju Liu, Furqan Jameel, Vishal Sharma, Riku Jäntti, and Zhu Han, "Spectral efficiency optimization for next generation noma-enabled iot networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 15284–15297, 2020.

[9] Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan, and V. K. Bhargava, "A Survey on Non-Orthogonal Multiple Access for 5G Networks: Research Challenges and Future Trends," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 10, pp. 2181–2195, 2017.

[10] H. Chamkhia and A. Al-Ali and A. Mohamed and M. Guizani and A. Erbad and A. Refaey, "Performance Analysis of IoT Physical layer Security Using 3-D Stochastic Geometry," in *2020 International Conference on Computational Science and Computational Intelligence (CSCI)*, 2020, pp. 1022–1027.

[11] Zhongwu Xiang, Weiwei Yang, Yueming Cai, Zhiguo Ding, Yi Song, and Yulong Zou, "Noma-assisted secure short-packet communications in iot," *IEEE Wireless Communications*, vol. 27, no. 4, pp. 8–15, 2020.

[12] Ning Wang, Pu Wang, Amir Alipour-Fanid, Long Jiao, and Kai Zeng, "Physical-layer security of 5g wireless networks for iot: Challenges and opportunities," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8169–8181, 2019.

[13] Kai Zeng, "Physical Layer Key Generation in Wireless Networks: Challenges and Opportunities," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 33–39, 2015.

[14] Reem Melki, Hassan N. Noura, and Ali Chehab, "Lightweight and secure d2d authentication key management based on pls," in *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*, 2019, pp. 1–7.

[15] Yuli Yang, Meng Ma, Sonia Aïssa, and Lajos Hanzo, "Physical-layer secret key generation via cqi-mapped spatial modulation in multi-hop wiretap ad-hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1322–1334, 2021.

[16] Yin Zhang, Yi Sun, Yi Sun, Renchao Jin, Kaixiang Lin, Kaixiang Lin, Wei Liu, and Wei Liu, "High-performance isolation computing technology for smart iot healthcare in cloud environments," *IEEE Internet of Things Journal*, pp. 1–1, 2021.

[17] X. Lin and et al, "Towards Understanding the Fundamentals of Mobility in Cellular Networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 4, pp. 1686 – 1698, 2013.

[18] S. Ribouh, K. Phan, A. V. Malawade, Y. Elhillali, A. Rivenq, and M. A. A. Faruque, "Channel State Information-Based Cryptographic Key Generation for Intelligent Transportation Systems," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–12, 2020.

[19] A. Badawy, T. Elfouly, T. Khattab, C. F. Chiasserini, A. Mohamed, and D. Trinchero, "Robust secret key extraction from channel secondary random process," *Wireless Communications and Mobile Computing*, vol. 16, no. 11, pp. 1389–1400, 2016.

[20] S. T. Ben Hamida, J. Pierrot, and C. Castelluccia, "An Adaptive Quantization Algorithm for Secret Key Generation Using Radio Channel Measurements," pp. 1–5, 2009.

[21] I.S. Gradshteyn and I.M. Ryzhik, *Table of Integrals, Series, and Products*, Academic Press, 2014.

[22] NIKOLAI . KOROTKOV and ALEXANDER N. KOROTKOV, *Table of Integrals Related to Error Function*, 2019.