Vamvakas *et al. EURASIP Journal on Wireless Communications and Networking* (2019) 2019:286
https://doi.org/10.1186/s13638-019-1616-9

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Exploiting prospect theory and risk-awareness to protect UAV-assisted network operation

Panagiotis Vamvakas[1], Eirini Eleni Tsiropoulou[2*] and Symeon Papavassiliou[1]

Abstract

In this paper, a novel resource management framework is introduced and exploited to ensure the efficient and smooth operation of a wireless network, assisted by an unmanned aerial vehicle (UAV), operating under the non-orthogonal multiple access (NOMA) scheme and consisting of both normal and malicious risk-aware users. User devices are assumed capable of splitting their transmission power in two different communication alternatives, established via either the UAV or the macro base station (MBS). The bandwidth offered by the UAV is accessible by everyone, delivers potentially higher rate of return taking into account the enhanced communication channel gains owing to its proximity to the serving users, but is prone to failure due to its potential over-exploitation. Accordingly, the UAV's bandwidth is considered as common pool of resources (CPR). In contrast, the MBS's bandwidth is considered as a safe resource offering to the users a more limited but guaranteed level of service, due to the fact that though it has less available bandwidth it operates under a more controlled access scheme. The theory of the tragedy of the commons is used to capture the probability of failure of the CPR, while the prospect theory is adopted to study the normal and malicious users' risk-aware behavior in the UAV-assisted network. A non-cooperative power control game among the users is formulated and solved, in order to determine the users' power investment to the dual communication environment. The existence and uniqueness of a Pure Nash Equilibrium point is shown and a distributed algorithm is introduced to converge to the PNE point. This overall resource allocation framework is intelligently exploited as the vehicle to detect malicious user behavior and therefore protect the network from the undesired effects of such behaviors. The performance and inherent attributes of the proposed user-centric risk-aware operation framework, in terms of its capability to effectively utilize the available system and user resources (i.e., bandwidth and power), while succeeding in identifying potential abnormal or malicious user behaviors is assessed via modeling and simulation, under different operation scenarios.

Keywords: Risk-awareness, Malicious users, Behavioral modeling, NOMA, Wireless network, Resource management, Game theory, Intrusin detection

1 Introduction

Unmanned aerial vehicles (UAVs) have gained increasing research and commercial popularity due to their salient attributes, such as flexible and effortless deployment, mobility, strong line-of-sight (LoS) connection links, adaptive altitude, low-cost, adjustable usage, maneuverability, and hovering ability [1, 2]. Emphasizing on the usage of UAVs for wireless communications over existing network infrastructure, their main benefits, and advantages include cost-effective compared to a fixed ground base stations' deployment, swift and easy deployment, maneuverability to improve the signal reception, extended coverage, enhanced connectivity, improved performance, massive data transmission, etc. [3]. Many key industrial vendors have invested on deploying UAVs to improve the wireless connectivity, especially in disaster struck areas after a natural disaster has occurred. Indicative examples include Facebook's Aquila UAV project [4] and Google's

*Correspondence: eirini@unm.edu
[2]Department of Electrical and Computer Engineering, University of New Mexico, NM 87131 Albuquerque, USA
Full list of author information is available at the end of the article

Project Loon, where the latter has deployed UAVs in a disaster response scenario in Puerto Rico [5]. This new reality motivates and demands the examination of the major challenging research problems of resource management and security in UAV-assisted wireless networks due to the critical missions that the UAVs support.

1.1 Related work and motivation

Efficient resource management in UAV-assisted wireless networks affects various network performance metrics, such as connectivity, energy saving, throughput, coverage, and revenue. In [6], the authors formulate and solve a non-convex joint optimization problem towards determining the users' optimal transmission power, achievable data rate, the optimal position of the UAV, and the optimal bandwidth usage. In this research work, the UAV acts as a relay, enabling the communication of the users with the macro base station (MBS). In [7], a coalition formation mechanism among the users based on reinforcement learning is proposed, and the optimal UAV's position, energy harvesting levels of the users from the UAV, and the users' optimal transmission power is determined following a game-theoretic approach. In [8], a non-orthogonal multiple access (NOMA)-based UAV-assisted wireless network is examined by formulating a centralized resource allocation problem towards maximizing the overall users' throughput.

The theory of minority games is used in [9] to create clusters among the users based on their physical characteristics (energy availability, communication distance from the UAV) and determine their optimal transmission power to communicate with the UAV. In [10], the authors exploit the UAV wireless system's physical characteristics, i.e., UAV's maximum speed constraint and the users' energy availability, towards maximizing the minimum uplink throughput of all the users during an examined period of the UAV's flight. A non-cooperative power control problem is formulated in [11] to determine the users' optimal transmission power to the UAV in a distributed manner. In this model, the users create coalitions among each other by exploiting their socio-physical characteristics and following the Chinese Restaurant Process.

Moreover, the authors in [12] introduce a risk-aware resource management problem considering a static and a mobile UAV serving the ground users, and accordingly they determine the optimal power transmission of each user via a game-theoretic approach, in order to communicate with the two available receivers. This work is further extended in [13] towards determining the users' optimal transmission power in order to communicate with the macro base station or the flying UAV, following a risk-aware analysis, where risk stems from the incomplete available information in the users' decision-making process. Both these works provide some insight about the potential and benefit of introducing the concept of user risk-based behavior in the operation of public safety networks; however, they do not treat or consider the impact of the existence of malicious users. The authors in [14] focus on the application of structural inspection services assisted by the UAVs and they propose an algorithm to enable the unmanned aerial system to provide uninterrupted services considering the feasible flying time of the UAVs. In [15], the open challenges regarding the resource management problem in the UAV-assisted public safety systems are presented. Moreover, in [16] a zero-sum network interdiction game is formulated between a vendor, operating a drone delivery system, and a malicious attacker in order to study the cyber-physical security challenges in drone delivery systems. This work has been further extended in [17] to study the cyber-physical security challenges of time-critical UAV applications.

Additional research efforts have been devoted to the problem of UAV positioning to improve the resource management process. In [18], the problem of optimal placement of a single UAV in the presence of device-to-device (D2D) underlaid links is examined. This problem is extended in [19] to the multi-UAV optimal placement to support the data aggregation in an Internet of Things (IoT) setting. Also, the problem of UAV optimal positioning for system's throughput optimization is studied in [20], where a heuristic and an approximation method have been proposed.

Although great research efforts have been devoted to the resource management problems in UAV-assisted wireless networks, the problem of detecting attacks in UAV-based communication networks has not been well addressed in the literature. UAVs are vulnerable to attacks, as they are highly exposed technical systems, while gaining illegitimate entry into the UAVs' operation and network can cause an enormous amount of losses regarding data confidentiality, money, and reputation. Wireless attacks are the most common form of UAVs' hacking, such as password theft, Wireshark, Global Positioning System (GPS) spoofing, man-in-the-middle attacks, Trojan horse viruses, and distributed denial of service (DDoS) attacks [21]. A very well-known GPS spoofing example (however, the legitimacy of this attack has not been confirmed) occurred in 2011, when an Iranian engineer reported that they have spoofed false GPS coordinates to an US UAV, and they guided it to land safely on an Iranian airfield [22]. Examples and events like that raise concerns regarding the state of UAV-based communication security. Some indicative mechanisms in order to detect and/or defend against the hacking of the UAVs are: encryption and cryptography, anomaly detection, defense techniques against DDoS attacks, and the development of intrusion detection and intrusion ejection systems [23].

In [24], a risk assessment scheme for UAVs is developed based on the UAVs' provided services, equipped communication infrastructures and sensor systems, as well as the existing UAVs' fault handling mechanisms. In [25], the authors discuss the security and privacy challenges of the UAVs' systems and networks. In [26], the Bayesian game theory is adopted to design an intrusion detection system for monitoring the network and an intrusion ejection system for excluding the malicious nodes that are anticipated to instigate an attack is presented. In [27], the authors proposed a differential game-theoretic approach to determine the optimal strategies of multiple UAVs evading the attack of an aerial jammer on the communication channel. In [28], an intrusion detection and response scheme is implemented focusing on the most lethal cyber-attacks (i.e., false information dissemination, GPS spoofing, jamming, and black and gray hole attacks) and identifying the UAVs' behavior as normal, abnormal, suspect, or malicious. In [29], the authors introduce a prototype UAV monitoring system that captures UAVs' flight data and it detects anomalies by performing real-time behavioral modeling. A survey summarizing the state-of-the-art intrusion detection systems which identify attacks under networked UAV environments is presented in [30], while in [31], a survey of the game-theoretic approaches that study UAV-assisted wireless communication network security is introduced.

1.2 Contributions

One important observation however is that the aforementioned related literature examines the resource management and security aspects of the UAV-assisted wireless networks, assuming that all the users have rational characteristics and aim at maximizing their perceived utility, i.e., benefit from communicating with the UAV, regardless if they are normal or malicious users. Nevertheless, in real-life networking scenarios, the users demonstrate a risk-aware behavior, which is driven by their personal characteristics, the actions and behavior of the other users, and the conditions in the UAV-assisted network.

Our paper aims at exactly filling this gap by exploring user behavioral insights and incorporating behavioral factors into modeling normal and malicious users' decisions. The latter consideration enables to determine the users' optimal transmission power allocation in the two available communication alternatives, that is UAV-based and MBS-based communication, towards improving its utility, while capitalizing on this to devise a sophisticated intrusion detection and ejection process. Towards capturing normal and malicious users' behavior in a more pragmatic manner, prospect theory (PT) is adopted [32, 33]. Prospect theory, introduced by Kahneman and Tversky [34], has emerged as a dominant behavioral model in formulating decision making under probabilistic uncertainty. Prospect theory succeeds in integrating user subjectivity in decisions, illustrated by an S-shaped utility function capturing user preferences tending to overweight the probability of losses and underweight the probability of gains.

The users are assumed capable of communicating simultaneously with the UAV and the macro base station, by appropriately investing their uplink transmission power per each communication link. The above framework is facilitated by the multi mode/access capable advanced devices which have already become available in the market in recent years [35, 36] which can opportunistically access and utilize the bandwidth resources even from distinct cells or providers. Such a multi-communication interface environment immensely modifies the flexibility enjoyed by the users who are not restricted in selecting only one receiver but can proportionally split their invested transmission power to multiple ones. The UAV is allocated a greater portion of bandwidth compared to the MBS, as it is typically offered to all users (e.g., by a smart city possibly on a free access mode), resides closer to them (compared to the MBS) and thus can serve them more efficiently. Consequently, the users may achieve higher data rates with lower transmission power. Therefore, the available bandwidth in the UAV-based communication is considered as a *common pool of resources (CPR)*, since it is non-excludable (i.e., it is accessible by all users), rivalrous, and subtractable. However, the potential over-exploitation of the CPR would conclude to the failure of the UAV's bandwidth, as due to the increased interference at the receiver, i.e., UAV, none of the users will be eventually satisfied. This observation is motivated by the well-known concept of the tragedy of the commons [37]. In contrast, the MBS usually resides far away from the majority of the users and higher transmission power levels are required by the users to achieve their QoS satisfaction. Thus, the MBS-based communication becomes less attractive as it results to lower energy-efficiency transmissions. Though usually a smaller portion of bandwidth is available by the MBS to support the users' communication, it offers enhanced processing capabilities while at the same time it operates under a controlled user access scheme, and therefore in our system model the MBS's available bandwidth is treated as a safe resource alternative, due to the fact that each user can obtain a guaranteed level of QoS given its personal characteristics (e.g., channel gain, transmission power).

In such a setting, a malicious user can take advantage of the vulnerability of the UAV-based communication to failure, due to the over-exploitation of the UAV's bandwidth, and thus perform a distributed denial of service (DDoS) type of attack. During the attack, the malicious users demonstrate a risk-seeking behavior and they over-invest their available transmission power to the UAV-based

communication, driving the UAV's bandwidth to failure, thus the service of the normal users is denied. We propose an intrusion detection process that considers users' behavioral characteristics and transmission power levels to identify the malicious users. Additionally, by intelligently exploiting the successive interference cancellation (SIC) technique at the UAV-receiver that characterizes the NOMA technology, we propose a novel intrusion ejection methodology.

The main contributions of this research work, as summarized as follows:

(A) We introduce a holistic approach based on the prospect theory and the theory of the tragedy of the commons, to capture and model normal and malicious users' risk-aware behavioral characteristics in representative prospect-theoretic utility functions. Specifically, novel and generic enough prospect-theoretic utility functions are introduced, which do not simply represent the trade off between the number of transmitted bits to the corresponding consumed power, but on the contrary reflect normal and malicious users' risk-aware choices and priorities in the NOMA-based UAV-assisted wireless network. The bandwidth's fragility in the UAV-based communication is examined by examining the bandwidth's exploitation by the normal users, and its over-exploitation by the malicious users (Section 2).

(B) Based on the above modeling, a user-centric power control problem is formulated as a maximization problem of each normal and malicious user's expected prospect-theoretic utility, and it is treated as a non-cooperative game among the users [38]. The goal of each user (either normal or malicious) is to accordingly determine its optimal transmission power investment in the two available communication alternatives, i.e., UAV-based and MBS-based communication. The existence and uniqueness of a pure Nash equilibrium (PNE) is shown and the convergence of the users' power strategies to the unique PNE is proven (Section 3). A distributed low-complexity algorithm that converges to the unique PNE is also devised (Section 4).

(C) Capitalizing on the proposed prospect-theoretic resource management framework, a risk-aware and transmission-based intrusion detection process is introduced. Subsequently, a novel intrusion ejection methodology is proposed based on the salient characteristics of the non-orthogonal multiple access (NOMA) technology and the successive interference cancellation (SIC) technique (Section 5).

(D) A series of detailed simulation experiments are performed to evaluate the performance and inherent attributed of the proposed user-centric risk-aware operation framework, in terms of its capability to effectively utilize the available system and user resources (i.e., bandwidth and power), while succeeding in identifying potential abnormal or malicious user behaviors. The evaluation metrics refer to the users' transmission power investment, achievable data rate, fragility of the UAV's available bandwidth due to malicious attacks, and impact of users' risk-aware and malicious behavior on the system's operation (Section 6).

Finally, Section 7 concludes the paper.

2 UAV-assisted wireless network: operation overview and model

2.1 System model and the tragedy of the commons

We study the uplink communication of a UAV-assisted wireless network consisting of $|N_N|$ normal users and $|N_M|$ malicious users, where their corresponding sets are $N_N = \{1, \ldots, i, \ldots, |N_N|\}$ and $N_M = \{1, \ldots, i, \ldots, |N_M|\}$, respectively, and $N = N_N \cup N_M$. Each user $i, i \in N$ exploits both the MBS and UAV connectivity, while exhibiting risk-aware behavior. The UAV-based communication is characterized by greater portion of available bandwidth compared to the MBS-based communication. Due to the UAV's proximity to the users and respectively improved channel gain, the users tend to communicate over the UAV in order to achieve higher data rates, while transmitting at low power levels, thus, extending their battery life. However, the UAV has an upper limit capacity in terms of available bandwidth. Thus, if an increased number of users transmit over the UAV, its corresponding bandwidth becomes over-exploited, and consequently the UAV presents an increased probability of failure in serving the users, primarily due to the increased levels of interference at the reception of the users' signals. Based on this observation, the bandwidth that is available in the UAV-based communication is considered as a CPR, and its over-exploitation and probability of failure is captured by the theory of the tragedy of the commons [37]. On the other hand, the bandwidth that is available at the MBS-based communication is considered as a safe resource, and the user may achieve a more limited but guaranteed level of QoS given its personal characteristics, i.e., channel conditions, transmission power.

It should be also noted here that in this paper we assume that the UAV is provided with sufficient power supply to support the UAV-based communication network within the considered time window of operation. Given that in practice however, the UAV has limited power supply, its battery should be recharged in order to enable the continuous operation of the UAV-based communication network. Nowadays, there have been deployed several types of UAVs that are characterized by long flight endurance, such as the Boeing Insitu ScanEagle with flight endurance over 20 h [39] and Aerovel Flexrotor with

flight endurance of more than 30 h [40]. Also, several techniques to recharge the UAVs on the fly have been already proposed by complementing the on-board battery source of the UAV using advanced thin-film photovoltaic cells made of copper-indium-gallium di-selenide semiconductor materials [41]. Additionally, optimal flight path planning techniques have been proposed where the UAV determines a priori the optimal flight path taking into account the recharging stations located on or near the flight path [42].

Considering the described dual communication environment, each user i, has a maximum transmission power P_i^{Max}, which it invests to both the UAV-based and MBS-based communication to satisfy its goals (i.e., QoS prerequisites if a normal user, or its negative impact if a malicious user). Given the complexity of the dual UAV/MBS communication environment, a centralized resource management approach would introduce increased signaling overhead and would require a centralized entity to obtain and maintain a global view and control of the communication system. Thus, a distributed resource management approach is followed in this paper enabling both the normal and malicious users to determine in an autonomous manner their transmission power investment to the UAV-based communication P_i^{UAV} and to the MBS-based communication $P_i^{\text{MBS}}, \forall i \in N = N_N \cup N_M$. The percentage of normal and malicious user's i power investment to its transmission to the UAV is assumed to be $x_i, x_i \in [0,1]$, thus, $P_i^{\text{UAV}} = x_i P_i^{\text{Max}}$, and accordingly, $P_i^{\text{MBS}} = (1-x_i)P_i^{\text{Max}}$.

Given the considered communication environment, the malicious users perform a distributed denial of service (DDoS) attack by simply investing high transmission power levels to their UAV-based communication, thus, over-exploiting the UAV's available bandwidth and introducing high levels of interference to the reception of the normal users' signals at the UAV. The outcome of the malicious users' attack is the failure of the UAV's available bandwidth to serve the normal users. A conceptual illustration of the structure of a dual communication environment with both an MBS and a UAV, as well as normal and malicious users, is shown in Fig. 1.

2.2 Utility functions of risk-aware users based on prospect theory

In the examined UAV-assisted wireless network, the normal and malicious users exhibit risk-aware behavior regarding their decisions of investing their transmission power to the UAV-based and MBS-based communication. The users' risk-aware behavior in terms of their decision-making stems from the fact that the individuals assess uncertain outcomes under a loss averse attitude (instead of neutral) in real-life communication environments. Thus, the users' utility (i.e., perceived satisfaction) in the event of a loss (i.e., UAV's bandwidth failure) is served as of greater magnitude compared to the gains of equal extent given a reference point. This reference point is considered as the ground truth of user perceived utility scale, and it is not necessarily common for all the users. Furthermore, the users tend to overweight events, e.g., UAV's bandwidth failure, with small probabilities, and underweight events with higher probabilities, thus, instructing the formulation of the utility function following the probability weighting effect. These principles of describing the risk-aware behavior of the users in the UAV-assisted wireless network are provided by the prospect theory [34]. Accordingly, the users' cognitive risk-aware behavior is transformed in representative prospect-theoretic utility functions as follows:

$$\mathcal{V}_i(y_i) = \begin{cases} (y_i - y_{0,i})^{a_i} & , if\ y_i > y_{0,i} \\ -\kappa_i (y_{0,i} - y_i)^{\delta_i} & , \text{otherwise} \end{cases} \quad (1)$$

where $y_i(x_i, x_T)$ is the user's $i, i \in N = N_N \cup N_M$ actual utility, $x_T = \sum_{i=1}^{|N|} x_i$ denotes the total power investment

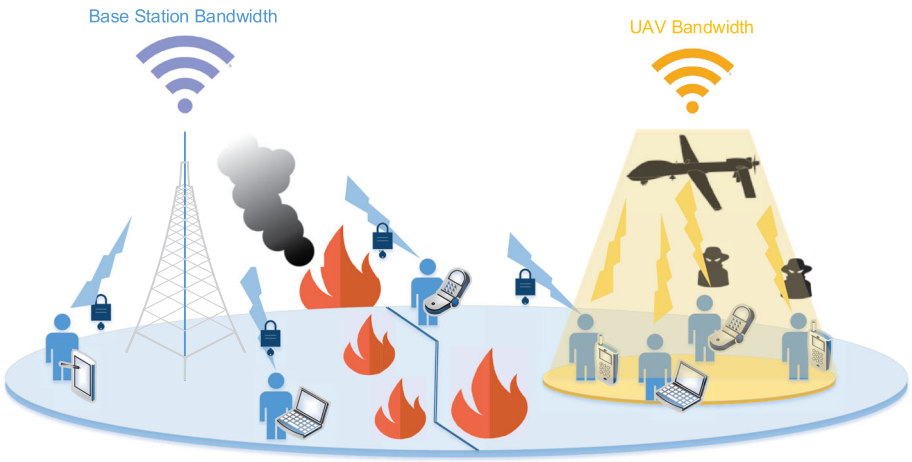

Fig. 1 UAV-assisted wireless network consisting of risk-aware users

of all users to the UAV-based communication, $|N| = |N_N| + |N_M|$ is the total number of users in the examined network including both the normal and the malicious users, and $y_{0,i}$ the reference point. The reference point is defined as the corresponding user's achieved energy-efficiency point, if the user was exploiting only the safe resource, i.e., if it was transmitting its data only to the MBS by solely investing all of its transmission power to the MBS-based communication [43]. Thus, the reference point is given as follows:

$$y_{0,i} \triangleq \frac{W_{\mathrm{MBS}}/N_{\mathrm{MBS}}}{P_i^{\mathrm{MBS}}} \log_2\left(1+\gamma_i^{\mathrm{MBS}}\right), \forall i \in N \tag{2}$$

where W_{MBS} is the available bandwidth at the MBS-based communication, N_{MBS} is the number of normal and malicious users transmitting to the MBS, $P_i^{\mathrm{MBS}} = P_i^{\mathrm{Max}}$ presents the user's transmission power (if the user was solely investing its available power to the MBS-based communication), and γ_i^{MBS} denotes the signal to interference plus noise ratio (SINR), as measured at the MBS receiver, given as follows:

$$\gamma_i^{\mathrm{MBS}} = \frac{h_i^{\mathrm{MBS}} P_i^{\mathrm{MBS}}}{\sum_{j>i} h_j^{\mathrm{MBS/UAV}} P_j^{\mathrm{MBS/UAV}} + \sigma^2} \tag{3}$$

where h_i^{MBS} is the user's communication channel gain to the MBS, and the interference sensed by user i during its transmission considering the NOMA technology is $\sum_{j>i} h_j^{\mathrm{MBS/UAV}} P_j^{\mathrm{MBS/UAV}}$, and σ^2 is the variance of the noise power. The communication system of the examined UAV-assisted wireless network is assumed to operate under the NOMA technology that utilizes the successive interference cancellation (SIC) technique at the receiver, which decodes first the signals from the users with better channel gains. Assuming, without loss of generality, that the channel gains pertaining to user i are sorted, then the SIC technique first decodes the signals received from the best channel. Thus, the users with better channel gains experience interference from users with worse channel conditions, while the transmissions of lower channel gain users receive less interference by removing the already decoded signals [44].

Given the definition of the reference point in Eq. 2 and the users' prospect-theoretic utility function as introduced in Eq. 1, it is concluded that the users' perceived satisfaction (Eq. 1) is determined with respect to the reference point (Eq. 2), which acts as the ground truth of the user's actual utility $y_i(x_i, x_T)$. The users' risk-aware behavior is further captured by the personalized parameters $\alpha_i, \delta_i, \kappa_i, i \in N = N_N \cup N_M$. Specifically, the risk-seeking behavior of a normal or malicious user in losses and its risk averse behavior in gains is reflected by small values of the parameter $\alpha_i, \alpha_i \in (0, 1]$. Furthermore, small values of parameter $\delta_i, \delta_i \in (0, 1]$ imply higher decrease of user's prospect-theoretic utility for small values of y_i and close to the reference point $y_{0,i}$. Without loss of generality, we assume $\alpha_i = \delta_i$. Additionally, the loss aversion parameter $\kappa_i, \kappa_i \in [0, +\infty)$ reflects the impact of losses compared to gains on user's prospect-theoretic utility. If $\kappa_i > 1$, the user i weighs the losses more than the gains, while if $0 \leq \kappa_i \leq 1$, the user weighs more or equal the gains than the losses, thus presenting an aggressive gain seeking behavior.

At this point, we would like to provide some insight about the physical meaning of the prospect-theoretic utility, as defined in Eq. 1. The fundamental principle of prospect theory is that a user will receive greater dissatisfaction from the loss of $y_i(x_i, x_T)$ amount of actual utility compared to the pleasure that it will enjoy by gaining the same amount. This concept represents the users' loss aversion behavior in realistic dynamic interdependent environments. The user's loss aversion behavior is mathematically expressed via the asymmetry in the slope of the prospect-theoretic utility function around the reference point, as presented in Fig. 2. It should be also highlighted that prospect theory has already been applied in diverse scientific and research fields involving decision-making under uncertainty, e.g., finance, insurance, labor markets, and crowd sourcing. Furthermore, prospect theory has been applied in several cases of the broader networking and communication era, such as smart grid networks [45], communications systems [46], and transportation networks, [47, 48]. In a nutshell, prospect theory has been widely established as a powerful tool to model humans' behavior and decision-making under risk and uncertainty.

Based on Eqs. 1 and 2, it is noted that the user's prospect-theoretic utility is expressed in terms of achieved energy-efficiency. Taken into account that the normal and malicious users exploit the dual communication

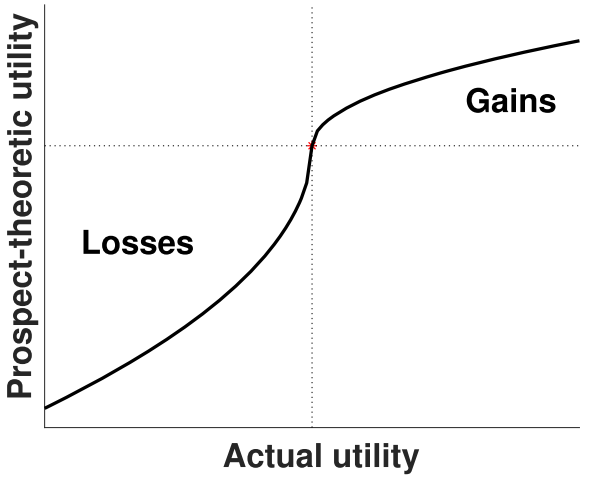

Fig. 2 Prospect-theoretic utility

environment consisting of the MBS and UAV receivers, their perceived actual utility $y_i(x_i, x_T)$ is expressed as the summation of the perceived satisfaction by the MBS-based communication, i.e., first term of Eq. 4, and the corresponding satisfaction by the UAV-based communication, i.e., second term of Eq. 4. Therefore, the user's actual utility is defined as follows:

$$y_i(x_i, x_T) = y_{0,i}(1 - x_i) + \mathscr{E}_i x_i \mathscr{R}(x_T) \tag{4}$$

where $\mathscr{E}_i$ is the achieved energy-efficiency by the UAV-based communication and is defined as follows:

$$\mathscr{E}_i = \frac{W_{\text{UAV}}/N_{\text{UAV}}}{P_i^{\text{UAV}}} log_2\left(1 + \gamma_i^{\text{UAV}}\right) \tag{5}$$

where W_{UAV} is the UAV's bandwidth, N_{UAV} is the number of normal and malicious users transmitting to the UAV, and γ_i^{UAV} is the SINR of user i as measured at the UAV receiver and is given as follows.

$$\gamma_i^{\text{UAV}} = \frac{h_i^{\text{UAV}} P_i^{\text{UAV}}}{\sigma^2 + \sum_{j>i} h_j^{\text{MBS/UAV}} P_k^{\text{MBS/UAV}}} \tag{6}$$

where h_i^{UAV} is the channel gain of user i communicating with the UAV. The function $\mathscr{R}(x_T)$ in Eq. 4 represents the rate of return of the UAV-based communication to the normal and malicious users, which is a decreasing concave function with respect to $x_T = \sum_{i=1}^{|N|} x_i$, as the more the users exploit the UAV's available bandwidth, the less the UAV is able to meet the users' QoS prerequisites. For demonstration purposes, in this work the rate of return $\mathscr{R}(x_T)$ of the CPR is formulated as follows.

$$\mathscr{R}(x_T) = 2 - e^{x_T - 1} \tag{7}$$

As discussed above, the UAV's bandwidth may fail to address all the normal and malicious users' service requests. Thus, the UAV's bandwidth, acting as a CPR, has a probability of failure $\mathscr{P}(x_T)$ (CPR's fragility) to serve the users who transmit to the UAV, which is increasing with respect to users' aggregate power investment x_T. In the following, we consider $\mathscr{P}(x_T) = x_T^2$ while x_T is considered normalized. At this point, it is highlighted that the malicious users have the intention to over-invest their transmission power to the UAV-based communication via performing a DDoS attack in order to drive the UAV's bandwidth to failure, thus, none of the normal users would enjoy the UAV's services.

If the CPR does not fail due to the over-exploitation and the transmission power over-investment by the users, then each user perceives an actual utility given by Eq. 4. In this case, the actual perceived utility is greater than the reference point $y_{0,i}$, i.e., $y_i > y_{0,i}$. Therefore, via subtracting the reference point (Eq. 2) from the actual utility (Eq. 4), and shaping the result according to the first branch of Eq. 1, we have

$$\mathscr{V}_i(x_i) = x_i^{a_i}\left[\mathscr{E}_i \mathscr{R}(x_T) - y_{0,i}\right]^{a_i} \tag{8}$$

For the simplicity of the notation, we normalize the rate of return function, so that $y_{0,i} = 1$ and denote $\overline{\mathscr{R}_i}(x_T) \triangleq (\mathscr{E}_i \mathscr{R}(x_T) - 1)^{a_i}$, where $\overline{\mathscr{R}_i}(x_T)$ is concave, decreasing, twice continuously differentiable, and positive. Thus, $\mathscr{V}_i(x_i) = x_i^{a_i}\overline{\mathscr{R}_i}(x_T)$. In the opposite case, where the CPR becomes over-exploited and fails to serve the normal and the malicious users' service requests, then no user receives any satisfaction from its transmission to the UAV. Therefore, the rate of return from the UAV is extremely small, and the second term of Eq. 4 is 0, while the user perceives satisfaction only by its transmission to the MBS, i.e., first term of Eq. 4. In this case, the actual utility is $y_i \leq y_{0,i}$, thus, by subtracting the actual utility from the reference point and reshaping the result based on the second branch of Eq. 1, we have $\mathscr{V}_i(x_i) = -\kappa_i x_i^{\alpha_i}$.

Following the above detailed argumentation, we can rewrite the normal and malicious user's prospect-theoretic utility function as follows.

$$\mathscr{V}_i(x_i) = \begin{cases} x_i^{a_i}\overline{\mathscr{R}_i}(x_T) & , if\ y_i > y_{0,i} \\ -\kappa_i x_i^{a_i} & , \text{otherwise} \end{cases} \tag{9}$$

The UAV's bandwidth (CPR) probability of failure is $\mathscr{P}(x_T)$, thus, the probability that the CPR survives and serves the users' service requests is $(1 - \mathscr{P}(x_T))$. As a result, considering the UAV's bandwidth probability of failure, Eq. 9 can be written equivalently as follows.

$$\mathscr{V}_i(x_i) = \begin{cases} x_i^{a_i}\overline{\mathscr{R}_i}(x_T), & \text{with prob. } (1 - \mathscr{P}(x_T)) \\ -\kappa_i x_i^{a_i}, & \text{with prob. } \mathscr{P}(x_T) \end{cases} \tag{10}$$

For convenience, all key involved notations are summarized in Table 1.

3 Fragile CPR games

3.1 Problem formulation

Given the above modeling, the normal users empowered by prospect theory are able to sense the increasing probability of UAV's bandwidth collapse in the incident of a DDoS attack. Towards safeguarding their transmission in uncertain conditions prevailing within the UAV network, normal users aim to maximize their expected prospect-theoretic utilities, defined below:

$$\mathbf{E}(\mathscr{V}_i) = \begin{cases} x_i^{a_i}\overline{\mathscr{R}_i}(x_T)\,(1 - \mathscr{P}(x_T)) - \kappa_i x_i^{a_i}\,\mathscr{P}(x_T) \\ \text{for normal users, } i \in N_N \\ x_i^{\beta_i}\overline{\mathscr{R}_i}(x_T)\,(1 - \mathscr{P}(x_T)) - \lambda_i x_i^{\beta_i}\,\mathscr{P}(x_T) \\ \text{for malicious users, } i \in N_M \end{cases} \tag{11}$$

where a_i, κ_i and β_i, λ_i are the personalized risk-aware parameters following the principles of prospect theory, as defined in Section 2.2, for the normal and malicious users. For notational convenience, we define

Table 1 List of parameters

Symbol	Description
$\Re$	Network radius [m]
N, $\|N\|$	Set of all users, cardinality of the set
x_i	User specific investment to UAV (%)
N_{UAV}	Users transmitting via the UAV
N_{MBS}	Users transmitting via the MBS
N_N, $\|N_N\|$	Set of normal users, cardinality of the set
N_M, $\|N_M\|$	Set of malicious users, cardinality of the set
W_{MBS}	MBS bandwidth [Hz]
W_{UAV}	UAV bandwidth [Hz]
γ_i	Signal to Interference plus noise ratio
P_i^{MBS}	Transmission power via MBS [W]
P_i^{UAV}	Transmission power via UAV [W]
x_T	Aggregate users investment to UAV-based communication
h_i	Channel gain
$\mathscr{R}(x_T)$	Rate of return function
$\overline{\mathscr{R}_i}(x_T)$	PT related rate of return
$\mathscr{P}(x_T)$	UAV's bandwidth probability of failure
a_i, β_i	Sensitivity parameters
κ_i, λ_i	Risk aversion parameters
$\mathscr{F}_i(x_T)$	Effective rate of return
$\mathscr{J}(x_T)$	User specific optimal non zero investment
R_i	User data rate [bps]
$\mathscr{B}_i(\mathbf{x_{-i}})$	User best response
$\mathscr{X}_i$	User power investment strategy set

$\mathscr{F}_i(x_T) = \overline{\mathscr{R}_i}(x_T)\,(1 - \mathscr{P}(x_T)) - \kappa_i \mathscr{P}(x_T)$ and $\mathscr{F}'_i(x_T) = \overline{\mathscr{R}_i}(x_T)\,(1 - \mathscr{P}(x_T)) - \lambda_i \mathscr{P}(x_T)$ as each normal and malicious user's effective rate of return, respectively. Thus, the expected prospect-theoretic utility can be re-written as follows:

$$\mathbf{E}(\mathscr{V}_i) = \begin{cases} {x_i}^{a_i} \mathscr{F}_i(x_T) & \text{for normal users, } i \in N_N \\ {x_i}^{\beta_i} \mathscr{F}'_i(x_T) & \text{for malicious users, } i \in N_M \end{cases} \tag{12}$$

Fragile common pool resource (CPR) games have emerged as a convenient class of games capturing investment in both safe and fragile resources, with the latter prone to collapse if over-exploited. Users have an initial endowment enabling them to invest by splitting it to each resource (i.e., power investment to allocate their transmission power to the MBS and the UAV). A fundamental characteristic of fragile CPR games is incorporating the probabilistic resource failure of the CPR (i.e., UAV's bandwidth) if the aggregate user investment surpassed system's capacity to address demand.

A fragile CPR game is assumed to satisfy the following properties:

- The probability of failure $\mathscr{P}(x_T)$ is a convex, strictly increasing, and twice differentiable function of the normalized total investment $x_T = [0, 1)$ and $\mathscr{P}(1) = 1$.
- The rate of return $\overline{\mathscr{R}_i}(x_T)$ in Eq. 7 is monotonic decreasing, i.e., $\frac{\partial \overline{\mathscr{R}_i}(x_T)}{\partial x_T} < 0$, concave $\left(\frac{\partial^2 \overline{\mathscr{R}_i}(x_T)}{\partial x_T^2} < 0\right)$, twice continuously differentiable, and positive $\forall x_T \in [0, 1]$.
- The strategy set of each user i is defined as $\mathscr{X}_i = [0, 1], \forall i \in N$.

Stemming from the ability of fragile CPR games to reflect how rivalrous and non excludable resources can be allocated among competing users, in this work we denote $\mathscr{G} = [N, \{\mathscr{X}_i\}_{i \in N}, \{\mathscr{V}_i\}_{i \in N}]$ as the corresponding security aware power investment for efficient network spectrum sharing (SAPIENSS) game in UAV-assisted communication networks under DDoS attack, where as mentioned before N denotes the index set of both normal and malicious users.

Each of the normal users aims at the maximization of its expected prospect-theoretic utility jointly targeting for the optimal allocation of its power investment across the MBS and the UAV, while at the same time adjusting its band preference based on the probability of failure of the UAV's available bandwidth. Thus, the corresponding optimization problem is formulated as the maximization of each normal user's expected prospect-theoretic utility, as follows:

$$\begin{aligned} \max \mathbf{E}(\mathscr{V}_i) = \max \left\{ x_i^{a_i} \mathscr{F}_i(x_T) \right\}, \ \forall i \in N_N \\ s.t.\ x_i \in [0, 1] \end{aligned} \tag{13}$$

On the other hand, malicious users follow a different prospect-theoretic behavior through the sensitivity and risk aversion parameters, with their expected prospect-theoretic utility maximization model as follows:

$$\begin{aligned} \max \mathbf{E}(\mathscr{V}_i) = \max \left\{ x_i^{\beta_i} \mathscr{F}'_i(x_T) \right\}, \ \forall i \in N_M \\ s.t.\ x_i \in [0, 1] \end{aligned} \tag{14}$$

The solution of the SAPIENSS game $\mathscr{G}$ determines a pure Nash equilibrium (PNE), where both the normal and the malicious users have determined their power investment to the MBS-based and UAV-based communication, while each user type aims at achieving its own personal goals, i.e., satisfy their QoS prerequisites for the normal users and deny the service of the normal users by the malicious users who over-invest their transmission power to the UAV-based communication.

For the examined game $\mathscr{G}$, PNE is a stable power investment vector $\mathbf{x}^* = \{x_i^*\}$ where no user can witness an improved utility from its transmission, i.e., $\mathscr{V}_i\left(x_i{}^*, \mathbf{x}^*_{-i}\right) \geq \mathscr{V}_i(x_i, \mathbf{x}^*_{-i})$, $\forall x_i \in \mathscr{X}_i$. On the other hand, the inability of the game to converge to a PNE would suggest an unstable

state for the network which would be associated to the collapse of the UAV's bandwidth with no normal user being able to transmit properly via the UAV network, since only the users who invested in communicating with the MBS will be able to transmit, however at the expense of very low returns (i.e., low data rates and inferior channel gains) in comparison to the UAV-based communication.

Let $\mathscr{B}_i$ be the best response correspondence of each user $i, i \in N$ where $\mathscr{B}_i(\mathbf{x_{-i}}) = argmax\mathbf{E}(\mathscr{V}_i(x_i, \mathbf{x_{-i}}))$, $\mathscr{B}_i : \overline{\mathscr{X}}_{-i} \rightrightarrows \mathscr{X}_i$, where $\overline{\mathscr{X}}_{-i}$ represents the aggregate investment from all users (both normal and malicious users), excluding user i. User's selected strategy for its joint transmission via both the MBS and the UAV is reflected through its best response, where a value $\mathscr{B}_i(\mathbf{x_{-i}}) = 0$ would imply that the user did not invest in communicating with the UAV and opted to transmit only with the MBS preferring to minimize any risks by utilizing only the safe resource. On the other hand, the case where a user opts to communicate only through the UAV-based communication without considering the fragility of the resource, mirrors a malicious user's desire to claim more aggressively the bandwidth from the UAV due to its favorable channel conditions compared to the MBS and thus perform a DDoS attack. This increased power investment of the malicious users to the UAV-based communication will lead to the UAV's bandwidth collapse with certainty due to excessive aggregate demand compared to its overall capacity. Thus, the users that exhibit abnormally aggressive behavior towards claiming data rate from the UAV can reveal malicious user actions aiming to disrupt UAV network's operation, an incident which can be of high criticality, especially in events where public safety is jeopardized, e.g., public safety networks (PSNs).

3.2 Solution

In this section, we examine the existence and uniqueness of a PNE point for the SAPIENSS game $\mathscr{G}$. Without loss of generality and for simplicity of the proof, we assume $a_i = \beta_i, \kappa_i = \lambda_i$, and $\mathscr{F}_i = \mathscr{F}_i'$.

Theorem 1 *The effective rate of return $\mathscr{F}_i$ function is decreasing, concave and positive in the modified strategy space $\mathscr{X}_i'$, $\forall a_i < 0.5$.*

Proof We examine the behavior of $\mathscr{F}_i$, via calculating its first order derivative:

$$\frac{\partial \mathscr{F}_i(x_T)}{\partial x_i} = \frac{\partial \overline{\mathscr{R}_i}(x_T)}{\partial x_i}(1 - x_T^2) - 2x_T\overline{\mathscr{R}_i}(x_T) - 2\kappa_i x_T \tag{15}$$

Since the rate of return $\overline{\mathscr{R}_i}(x_T)$ is positive, i.e., $\overline{\mathscr{R}_i}(x_T) > 0$ and decreasing, i.e., $\frac{\partial \overline{\mathscr{R}_i}(x_T)}{\partial x_T} < 0, x_T > 0$ and $\kappa_i \geq 0$, then all factors of Eq. 15 are negative, and hence the effective rate of return $\mathscr{F}_i$ is decreasing, i.e., $\frac{\partial \mathscr{F}_i(x_T)}{\partial x_i} < 0$.

Similarly, for the second order derivative:

$$\frac{\partial^2 \mathscr{F}_i(x_T)}{\partial x_i^2} = \frac{\partial^2 \overline{\mathscr{R}_i}(x_T)}{\partial x_i^2}(1 - x_T^2) + \theta(x_T) - 2\kappa_i \tag{16}$$

where $\theta(x_T) = -4x_T\frac{\partial \overline{\mathscr{R}_i}(x_T)}{\partial x_i} - 2\overline{\mathscr{R}_i}(x_T)$. Due to the fact that $\overline{\mathscr{R}_i}(x_T)$ is concave (i.e., $\frac{\partial^2 \overline{\mathscr{R}_i}(x_T)}{\partial x_T^2} < 0$) and aggregate investment $x_T \leq 1$ since it is normalized, and by proving that $\theta(x_T) < 0$ in $\mathscr{X}_i$, $\forall a_i < 0.5$, each factor of Eq. 16 is negative. Subsequently, the effective rate of return $\mathscr{F}_i$ is also concave, thus $\frac{\partial^2 \mathscr{F}_i(x_T)}{\partial x_i^2} < 0$.

Towards examining the sign of $\mathscr{F}_i$, we apply Bolzano's Theorem within $\mathscr{X}_i = [0, 1]$ which is an important specialization of Intermediate Value Theorem [49]. We observe that $\mathscr{F}_i(0) > 0$ and $\mathscr{F}_i(1) < 0$, hence there exists a value $\zeta \in \mathscr{X}_i$, such that $\mathscr{F}_i(\zeta) = 0$. As a result, $\mathscr{F}_i$ is positive in the reduced strategy space $\mathscr{X}_i' = [0, \zeta]$, $\mathscr{X}_i' \subset \mathscr{X}_i$. □

Theorem 2 ***(Existence of PNE)*** *For the Fragile CPR SAPIENSS game $\mathscr{G}$, there exists a value $\xi \in \mathscr{X}_i'$ which is a critical point for $\mathbf{E}(\mathscr{V}_i)$.*

Proof Towards proving the existence of a PNE, we investigate the first order condition for $\mathbf{E}(\mathscr{V}_i)$, as follows.

$$\frac{\partial \mathbf{E}(\mathscr{V}_i)}{\partial x_i} = x_i^{a_i - 1}\Phi(x_i) = 0 \tag{17}$$

where $\Phi(x_i) = \left(x_i\frac{\partial \mathscr{F}_i(x_T)}{\partial x_i} + a_i\mathscr{F}_i(x_T)\right)$. Similarly to Theorem 1, we apply Bolzano's Theorem for $\frac{\partial \mathbf{E}(\mathscr{V}_i)}{\partial x_i}$ in the modified space $\mathscr{X}_i'$. For $x_i = 0$, $\Phi(0) > 0$, since $\mathscr{F}_i > 0, \in \mathscr{X}_i'$. Assuming a very small positive value $\epsilon \to 0$, $\epsilon > 0$, the same holds for $\Phi(\epsilon) > 0$ and subsequently $\frac{\partial \mathbf{E}(\mathscr{V}_i)}{\partial x_i}|_{x_i=\epsilon} > 0$. Next, for a relatively larger value ζ within $\mathscr{X}_i'$, $\frac{\partial \mathbf{E}(\mathscr{V}_i)}{\partial x_i}|_{x_i=\zeta} < 0$, since $\Phi(\zeta) < 0$ due to the fact that $\mathscr{F}_i(\zeta) = 0$ from Theorem 1 and that $\frac{\partial \mathscr{F}_i(x_T)}{\partial x_i} < 0$, since $\mathscr{F}_i$ is decreasing, then $\frac{\partial \mathbf{E}(\mathscr{V}_i)}{\partial x_i}|_{x_i=\zeta} < 0$. As a result, according to Bolzano's Theorem, due to the change in the sign of $\frac{\partial \mathbf{E}(\mathscr{V}_i)}{\partial x_i}$, there exists at least one $\xi, \xi \in \mathscr{X}_i'$ such that $\frac{\partial \mathbf{E}(\mathscr{V}_i)}{\partial x_i}|_{x_i=\xi} = 0$ and the first order condition is satisfied, indicating that ξ is a critical point of $\mathbf{E}(\mathscr{V}_i)$. □

Theorem 3 ***(Uniqueness of PNE)*** *The critical point $\xi \in \mathscr{X}_i'$ is a unique PNE for the SAPIENSS game $\mathscr{G}$.*

Proof In order to prove that the above determined critical point is a unique PNE for SAPIENSS game $\mathscr{G}$, we

examine the concavity of $\mathbf{E}(\mathscr{V}_i)$. The second order derivative of $\mathbf{E}(\mathscr{V}_i)$ is given as follows:

$$\frac{\partial^2 \mathbf{E}(\mathscr{V}_i)}{\partial x_i^2} = a_i(a_i-1){x_i}^{a_i-2}\mathscr{F}_i(x_T) + 2a_i{x_i}^{a_i-1}\frac{\partial \mathscr{F}_i(x_T)}{\partial x_i} + {x_i}^{a_i}\frac{\partial^2 \mathscr{F}_i(x_T)}{\partial x_i^2} \tag{18}$$

From Eq. 18, since we assume that $a_i < 0.5$, $x_i > 0 \in \mathscr{X}_i'$, and $\mathscr{F}_i$ is positive, decreasing and concave in $\mathscr{X}_i'$, then all terms of $\frac{\partial^2 \mathbf{E}(\mathscr{V}_i)}{\partial x_i^2}$ are negative, and $\mathbf{E}(\mathscr{V}_i)$ is concave, so that the critical point $\xi \in \mathscr{X}_i'$ is a unique global maximum and a unique PNE for SAPIENSS game $\mathscr{G}$ is identified. □

3.3 Convergence

In this section, we prove the convergence of the normal and malicious users' decisions to the above unique PNE. According to [50], concerning the class of fragile CPR games, convergence is established sufficiently via proving that users' best response dynamics $\mathscr{B}_i(\mathbf{x_{-i}})$ monotonically decrease with users' aggregate investment x_T to the CPR.

Theorem 4 *The Best Response (BR) strategies of SAPIENSS game $\mathscr{G}$ are monotonically decreasing in x_T.*

Proof Let $\mathscr{J}(x_T) = -a_i\frac{\mathscr{F}_i(x_T)}{\partial \mathscr{F}_i(x_T)/\partial x_i}$ be defined as the optimal non zero investment of each player $i, i \in N$, where $\mathscr{J}(\mathscr{B}_i(\mathbf{x_{-i}}) + \mathbf{x_{-i}}) = \mathscr{B}_i(\mathbf{x_{-i}})$, when $\mathscr{B}_i(\mathbf{x_{-i}}) > 0$. It is easily shown that $\frac{\partial \mathscr{J}(x_T)}{\partial x_i} < 0$, thus, $\mathscr{J}$ is monotonically decreasing in x_i. Let now $x_1 = \mathscr{B}_i(\mathbf{x_{-1}})$, $x_2 = \mathscr{B}_i(\mathbf{x_{-2}})$, with $\mathbf{x_{-1}}, \mathbf{x_{-2}} \in \overline{\mathscr{X}'}_{-i}$. If $\mathscr{B}_i$ is increasing, then for $x_2 > x_1$, then $\mathscr{B}_i(x_{-2}) > \mathscr{B}_i(x_{-1})$. However, since $\mathscr{J}$ is decreasing, for $x_2 > x_1$, $\mathscr{J}(\mathscr{B}_i(\mathbf{x_{-2}}) + \mathbf{x_{-2}}) = \mathscr{B}_i(x_{-2}) < \mathscr{B}_i(x_{-1}) = \mathscr{J}(\mathscr{B}_i(\mathbf{x_{-1}}) + \mathbf{x_{-1}})$, which is contradicting. Subsequently, we conclude that best response $\mathscr{B}_i$ is decreasing in x_T, and the users' strategies converge to the game's $\mathscr{G}$ unique PNE. □

4 Distributed algorithm

In this section, we present the distributed and low complexity algorithm for the practical implementation of the SAPIENSS game. The algorithm is executed in an iterative manner where the normal and malicious users configure their topological and behavioral characteristics and in each step they are allowed to adjust their transmission power levels between the MBS and the UAV towards maximizing their expected prospect-theoretic utility. The algorithm is able to identify intrusive behavior within the network by tracking abnormally high transmission power and interference with regards to the UAV-based communication (see Section 5 and numerical results in Section 6.3.2).

SAPIENSS algorithm ultimately operates under two potential outcomes: The first is the optimal power investment allocation of all users between the MBS and the UAV, reflecting a successful transmission from the normal users in the UAV network (also considering the case that defensive actions against attackers were applied). The above suggests that game's PNE was determined implying a stable outcome for the resource allocation process where no user wishes to deviate with regards to its perceived QoS satisfaction from its transmission. On the contrary, the algorithm may alternatively conclude to the failure of communication between the UAV and the normal users due to excessive investment from the users in the UAV-based communication, potentially due to malicious behavior of attackers. The system is able to track harmful user behavior during the transmission (which can also be confirmed by the prospect-theoretic modeling of the users' behavior); however, if no actions are taken or if the overall demand is significantly higher compared to the available bandwidth from the UAV, then SAPIENSS algorithm announces the cease of UAV's operations. In this case, only the users who partially transmitted via the MBS will be able to exchange information with in the overall considered communication environment.

4.1 Operation details

Users initiate their transmission with a randomly selected power investment value x_i within the physical limitations of the network, with the algorithm being able to converge to the PNE or to conclude the collapse of UAV's bandwidth due to a performed attack. Given the principles of the NOMA access technique, SIC methodology is applied based on users channel gains in the UAV network and the overall interference is calculated.

Based on the initial power investment, the normal and malicious users split their transmission among the MBS and the UAV and calculate their expected prospect-theoretic utilities accordingly. UAV is considered to be active during this stage, with the above process being iterated until system converges to stable transmission power allocation between the MBS and the UAV. In the event that malicious behavior is identified via the calculation of overall interference in the communication environment, SAPIENSS algorithm detects this status, and notifies accordingly the system administrator in case that counter defensive actions should be taken (see Section 5). If no specific actions are taken and the system fails to address the issue of excessive demand compared to the UAVs' bandwidth availability, the algorithm changes the operation status of the UAV to inactive and concludes its execution. The detailed implementation steps of SAPIENSS algorithm are summarized below.

Algorithm 1 SAPIENSS: security aware power investemnt for efficient network spectrum sharing in UAV-based communication networks

Require:

Number of users$|N_N|$; constants κ_i, a_i, λ_i, β_i; users position coordinates; W_{UAV}, W_{MBS}, $Bound_{interference}$

$ite \leftarrow 1$; $UAV_{active}^{(ite)} \leftarrow 1$; $convergence^{(ite)} \leftarrow 0$
Apply SIC for NOMA band
Assign initial random $x_i^{(ite)}$
while $convergence^{(ite)}$=0 **and** $UAV_{active}^{(ite)}$=1 **do**
  Calculate P_i^{UAV}, P_i^{MBS};
  UAV and MBS broadcast the overall interference and each user calculates its own sensed interference
  if interference> $Bound_{interference}$ **then**
    Apply defense mechanisms (Go To Step 1) or take no action*
  end if
  Calculate utility $\mathbf{E}(\mathscr{V}_i)^{(ite)}$ according to Eq. 12
  for all $x_i \in [0, 1]$ **do**
    x_i^*=$argmax_{x_i}\mathbf{E}(\mathscr{V}_i)$
    if $\mathbf{E}(\mathscr{V}_i) > \mathbf{E}(\mathscr{V}_i)^{(ite)}$ **then**
      $x_i^{(ite+1)} \leftarrow x_i^*$ **and** $\mathbf{E}(\mathscr{V}_i)^{(ite+1)} \leftarrow \mathbf{E}(\mathscr{V}_i)$
    end if
  end for
  Calculate *normalized* $x_T = \frac{\sum_1^{|N|} x_i^{(ite+1)}}{|N|}$
  if $\sum R_i^{UAV} > W_{UAV}$ **then**
    $UAV_{active}^{(ite+1)} \leftarrow 0$
  end if
  if $x_i^{(ite+1)} - x_i^{(ite)} < \epsilon$ **then**
    $convergence^{(ite+1)} \leftarrow 1$
  end if
  $ite \leftarrow ite + 1$
end while
return

User investment x_i and UAV_{active} if UAV still active

* *more details in Section 5 and 6.3.2*

SAPIENSS algorithm functions under a decentralized approach where the main decision steps affecting the transmission power (i.e., MBS or UAV) as well as the resource allocation process lie at the users' level. This decentralized execution of actions and the reduced data exchange between the users and the system administrator (e.g., only the overall interference is broadcasted by the MBS and UAV), contribute to the fast convergence of the algorithm to the PNE of the game or the identification of the UAV collapse within only a few iterations.

Moreover, the user-centric design allows users to differentiate their transmission priorities according to their QoS requirements or their behavioral modeling. Hence, the algorithm can also quickly track users who are attacking the UAV network without spending additional resources via calculating the intracell interference. The simplified arithmetic calculations and the absence of maintaining historical data minimize the computational and storage requirements as well as data overhead, reducing the complexity of the involved calculations. The algorithm was run in an Intel(R) Core(TM) i7-7500U CPU at 2.70 GHz 2.90 GHz laptop with 8.00 GB RAM, with its average run time per user being approximately 0.3 msec, a figure close to realistic timeslot duration (e.g., 0.5 ms), allowing the implementation of SAPIENSS algorithm in practical application scenarios. The aforementioned convergence of the SAPIENSS algorithm is guaranteed by the Best Response dynamics approach that is followed to determine the PNE [51]. Moreover, it should be clarified that the proposed framework and the corresponding SAPIENSS algorithm are fully distributed and each user makes an autonomous decision of its power investment to the UAV-based and the MBS-based communication. Thus, the SAPIENSS algorithm scales with respect to the number of users within the examined network, as there is no centralized decision-making entity which imposes additional signaling overhead and communication delay in the system.

5 Intrusion detection and ejection

Exploiting the SAPIENSS distributed algorithm presented is Section 4, in this section, we introduce a sophisticated joint intrusion detection and ejection process. As mentioned before, the UAV-receiver is able to measure the overall sensed interference by all the users, i.e., normal and malicious users. If the measured interference exceeds a predefined acceptable level of interference to successfully perform the decoding of the received signals, then the SAPIENSS algorithm raises an alarm flag that a failure is observed, potentially due to the presence of malicious behavior or extremely selfishly acting users, where both cases conclude to the failure of the UAV to serve the users. This mechanism consists a simple intrusion detection process that autonomously operates at the UAV's receiver without requesting any human intervention.

After detecting a potential malicious behavior, an efficient mechanism should exist to protect the UAV network from concluding to a probability of UAV's bandwidth failure close to one, thus, the UAV being unable to serve the normal users' QoS requests. Therefore, an intrusion ejection methodology is proposed to isolate the suspicious malicious user and enable the smooth operation of the UAV network. The proposed approach is based on the principles and characteristics of NOMA technology and SIC technique. It is highlighted that the SIC technique decodes first the signals of the users with better channel conditions, thus the users with worse channel conditions

are able to cancel the interference stemming from the transmissions of the users with better channel conditions. Therefore, it is evident that if the malicious users have the worse channel conditions in the wireless network, then they can cause the maximum damage. Based on this observation and exploiting the capabilities of the SIC technique, we argue that as the UAV decodes the received signals, it can identify the signal with the greater contribution to the overall sensed interference. Thus, for the specific transmitter (i.e., potential malicious user), the UAV-receiver sets a virtual malicious user's channel gain, which is close to infinity. Following this strategy, the malicious user's signal will be decoded first at the receiver, thus, based on the SIC technique, the contribution to the overall interference provided by the potential malicious user's signal is cancelled. Therefore, the transmissions and communication of the rest of the normal users in the examined UAV network are protected. Detailed numerical results showing the operation and efficiency of the proposed methodology are presented in Section 6.3.2.

6 Numerical results and discussion

6.1 Simulation scenario

In this section, we provide a series of numerical results to evaluate the operational features and the performance of the proposed SAPIENSS algorithm. For demonstration purposes, we consider a UAV-assisted wireless network supporting $|N| = 20$ continuously backlogged users, consisting of a standard MBS and a mobile UAV which hovers close to the users, both operating under the NOMA transmission technology. The MBS-based wireless network provide coverage over an area of radius $\Re = 6$ km, while the UAV covers an area of approximately 2.5 km within the network. We assume that the users are gathered around a specific area of the network with their ID denoting increasing distance from both the MBS and the UAV. The UAV positions itself closer to the users towards providing more favorable channel conditions, in comparison to the MBS which is impacted by inferior channel gains especially for the distant users. Additionally, the total available bandwidth is 4 MHz, 80% of which is offered by the UAV and the rest provided by the MBS. Given the technical and physical limitations of the system, we set the maximum feasible transmission power $P_i^{\text{Max}} = 0.2$ W, while, unless otherwise explicitly stated, the user is assumed to request services up to 256 kbps for the basic evaluation scenario. For demonstration and comparison mainly purposes, indicative numerical results for additional user service rates up to 512 kbps are presented as well.

Focusing further on the security perspective of our proposed approach, we consider operational scenarios where we assume that a number of users exhibit malicious behavior with their main objective to disrupt the function of the UAV communication part. In particular, we investigate how malicious or intrusive user behavior can be identified, as well as how the system can cope with such attacks by establishing and utilizing effective defensive mechanisms. In the examined scenarios, the malicious users abuse the UAV bandwidth by transmitting at abnormally high transmission power levels which deteriorate the quality of transmission for all other normal users especially via increasing the overall interference, while also by claiming a higher portion of the available UAV's bandwidth, implicitly restricting or limiting other users from having access to this part of the bandwidth.

In the next sections, we present different stages of the operation of the UAV-assisted wireless network starting with a baseline scenario where the system operates without any disruptions from intruders, and subsequently we examine how the system adjusts to cases of user attacks, how their behavior can be identified both from the practical and the theoretical perspective of the model as well as how the UAV network can sustain such incidents protecting the rest of the normal users with regards to ensuring reliable transmission conditions.

6.2 Normal operation

As an initial reference scenario, we consider a snapshot of the system where the UAV is positioned above a homogeneous population of users with respect to their transmission preferences and risk perceptions ($\kappa_i = 40$ and $a_i = 0.05$) with absence of malicious users. As instructed by the system model, the users are given the option to transmit via both the MBS and the UAV by determining their power investment portion x_i to the UAV, while at the same time are aware of the rising risk of the UAV's bandwidth collapse in case of excessive cumulative by all users investment. The significant portion of the bandwidth reserved by the UAV acts as an additional motive to users to communicate with the UAV, in comparison to the lower data rates which can be delivered if users select to transmit with the MBS, despite the fact that in the latter option they will receive a guaranteed QoS.

Specifically, Fig. 3 depicts user power investment x_i to the UAV bandwidth per user ID (increasing ID values correspond to increasing distance from the UAV and MBS position). We observe that due to the relatively high value of the loss aversion parameter κ_i the users are conservative enough towards transmitting via the UAV magnifying the probability of the potential risk of the collapse of its bandwidth. As a result, the maximum investment in the UAV bandwidth is below 50%, while the users also select to invest a significant portion of their transmission power to the safe communication with the MBS. Moreover, we observe that users closer to the MBS and the UAV select a very low investment to the UAV since their favorable channel conditions allow them to obtain satisfactory data rates without devoting a high portion

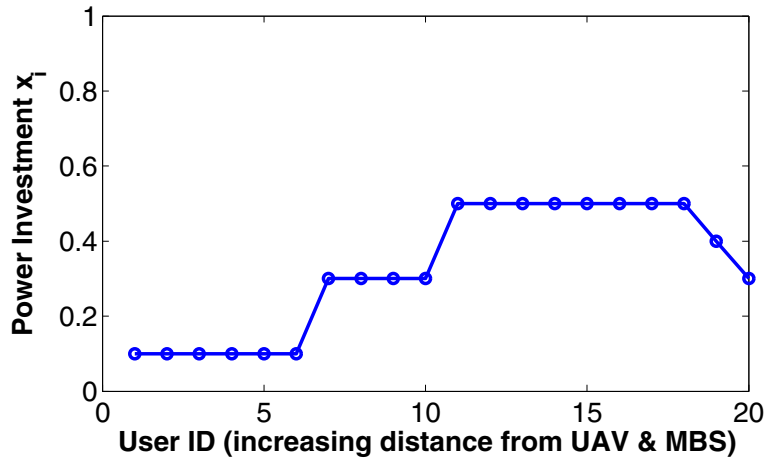

Fig. 3 User power investment x_i vs user ID: case of absence of malicious users

of their transmission power to the collapse prone UAV-based communication. The same applies for the very distant users (i.e., 19 and 20) who sense almost no interference since it has been significantly cancelled due to the application of the NOMA SIC technique. On the other hand, middle distance users are simultaneously affected by worsening channel conditions and rising interference levels, and subsequently they are attracted to invest more transmission power to the UAV communication, since it is expected to provide higher return - than the respective return of the the use of the safe resource of the MBS-based communication—for the same power investment.

The above analysis is also confirmed by the results in Fig. 4, illustrating the achievable data rates of each user from both its communication with the UAV and the MBS. As explained before, the close or the distant users manage to obtain high data rates from the UAV (blue bars) without excessive investment, whilst middle distance users achieve lower data rates since their transmission conditions (i.e., channel gain and interference) hinder meeting their QoS targets. On the other hand, all users obtain almost the same data rate (small variations are only observed) from their transmission via the MBS (red curve). The lower magnitude of MBS's bandwidth and the higher distance of the MBS from the users (compared to the UAV distance from the users) results in the delivery of significantly lower data rates, which however are considered as a safe and guaranteed return, due to the controlled access scheme of the operation of the MBS, and the strict bandwidth monitoring policies.

Similar behaviors are noted and same observations are drawn, as demonstrated in the following Figs. 5 and 6,

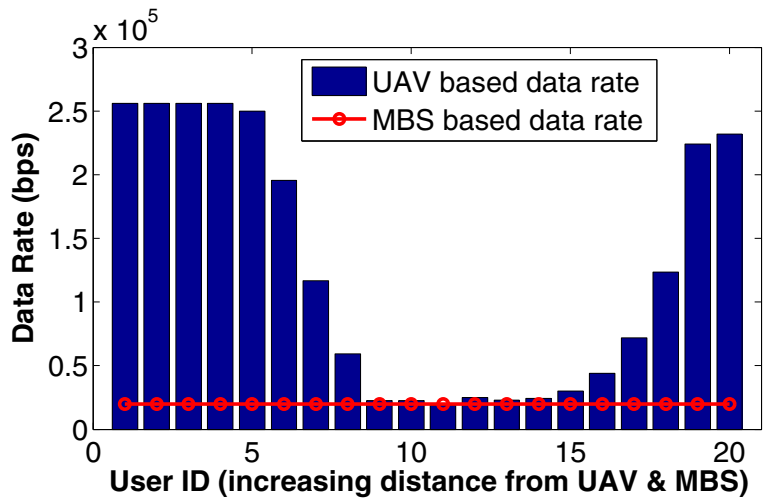

Fig. 4 User data rate vs user ID: case of absence of malicious users

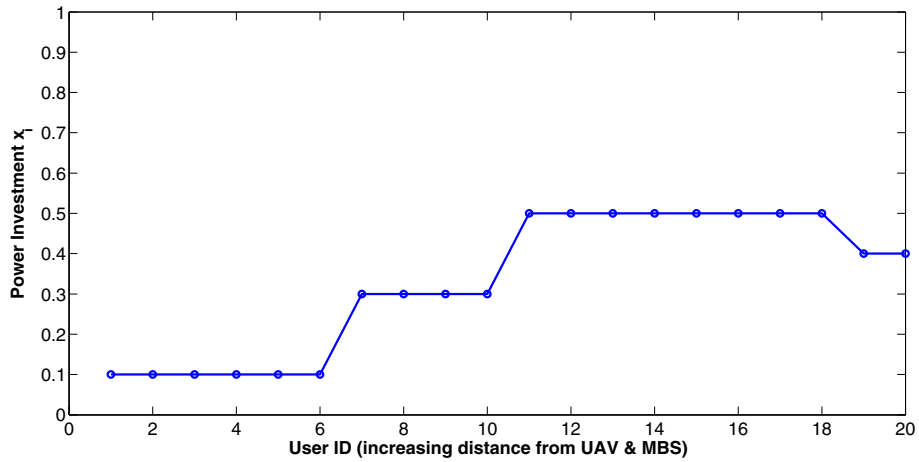

Fig. 5 User power investment x_i vs user ID (bandwidth 8 MHz, target data rate 512 kbps)

where the corresponding user power investment x_i to the UAV bandwidth per user ID, and the achievable data rates of each user from both its communication with the UAV and the MBS parameters are depicted respectively, for the case that the users are requesting a service of user data rate of 512 kbps, while the total available bandwidth is assumed 8 MHz. This outcome is quite well aligned with the holistic nature of our framework, in the sense that it can adapt its operation to the system-specific parameters (i.e., total available spectrum), as well as users' requested services. In addition, if we still maintain the limited available bandwidth of 4 MHz as in the original scenario, while on the other hand, we target at the user higher data rates of 512 kbps, then the corresponding results are presented in Figs. 7 and 8, respectively. In this case, the users with favorable transmission conditions (the ones closest to the UAV due to good channel gains or far away due to low interference) consume the majority of the available spectrum, since their achievable data rate is double than the original case presented in the paper (where 256 kbps was the targeted rate). As a result, the investment parameter follows a different trend than in the original case. In particular, users close to the UAV invest low power which suffices to meet their target, while the users farthest from the UAV, communicate with satisfactory data rates but have to invest to the full in the CPR, since the users closer to the UAV have already consumed a the largest fraction of the spectrum. The intermediate users are on the other hand so heavily impacted by the highest data rates of the close or most distant users, that practically do not manage to transmit via the CPR due to the high competition stemming from the increased data rates.

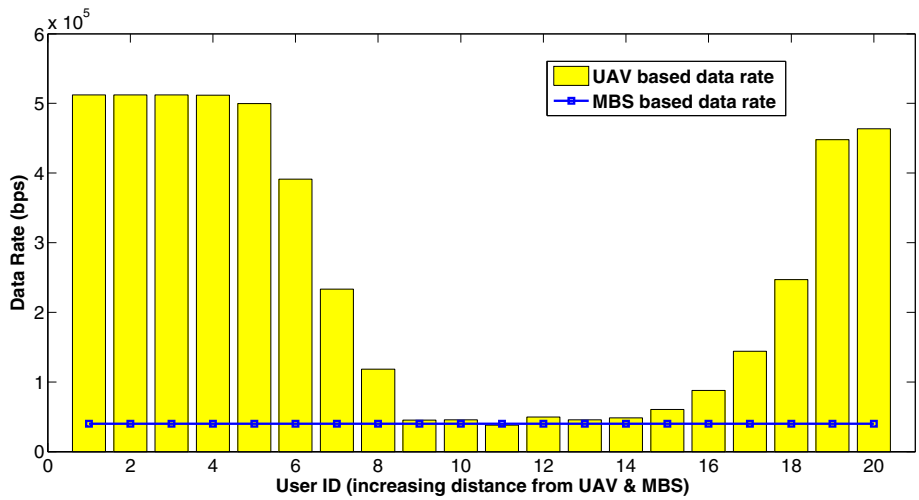

Fig. 6 User data rate vs user ID (bandwidth 8 MHz, target data rate 512 kbps)

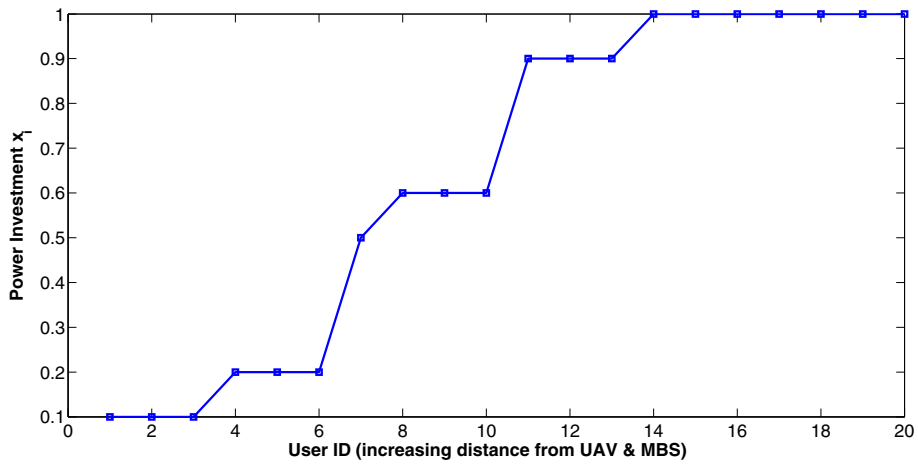

Fig. 7 User power investment x_i vs user ID (bandwidth 4 MHz, target data rate 512 kbps)

6.3 Malicious user behavior

Next, we discuss the case that the users with ID 11, 12, and 13 are presenting malicious behavior (i.e., $|N_M| = 3$), with their objective being the disruption of the UAV-based wireless communication. The latter is achieved through transmitting with abnormally high transmission power levels to the UAV causing interference and claiming significant bandwidth resources otherwise available to the rest of the normal users (i.e., $|N_N| = 17$), whose behavior is considered unmodified compared to the previous scenario. Specifically, users with ID 11–13 are assumed to eliminate their risk aversion parameter (i.e., $\lambda_i = 0$) and at the same time present a threefold increase of their sensitivity parameter towards the CPR (i.e., $\beta_i = 0.15$). As shown in Fig. 9, the power investment of users with ID 11–13 rises to the upper value (i.e., $x_i = 1$), implying that they solely try to communicate through the UAV. Under this scenario, we assume the case that the UAV's bandwidth sustains the attack both in terms of the higher interference levels and bandwidth distribution among the users. In Fig. 10, it is clearly observed that users with ID 11–13 due to their considerably risk seeking behavior managed to significantly increase their data rates in the CPR (i.e., the UAV-based communication), while they stopped transmitting via the MBS. The negative impact to the rest of the normal users has been mostly visible for users with ID 6–10 since they are the ones sensing the additional interference from the malicious users while also they have to manage their low quality channel gains. On the other hand, normal users still investing in the safe resource (i.e., the MBS-based communication) experienced a small increase in their attainable data rates through the MBS,

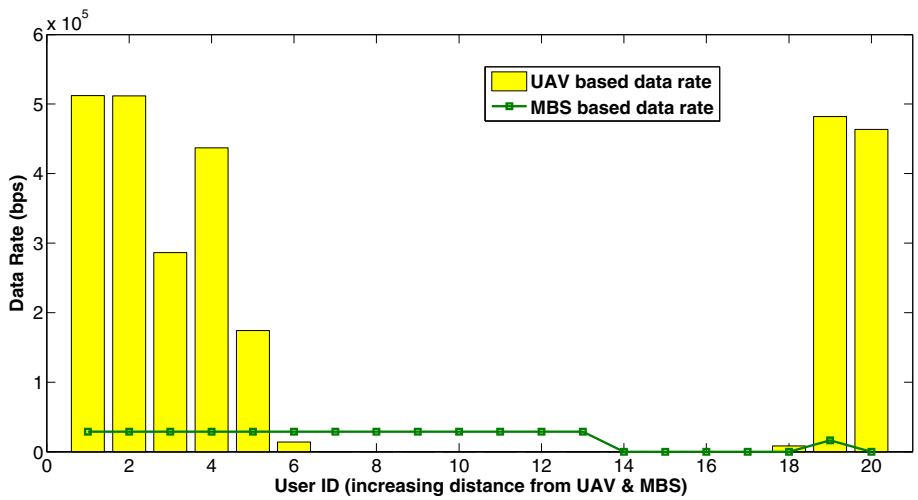

Fig. 8 User data rate vs user ID (bandwidth 4 MHz, target data rate 512 kbps)

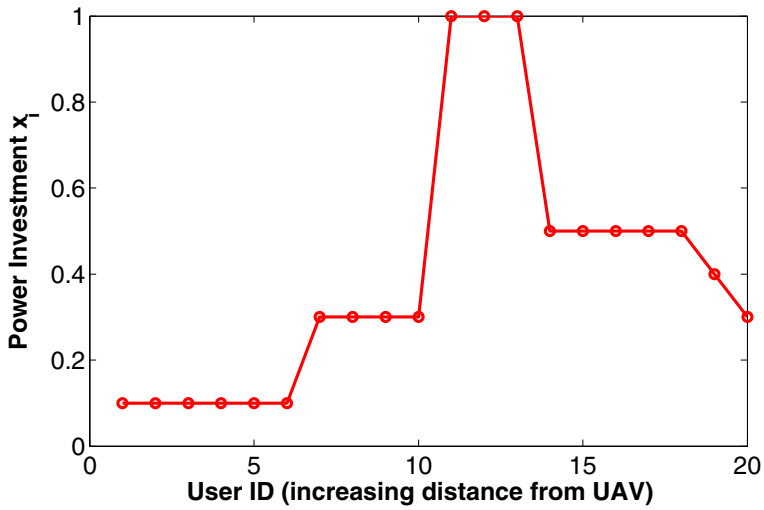

Fig. 9 User power investment x_i vs user ID: case of presence of malicious users 11–13

since the malicious users with ID 11–13 stopped transmitting via the MBS, thus they reduced the competition in this part of the network. The observed increase in the normal users' achievable data rate through the MBS is approximately 17.6%, as obtained by comparing the results presented in Figs. 4 and 10.

Subsequently, we consider another scenario with an intensified and of wider scale attack, performed by multiple malicious users. In particular, users with ID 10-18 are considered malicious (i.e., $|N_M| = 9$), where all of them completely invest in the UAV-based communication, hence driving the commonly shared UAV's bandwidth to collapse due to excessive demand and rising interference levels. This has immediate impact on the achieved energy-efficiency of the system, representing the transmitted data bits per Joule of consumed energy, measured in [bits/Joule]. In Fig. 11, we compare the energy-efficiency of each user for increasing distance from the UAV and the MBS. In the case where the system operates normally without any DDoS attack (green curve), we notice the trend explained before, with close and distant (from the receiver) users to have significantly higher energy-efficiency levels due to their favorable transmission in comparison to the middle distant users. On the other hand, in the incident of the intensive DDoS attack against the UAV bandwidth (red curve), the energy-efficiency is significantly reduced due to the failure of the UAV's bandwidth to serve the users requests. In this case, the malicious users do not manage to transmit at all, while the rest of normal users manage to obtain some returns only from their communication with the MBS.

6.3.1 Detection of malicious users

The detection of the malicious users' behavior towards protecting the proper operation of the UAV-based communication can be achieved both through the SAPIENSS

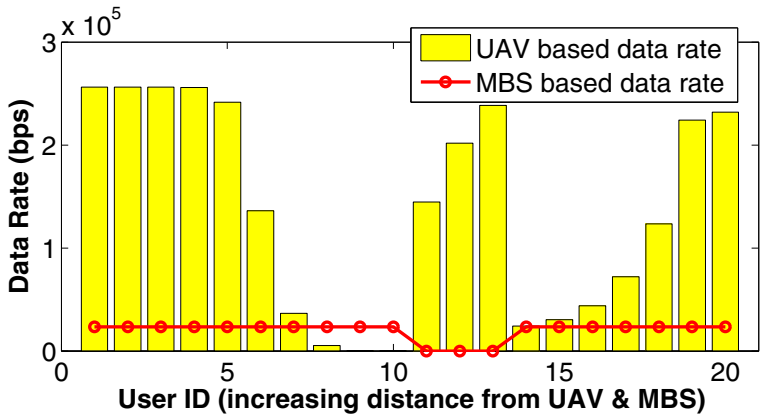

Fig. 10 User data rate vs user ID: case of presence of malicious users 11–13

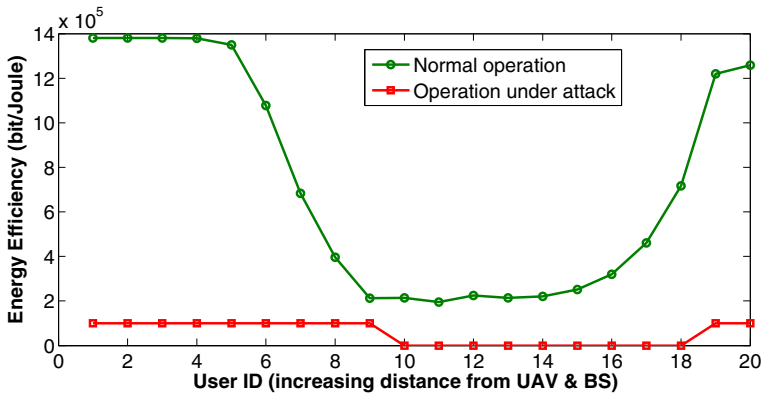

Fig. 11 Energy-efficiency vs user ID: case of intensive attack due to presence of malicious users 10–18 and collapse of UAV bandwidth

algorithm, as well as from the theoretical system model based on the principles of prospect theory. In particular, Fig. 12 compares each user invested transmission power to the UAV-based communication, when the system operates normally (green curve) with the case where the users with ID 11–13 present malicious behavior. It is shown that in the case that the UAV bandwidth is under attack, the malicious users transmit to the UAV choice with maximum power (i.e., $P_i^{\text{Max}} = 0.2$ W), which acts as a clear indication of their malicious behavior. The above result is well aligned with the overall behavioral modeling adopted in this work, allowing heterogeneous user preferences and risk perceptions. By studying the values of loss aversion and sensitivity parameters, malicious user behavior is reflected by their risk seeking attitude with regards to aggressively claiming bandwidth from the UAV. In Fig. 13, the behavioral deviation of normal and malicious users is easily noticed via the elimination of risk aversion from the latter, ($\kappa_i > 0$, $\lambda_i = 0$) and the increase in sensitivity ($a_i = 0.05$, $\beta_i = 0.15$), implying an aggressive stance of attackers ignoring the impact of UAV's bandwidth failure, which could result in an interruption of the UAV communication. On the other hand, normal users are implicitly concerned for the potentiality of system collapse so they tend to overweight the probability of failure of the UAV's bandwidth and subsequently adopt a more conservative behavior when transmitting via the UAV-based communication.

6.3.2 Defense mechanisms

In the following, we discuss an indicative counter measure when suspicious user activity is identified, in order to demonstrate the potential use of the proposed approach as an enhanced joint intrusion detection and ejection mechanism, towards ensuring the proper network operation and highest possible bandwidth availability to its users. As argued in the previous subsection, one of the basic operational characteristics of the malicious users in this work, which can be easily recognized is the considerably higher transmission power towards the UAV-based communication. The above feature can be used as an instant autonomous detection and intrusion ejection method. Towards this direction, in Fig. 14, we show the outcome and impact of the application of the proposed intrusion detection and ejection methodology described in Section 5. In particular, in this case, the SAPIENSS

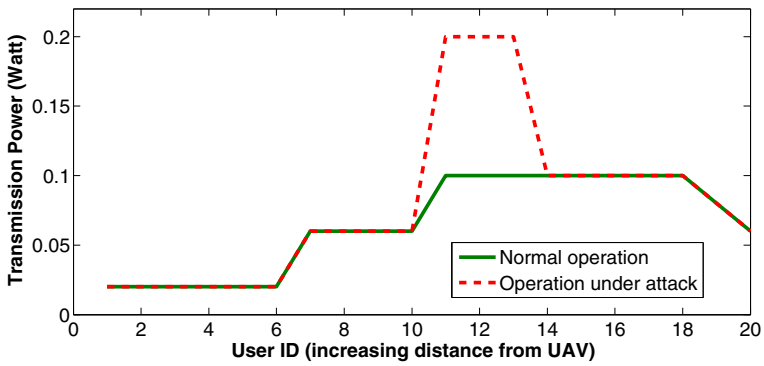

Fig. 12 Detecting malicious user behavior: Transmission power vs user ID

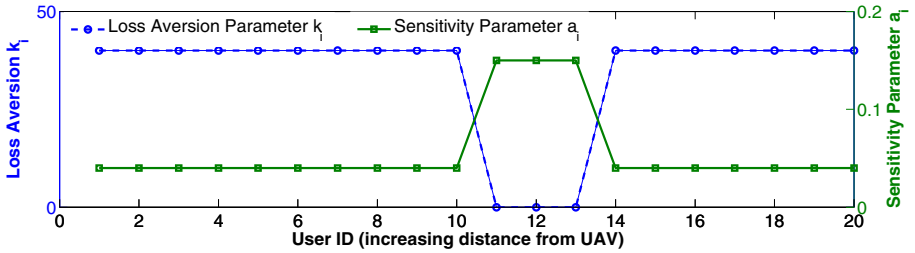

Fig. 13 Detecting malicious user behavior: Prospect-theoretic parameters vs user ID

algorithm identifies the potentially malicious users during its implementation steps, in case their transmission power is abnormally high compared to their closer neighbors, and further cancels the impact of their transmission on the rest of the users. In more detail, in the red curve, the original attack scenario is shown where the users with 11–13 are considered as malicious, since all the rest of the users transmit to the UAV with less than the half of their transmission power. Accordingly, the SAPIENSS algorithm in its next iteration ignores the transmission of those users and following the principles of the NOMA SIC technique, as described in Section 5, manages to mitigate their caused interference. This is shown in the green curve of Fig. 14, where we observe that the UAV has cancelled the interference caused by them to the rest of the normal users, thus the malicious users appear to the rest of the users like they do not transmit at all. Interestingly enough, this impacts positively the rest of the users of the network, since users with ID 7–10 reduce their investment to the UAV-based communication since their sensed interference has decreased according to the NOMA technology, while the users with ID 14–20 increase their investment to the UAV due to the reduced competition after the transmission cancellation of the users with ID 11–13.

7 Conclusions

In this paper, a novel framework towards ensuring the efficient and smooth operation of a UAV-assisted wireless network consisting of both normal and malicious risk-aware users is proposed. User devices are assumed capable of splitting their transmission power in two different communication alternatives—that is UAV-based and MBS-based communication links. The UAV's bandwidth is considered as common pool of resources (CPR), accessible by everyone, offering potentially high rate of return, but being susceptible to failure due to its potential over-exploitation. In contrast, the MBS's bandwidth is considered as a safe resource offering to the users a more limited but guaranteed level of service, due to the fact that though it has less available total bandwidth, it operates under a more controlled access and monitoring scheme. The theory of the tragedy of the commons is used to capture the probability of failure of the CPR, while the prospect theory is adopted to study the normal and malicious users' risk-aware behavior in the UAV-assisted network.

Representative prospect-theoretic utility functions have been introduced to reflect the users' power investment to the dual communication environment and a corresponding non-cooperative power control game among the users is formulated and solved. The existence and uniqueness of a pure Nash equilibrium point is shown and a distributed algorithm is introduced to converge to the PNE point. Based on the normal and malicious users' risk-aware behavioral characteristics, their corresponding transmission power investments as an outcome of the power control game, and the operational principles of the

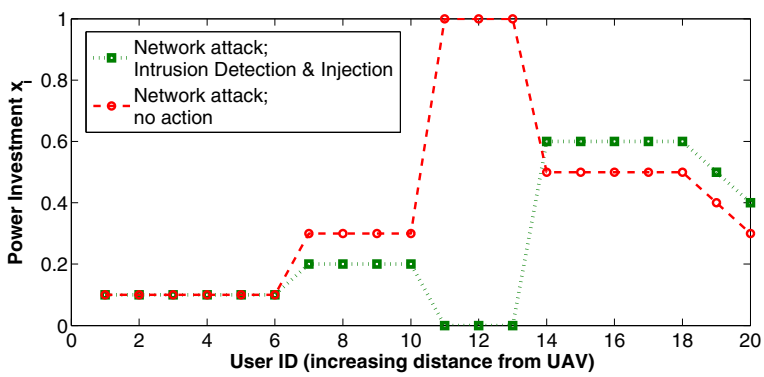

Fig. 14 Power investment vs user ID implementing intrusion detection and ejection

NOMA technology and the SIC technique, a novel intrusion detection and ejection methodology is introduced. The performance and inherent attributes of the proposed user-centric risk-aware operation framework, in terms of its capability to effectively utilize the available system and user resources (i.e., bandwidth and power), while succeeding in identifying potential abnormal or malicious user behaviors is assessed, under several different operation scenarios.

It should be noted that the problem addressed in this paper considered only one MBS and one UAV. Part of our current work is to extend this framework by considering the use of multiple UAVs, while at the same time taking into account the problem of UAV optimal placing as a mitigation action of the impact of malicious users. Also, though in our work we have assumed that the UAV is provided with sufficient power supply to support the UAV-based communication network within the considered time window of operation, the consideration of the UAV's battery life availability and flight duration within the overall proposed users' risk-aware resource management in UAV-assisted communication networks, is indeed a very interesting and challenging topic, and part of our current and future research. Finally, our current and future work contains the extension of the introduced framework and users' realistic behavior modeling, in several other emerging wireless communication and computing systems within the 5G and Internet of Things (IoT) era, including mobile edge computing (MEC), where the users decide their optimal data offloading to the MEC server and/or processing the data locally.

8 Method

This paper studies the problem of orchestrating and securing the dual communication in cognitive risk-aware UAV-assisted wireless networks, where users can select to communicate both with an MBS and UAV, with the first considered as a safe resource and the latter susceptible to failure if its bandwidth is over-exploited. The unrestricted access nature of the UAV's bandwidth by the users, may attract malicious users to infiltrate it and target to hinder its operation by transmitting at very high power levels. The proposed approach was formulated under the principles of prospect theory and the theory of the tragedy of the commons, allowing to model diverting risk preferences, while studying how system performance is impacted by individual users' behaviors and the counter active mechanisms, i.e., intrusion detection and ejection, towards protecting its uninterrupted operation. A series of numerical experiments investigated different operational scenarios confirming the importance of safeguarding the network against interference and bandwidth over-exploitation and/or abuse. The simulation code was written in MATLAB.

Abbreviations

BR: Best response; CPR: Common pool resource; D2D: Device-to-device; DDoS: Distributed denial of service; GPS: Global positioning system; IDS: Intrusion detection system; IES: Intrusion ejection system; IES: Intrusion ejection system; IoT: Internet of things; LoS: Line-of-sight; MBS: Macro base station; NOMA: Non orthogonal multiple access; PNE: Pure Nash equilibrium; PSN: Public safety networks; PT: Prospect theory; QoS: Quality of service; SAPIENSS: Security aware power investment for efficient network spectrum sharing; SIC: Successive interference cancellation; UAV: Unmanned aerial vehicles

Acknowledgements

This research was supported in part by the Hellenic Foundation for Research & Innovation (Award#: HFRI-FM17-2436). The research of Dr. Eirini Eleni Tsiropoulou was conducted as part of the NSF CRII-1849739.

Authors' contributions

All authors contributed significantly to the research work presented in this paper. P.V. had a leading role in the mathematical proof and the solution of the corresponding non cooperative game, while also evaluated the practical application of the proposed approach via designing the distributed algorithm and running an extensive series of numerical results via computer simulations. E.E.T. mainly contributed to the design of the prospect-theoretic models and the formulation of the considered utility functions, while devoted significant efforts in the article content, outline, and presentation. S.P. introduced the original concept and coordinated the overall preparation of the work with regard to both the theoretical background and its performance assessment, while he also orchestrated the writing of the article. All authors read and approved the final manuscript.

Competing interests

The authors declare that they have no competing interests.

Author details

[1]School of Electrical and Computer Engineering, National Technical University of Athens, 15780 Athens, Greece. [2]Department of Electrical and Computer Engineering, University of New Mexico, NM 87131 Albuquerque, USA.

Received: 30 August 2019 Accepted: 4 December 2019
Published online: 27 December 2019

References

1. L. Gupta, R. Jain, G. Vaszkun, Survey of important issues in uav communication networks. IEEE Commun. Surv. Tutor. **18**(2), 1123–1152 (2015)
2. S. Hayat, E. Yanmaz, R. Muzaffar, Survey on unmanned aerial vehicle networks for civil applications: a communications viewpoint. IEEE Commun. Surv. Tutor. **18**(4), 2624–2661 (2016)
3. R. Shakeri, M. A. Al-Garadi, A. Badawy, A. Mohamed, T. Khattab, A. K. Al-Ali, K. A. Harras, M. Guizani, Design challenges of multi-uav systems in cyber-physical applications: A comprehensive survey, and future directions. CoRR. **abs/1810.09729**, 1–44 (2018)
4. M. Zuckerberg, The technology behind aquila (2016). https://www.facebook.com/notes/mark-zuckerberg/the-technology-behind-aquila/10153916136506634/. Accessed 22 April 2019
5. A. Westgarth, Turning on project loon in puerto rico. https://blog.x.company/turning-on-project-loon-in-puerto-rico-f3aa41ad2d7f. Accessed 22 April 2019
6. R. Fan, J. Cui, S. Jin, K. Yang, J. An, Optimal node placement and resource allocation for uav relaying network. IEEE Commun. Lett. **22**(4), 808–811 (2018)
7. D. Sikeridis, E. E. Tsiropoulou, M. Devetsikiotis, S. Papavassiliou, Wireless powered public safety iot: a uav-assisted adaptive-learning approach towards energy efficiency. J. Netw. Comput. Appl. **123**, 69–79 (2018)
8. J. Baek, S. I. Han, Y. Han, Optimal resource allocation for non-orthogonal transmission in uav relay systems. IEEE Wirel. Commun. Lett. **7**(3), 356–359 (2018)
9. D. Sikeridis, E. EleniTsiropoulou, M. Devetsikiotis, S. Papavassiliou, in *2018 IEEE 19th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*. Self-adaptive energy efficient operation in uav-assisted public safety networks (IEEE, 2018), pp. 1–5

10. M. Hua, C. Li, Y. Huang, L. Yang, in *Wireless Communications and Signal Processing (WCSP), 2017 9th International Conference On*. Throughput maximization for uav-enabled wireless power transfer in relaying system (IEEE, 2017), pp. 1–5
11. D. Sikeridis, E. E. Tsiropoulou, M. Devetsikiotis, S. Papavassiliou, in *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)*. Socio-spatial resource management in wireless powered public safety networks (IEEE, 2018), pp. 810–815
12. P. Vamvakas, E. E. Tsiropoulou, S. Papavassiliou, Risk-aware resource management in public safety networks. Sensors. **19**(18), 3853 (2019)
13. P. Vamvakas, E. E. Tsiropoulou, S. Papavassiliou, in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. On the prospect of uav-assisted communications paradigm in public safety networks, (2019), pp. 762–767. https://doi.org/10.1109/INFCOMW.2019.8845131
14. M. Erdelj, O. Saif, E. Natalizio, I. Fantoni, Uavs that fly forever: Uninterrupted structural inspection through automatic uav replacement. Ad Hoc Networks. **94**, 1–12 (2017)
15. M. Erdelj, E. Natalizio, K. R. Chowdhury, I. F. Akyildiz, Help from the sky: leveraging uavs for disaster management. IEEE Pervasive Comput. **16**(1), 24–32 (2017)
16. A. Sanjab, W. Saad, T. Başar, in *2017 IEEE International Conference on Communications (ICC)*. Prospect theory for enhanced cyber-physical security of drone delivery systems: A network interdiction game (IEEE, 2017), pp. 1–6
17. A. Sanjab, W. Saad, T. Başar, A game of drones: Cyber-physical security of time-critical uav applications with cumulative prospect theory perceptions and valuations. arXiv preprint arXiv:1902.03506, 1–14 (2019)
18. M. Mozaffari, W. Saad, M. Bennis, M. Debbah, Unmanned aerial vehicle with underlaid device-to-device communications: Performance and tradeoffs. IEEE Trans. Wirel. Commun. **15**(6), 3949–3963 (2016)
19. M. Mozaffari, W. Saad, M. Bennis, M. Debbah, Mobile unmanned aerial vehicles (uavs) for energy-efficient internet of things communications. IEEE Trans. Wirel. Commun. **16**(11), 7574–7589 (2017)
20. S. Rahman, Y.-Z. Cho, Uav positioning for throughput maximization. EURASIP J. Wirel. Commun. Netw. **2018**(1), 31 (2018)
21. E. E. Tsiropoulou, J. S. Baras, S. Papavassiliou, G. Qu, in *International Conference on Decision and Game Theory for Security*. On the mitigation of interference imposed by intruders in passive rfid networks (Springer, 2016), pp. 62–80
22. A. Rawnsley, Iran's alleged drone hack: Tough, but possible. http://www.wired.com/dangerroom/2011/12/irandrone-hack-gps. Accessed 22 April 2019
23. C. Rani, H. Modares, R. Sriram, D. Mikulski, F. L. Lewis, Security of unmanned aerial vehicle systems against cyber-physical attacks. J. Defense Model. Simul. **13**(3), 331–342 (2016)
24. K. Hartmann, C. Steup, in *2013 5th International Conference on Cyber Conflict (CYCON 2013)*. The vulnerability of uavs to cyber attacks-an approach to the risk assessment (IEEE, 2013), pp. 1–23
25. T. Lagkas, V. Argyriou, S. Bibi, P. Sarigiannidis, Uav iot framework views and challenges: towards protecting drones as "things". Sensors. **18**(11), 4015 (2018)
26. H. Sedjelmaci, S. M. Senouci, N. Ansari, Intrusion detection and ejection framework against lethal attacks in uav-aided networks: A bayesian game-theoretic methodology. IEEE Trans. Intell. Transport. Syst. **18**(5), 1143–1153 (2016)
27. S. Bhattacharya, T. Başar, in *Proceedings of the 2010 American Control Conference*. Game-theoretic analysis of an aerial jamming attack on a uav communication network (IEEE, 2010), pp. 818–823
28. H. Sedjelmaci, S. M. Senouci, N. Ansari, A hierarchical detection and response system to enhance security against lethal cyber-attacks in uav networks. IEEE Trans. Syst., Man, Cybernet.: Syst. **48**(9), 1594–1606 (2017)
29. Z. Birnbaum, A. Dolgikh, V. Skormin, E. O'Brien, D. Muller, C. Stracquodaine, in *2015 International Conference on Unmanned Aircraft Systems (ICUAS)*. Unmanned aerial vehicle security using behavioral profiling (IEEE, 2015), pp. 1310–1319
30. G. Choudhary, V. Sharma, I. You, K. Yim, R. Chen, J.-H. Cho, in *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*. Intrusion detection systems for networked unmanned aerial vehicles: A survey (IEEE, 2018), pp. 560–565
31. M. E. Mkiramweni, C. Yang, J. Li, Z. Han, Game-theoretic approaches for wireless communications with unmanned aerial vehicles. IEEE Wirel. Commun. **25**(6), 104–112 (2018)
32. P. Vamvakas, E. E. Tsiropoulou, S. Papavassiliou, in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*. Dynamic spectrum management in 5g wireless networks: A real-life modeling approach (IEEE, 2019), pp. 2134–2142
33. P. Vamvakas, E. E. Tsiropoulou, S. Papavassiliou, On controlling spectrum fragility via resource pricing in 5g wireless networks. IEEE Network. Lett. **1**(3), 111–115 (2019)
34. D. Kahneman, A. Tversky, in *Handbook of the Fundamentals of Financial Decision Making: Part I*. Prospect theory: An analysis of decision under risk (World Scientific, 2013), pp. 99–127
35. A. Jones, P. Darwood, P. Howard, Simultaneous dual mode operation in cellular networks. Google Patents. US Patent App. 11/398,255 (2007)
36. K. Etemad, V. Gupta, N. Himayat, S. Talwar, Opportunistic carrier aggregation for dynamic flow switching between radio access technologies. Google Patents. US Patent 9,119,154 (2015)
37. G. Hardin, Extensions of the tragedy of the commons. Science. **280**(5364), 682–683 (1998)
38. E. E. Tsiropoulou, P. Vamvakas, S. Papavassiliou, in *2012 IEEE Wireless Communications and Networking Conference (WCNC)*. Energy efficient uplink joint resource allocation non-cooperative game with pricing (IEEE, 2012), pp. 2352–2356
39. Boeing insitu scaneagle (2019). https://www.insitu.com/information-delivery/hardware#2. Accessed 14 Oct 2019
40. Aerovironment rq-11 raven (2019). https://www.avinc.com/uas/view/raven. Accessed 14 Oct 2019
41. C. K. Chin, Extending the endurance, missions and capabilities of most uavs using advanced flexible/ridged solar cells and new high power density batteries technology. Tech. Rep. (2011)
42. I. Kantor, A. N. Srivastava, D. M. Pasko, H. Batla, G. Ubhi, Unmanned aerial vehicle network-based recharging. Google Patents. US Patent 9,412,279 (2016)
43. E. E. Tsiropoulou, G. K. Katsinis, S. Papavassiliou, in *2010 European Wireless Conference (EW)*. Utility-based power control via convex pricing for the uplink in cdma wireless networks (IEEE, 2010), pp. 200–206
44. P. Vamvakas, E. E. Tsiropoulou, S. Papavassiliou, J. S. Baras, in *2017 IEEE Symposium on Computers and Communications (ISCC)*. Optimization and resource management in noma wireless networks supporting real and non-real time service bundling (IEEE, 2017), pp. 697–703
45. L. Xiao, N. B. Mandayam, H. V. Poor, Prospect theoretic analysis of energy exchange among microgrids. IEEE Trans. Smart Grid. **6**(1), 63–72 (2014)
46. L. Xiao, J. Liu, Y. Li, N. B. Mandayam, H. V. Poor, in *2014 IEEE Global Communications Conference*. Prospect theoretic analysis of anti-jamming communications in cognitive radio networks (IEEE, 2014), pp. 746–751
47. A. Sumalee, R. D. Connors, P. Luathep, in *Transportation and Traffic Theory 2009: Golden Jubilee*. Network equilibrium under cumulative prospect theory and endogenous stochastic demand and supply (Springer, 2009), pp. 19–38
48. S. Gao, E. Frejinger, M. Ben-Akiva, Adaptive route choices in risky traffic networks: A prospect theory approach. Trans. Res. Part C: Emerg. Technol. **18**(5), 727–740 (2010)
49. T. M. Apostol, *Calculus, Volume I, One-variable Calculus, with an Introduction to Linear Algebra*, vol. 1. (John Wiley & Sons, 2007)
50. A. R. Hota, S. Garg, S. Sundaram, Fragility of the commons under prospect-theoretic risk attitudes. Games Econ. Behav. **98**, 135–164 (2016)
51. E. E. Tsiropoulou, P. Vamvakas, S. Papavassiliou, Joint customized price and power control for energy- efficient multi-service wireless networks via s-modular theory. IEEE Trans. Green Commun. Network. **1**(1), 17–28 (2017)

Publisher's Note