Optimization of Secure Emergency Call Services in Asynchronous-NOMA D2D Network

Vishaka Basnayake[1,2], Ambrish Kumar[1], Dushantha Nalin K. Jayakody[3]
Sri Lanka Technological Campus (SLTC Research University), 10500 Padukka, Sri Lanka[1]
DISC/FEMTO-ST, Univ. Bourgogne Franche-Comte, Cours Louis Leprince-Ringuet, 25200, Montbeliard, France[2]
Centro de Investigaçă em Tecnologias - Autónoma TechLab, Universidade Autónoma de Lisboa, Lisbon, Portugal[3]
vishakab@sltc.ac.lk

***Abstract*—This paper investigates the issue of improving secrecy capacity of device-to-device (D2D) communications in disaster scenarios under the presence of jammers in close proximity. Furthermore, an asynchronous-non orthogonal multiple access (A-NOMA) assisted transmission scheme is considered due to the resource limitations and the asynchrony in signal receptions in out-of-coverage D2D scenarios. A binary optimization problem is proposed to select the optimal data which enhances the sum secrecy capacity of the transmissions. The results show that the proposed optimized scheme outperforms the conventional secrecy capacity.**

***Index Terms*—Asynchronous-NOMA, binary optimization, D2D, secrecy capacity**

I. Introduction

Reliable emergency call services are required to save victims during catastrophes in a timely manner. The presence of jammers in a disaster areas can impact the reliability of the emergency call transmissions. Hence, enhancing the secrecy capacity of the wireless communication networks has become one of the research focuses in the B5G/6G networks [1]. Moreover, D2D assisted multi-hop emergency protocols have been proposed for emergency call transmissions [2]. In D2D networks, due to the distributed locations of the transmitters, signals arrive at the receiving terminal with varying time offsets and hence, time-synchronous data reception is not possible. In [3], an asynchronous NOMA (A-NOMA) scheme is proposed for enhancing spectral efficiency and reducing the bit error rate (BER) of the communication.

Hence, in this work a novel binary optimization problem is proposed for optimal data detection which will enhance the secrecy capacity of an A-NOMA assisted D2D communication under the presence of jamming users. Further, the secrecy capacity of the proposed optimized scheme is compared with the conventional secrecy capacity values.

II. System model and problem formulation

A. System overview

We assume a multi-hop emergency call forwarding system for a network area under a disaster, where device-to-device (D2D) uplink transmissions are occurring between a $k \leq K$ number of victim/relay nodes (e.g., Victim A, Victim B, etc), and $r \leq R$ number of receiving victim/relay nodes (e.g., Victim C, etc) as shown in Figure 1. However, such k transmitters can comprise of an equal number of both $m \leq K$ legitimate users, and $e \leq K$ jamming users, and $m + e = K$. It is assumed that such e nodes (e.g. Jammer A, etc) send a noisy data signal toward the receiver nodes to deteriorate its decoding ability. Moreover, all users are geographically distributed within a small local neighborhood. Hence, the total K users share a single subcarrier out of a total N subcarriers that are allocated to the D2D communication system. In addition, in the realistic channel conditions, we assume that the signals are affected through propagation delays, and hence, signals between transceivers are received asynchronously. Thus, an A-NOMA scheme is utilized to decode the received data signals.

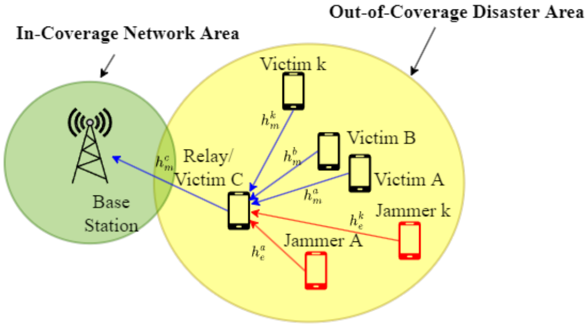

Figure 1: Asynchronous-NOMA uplink scheme for D2D Emergency Call Forwarding Services.

The received signal for the k^{th} user at sth symbol is given as,

$$y^k[s] = h^k.\sqrt{P^k}.x^k[s] + \eta^k_{k,i}[s] + n_0, \tag{1}$$

where $k \in \{\text{Victim } k, \text{Jammer } k\}$ and $x^k[s]$ denotes the sth symbol of the k^{th} user's data which is complex and generated by a higher modulation M-ary QAM symbol mapper. P^k denotes the transmission power of k^{th} user, h^k denotes the k^{th} user channel state information (CSI) and $\eta^k_{k,i}[s]$ denotes the interference from other ith users on the desired k^{th} user's sth symbol. Additionally, the received signal to noise ratio (SINR) of the k^{th} user, γ^k, is formed as,

$$\gamma^k = \frac{P^k g^k}{\text{Var}(\eta^k_{k,i}) + \sigma^2}, \tag{2}$$

where the channel gain of k^{th} user, thermal noise variance are given by g^k, σ^2 respectively. The γ^k_m of the m^{th} user

$\gamma_m^k = \frac{P_m^k g_m^k}{\text{Var}(\eta_{m,i}^k)+\sigma^2}$. It is assumed that the receiver detects the presence of a jammer e during the post processing stage and the γ_e^k of such an e user $\gamma_e^k = \frac{P_e^k g_e^k}{\text{Var}(\eta_{e,i}^k)+\sigma^2}$.

B. Optimization

The objective is to detect the optimal combination of s symbols of each k user which maximizes number of decoded symbols, n_{sym}, of the A-NOMA transmissions under the presence of e users. Further, a binary decision vector of the optimal data symbols to be decoded is introduced as $\boldsymbol{D} = [D_k]_{k\in\mathcal{K}}$, where D_k = 1 if the data symbols of the k^{th} user are selected to be decoded, and $n_{sym} = \sum_{k=1}^{K} D_k(K-k+1)$. The number of symbols decoded per each k^{th} user is $(K-k+1)$ under the T-SIC decoding scheme proposed in [3] for A-NOMA schemes. Hence, an optimization problem is formed as ,

$$\underset{\boldsymbol{D}}{\text{maximize}} \quad \sum_{k=1}^{K} D_k(K-k+1) \tag{3a}$$

$$\text{subject to} \quad c_r \geq 0, \tag{3b}$$

where,

$$c_r = D_k\Bigg[\left\{B\log_2\left(1+\gamma_m^k\right) - R_{\text{min}}\right\} - \left\{R_{\text{max}} - B\log_2\left(1+\gamma_e^k\right)\right\}\Bigg]^+, \tag{4}$$

here $[]^+$ represents a positive quantity, which means that (4) is valid is positive or $\gamma_m^k \geq \gamma_e^k$ and $R_{max} \geq R_{\text{min}}$. The solutions derived from such an optimization problem is used thereby to maximize the sum-secrecy capacity, C_s, of the communication system given as [1],

$$C_s = \sum_{k=1}^{K} D_k \log_2\left(\frac{1+\gamma_m^k}{1+\gamma_e^k}\right). \tag{5}$$

Further, k^{th} user data with $D_k = 1$ are decoded while the remaining users' data are decoded upon the reception of retransmissions from such users.

III. Performance analysis

The performance of the proposed algorithm is evaluated for a D2D A-NOMA transmission with three m users and three e users. For simplicity, a unit total bandwidth of 1 Hz, equal P_m^k for each m user and equal P_e^k for each e user, and a channel with Rayleigh fading is considered. In addition, R_{min} and R_{max} are set to 1 Hz and 10 Hz respectively. The distance gap between the transmitters and its associated receiver is uniformly distributed in [0m, 100m]. Further, the noise level of the channel n_0 is set to 0.1W.

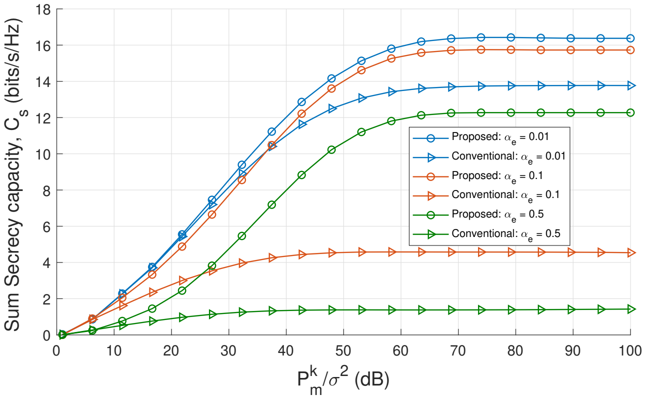

Figure 2: Sum secrecy capacity vs P_m^k/σ^2 in an A-NOMA assisted D2D uplink communication under different α_e values.

Figure 2 depicts the variation of C_s against the transmit SNR at the legitimate user, under different $\alpha_e = \frac{P_e^k}{P_m^k}$ values. Variation of C_s is considered under the proposed scheme and compared with the conventional C_s under $\alpha_e \in 0.01, 0.1, 0.5$. It is seen that as the α_e increases, the C_s decreases. The reason is that as jammer's γ_e^k increases, the $\log_2(1+\gamma_e^k)$ increases and hence C_s decreases. Moreover, it is seen that the proposed scheme achieves a higher C_S value compared to the conventional C_s when the transmit SNR of the legitimate m user is increased. The $D_k = 0$ for the k^{th} user data with $\gamma_e^k > \gamma_m^k$, and hence such data are omitted from decoding and only the reliable data with $\gamma_e^k \leq \gamma_m^k$ are decoded. Meanwhile, in the conventional C_s, the k^{th} user data with $\gamma_e^k > \gamma_m^k$ result in $C_{s_k} \leq 0$. In addition, the achievable C_s converges as the optimal D_k vector is reached under the constraint imposed by c_r. To sum up, the proposed scheme C_s becomes higher than the conventional C_s and it was observed that the proposed scheme achieves a C_s gain of 30.7%, 75.4%, 84.0% under α_e values of 0.01, 0.1, and 0.5, than the conventional C_s.

IV. Conclusion

The problem of improving the achievable C_s in an A-NOMA enabled D2D communication under the presence of jammers in a disaster scenario is studied in this paper. A binary optimization algorithm is proposed for reliable data detection at the receiver by taking the γ values of the legitimate users and jammers into account. It is observed that the proposed optimized scheme outperforms the conventional C_s with a gain of 30.7%, 75.4%, 84.0% under α_e values of 0.01, 0.1 and 0.5.

V. Acknowledgements

This work is funded, in part, by the CEU-Cooperativa de Ensino Universitário, Portugal.

References

[1] A. Kumar and D. N. K. Jayakody, "Secure noma-assisted multi-led underwater visible light communication," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 7, pp. 7769–7779, 2022.

[2] V. Basnayake, H. Mabed, D. N. K. Jayakody, and P. Canalda, "M-help - multi-hop emergency call protocol in 5g," in *2020 IEEE 19th International Symposium on Network Computing and Applications (NCA)*, 2020, pp. 1–8.

[3] H. Haci, H. Zhu, and J. Wang, "Performance of non-orthogonal multiple access with a novel asynchronous interference cancellation technique," *IEEE Transactions on Communications*, vol. 65, no. 3, pp. 1319–1335, 2017.