CISTER
Research Centre in
Real-Time & Embedded
Computing Systems

Conference Paper

Proactive Eavesdropping via Jamming for Trajectory Tracking of UAVs

Kai Li
Salil S. Kanhere
Wei Ni
Eduardo Tovar
Mohsen Guizani

CISTER-TR-190404

Proactive Eavesdropping via Jamming for Trajectory Tracking of UAVs

Kai Li, Salil S. Kanhere, Wei Ni, Eduardo Tovar, Mohsen Guizani

CISTER Research Centre

Polytechnic Institute of Porto (ISEP P.Porto)

Rua Dr. António Bernardino de Almeida, 431

4200-072 Porto

Portugal

Tel.: +351.22.8340509, Fax: +351.22.8321159

E-mail:

https://www.cister-labs.pt

Abstract

This paper considers that a legitimate UAV trackssuspicious UAVs 19 flight for preventing intended crimes andterror attacks. To enhance tracking accuracy, the legitimateUAV proactively eavesdrops suspicious UAVs 19 communicationvia sending jamming signals. A tracking algorithm isdeveloped for the legitimate UAV to track the suspiciousflight by comprehensively utilizing eavesdropped packets,angle-of-arrival and received signal strength of the suspicioustransmitter 19s signal. A new co-simulation frameworkis implemented to combine the complementary features ofoptimization toolbox with channel modeling (in Matlab) anddiscrete event-driven mobility tracking (in NS3). Moreover,numerical results validate the proposed algorithms in termsof tracking accuracy of the suspicious UAVs 19 trajectory.

Proactive Eavesdropping via Jamming for Trajectory Tracking of UAVs

Kai Li*, Salil S. Kanhere†, Wei Ni‡, Eduardo Tovar*, and Mohsen Guizani§
*Real-Time and Embedded Computing Systems Research Centre (CISTER), Porto, Portugal.
Email: {kai_li, emt}@isep.ipp.pt.
†The University of New South Wales, Australia.
Email: salil.kanhere@unsw.edu.au.
‡Commonwealth Scientific and Industrial Research Organization (CSIRO), Sydney, Australia.
Email: wei.ni@csiro.au.
§Department of Electrical and Computer Engineering, University of Idaho, Moscow, USA.
Email: mguizani@ieee.org.

***Abstract*—This paper considers that a legitimate UAV tracks suspicious UAVs' flight for preventing intended crimes and terror attacks. To enhance tracking accuracy, the legitimate UAV proactively eavesdrops suspicious UAVs' communication via sending jamming signals. A tracking algorithm is developed for the legitimate UAV to track the suspicious flight by comprehensively utilizing eavesdropped packets, angle-of-arrival and received signal strength of the suspicious transmitter's signal. A new co-simulation framework is implemented to combine the complementary features of optimization toolbox with channel modeling (in Matlab) and discrete event-driven mobility tracking (in NS3). Moreover, numerical results validate the proposed algorithms in terms of tracking accuracy of the suspicious UAVs' trajectory.**

***Index Terms*—Unmanned Aerial Vehicles, Flight tracking, Proactive eavesdropping, Legitimate surveillance**

I. Introduction

Thanks to recent technological advances, many types of Unmanned Aerial Vehicles (UAVs), more popularly known as drones, are being widely used in complex real world environments. The recent availability of cost-effective UAVs has considerably promoted its use in information surveillance for homeland defense [1], [2]. However, with the rapidly growing popularity of UAVs in the consumer market, criminals or terrorists can potentially use them to establish wireless communication for committing crimes and terrorism, e.g., reconnoitring and locating targets together for dropping explosives [3], [4]. Therefore, there is a growing need for government agencies to legitimately monitor flight of suspicious UAVs while eavesdropping their critical data exchange. In particular, different from conventional wireless security that assumes communication links are used for lawful purposes and aims to maximize secrecy against illegitimate eavesdropping [5]–[7], we consider a legitimate UAV surveillance scenario, where the suspicious UAVs fly a collision-free formation flight, where they periodically exchange flight information so as to keep a prescribed relative distance and heading direction. A legitimate surveilling UAV aims to track flight trajectory of the suspicious UAVs via overhearing their communication, as shown in Figure 1, which contains a suspicious communication link, a wireless eavesdropping link and a jamming link. By tracking the flight of the suspicious UAVs, the legitimate UAV can monitor the suspicious UAVs' behavior for preventing intended crimes and terror attacks, e.g., reconnoitring and locating targets together for dropping explosives [8]. Moreover, tracking the flight trajectory of suspicious UAVs and eavesdropping their communication significantly affect each other in legitimate surveillance. Specifically, the flight trajectory of suspicious UAVs can be accurately tracked by the legitimate UAV if their flight information is eavesdropped. On the other hand, an accurate flight tracking guarantees that the suspicious UAVs are covered by the radio range of the legitimate UAV, which ensures their communications can be overheard. We also note that the legitimate UAV is able to jam the suspicious receiver in order to force a change in the suspicious communication (e.g., to a lower data rate) for overhearing more efficiently [9]. The legitimate UAV can control its jamming power to improve packet eavesdropping rate, especially when the legitimate UAV is far from the suspicious transmitter and receiver.

The problem of accurately tracking the suspicious flight via eavesdropping the suspicious transmission is not trivial. Several critical challenges arise in such a surveillance scenario. First, it could be possible that some suspicious packets are not successfully overheard due to poor signal-to-noise ratio (SNR) of the eavesdropping link. Thus, the legitimate UAV needs to be able to persistently track the suspicious flight trajectory given the uncertain channel dynamics. Second, given the time-varying, lossy airborne, fading channels, the legitimate UAV may not be able to precisely decode the entire message sent to the suspicious receiver as the received SNR (and accordingly the achievable data rate) at the legitimate UAV may not always be above the minimum threshold. Note that the suspicious transmitter can adapt its data rate so as to maintain a target outage probability at the suspicious receiver [10]. It is therefore critical to control the jamming power of the

legitimate UAV to ensure the received SNR is enough for decoding the data.

In this paper, a Legitimate Tracking Algorithm (LTA) is proposed to figure out waypoints of trajectory for the legitimate UAV by decoding the eavesdropped packet of the suspicious UAVs. In case the suspicious packet is not successfully eavesdropped, LTA also utilizes angle-of-arrival (AOA) and received signal strength (RSS) of the suspicious UAV's signal to ensure the eavesdropping coverage of the legitimate UAV for the sake of persistent surveillance. In order to evaluate the performance of tracking, a new co-simulation framework, JAMSIM, is implemented to combine the complementary features of optimization toolbox with channel modeling (in Matlab) and discrete event-driven mobility tracking (in NS3). Particularly, JAMSIM employs network socket programming to support message exchange between Matlab and NS3. The network socket with Matlab not only encapsulates the step information on the jamming power of the legitimate UAV and sends to the NS3, but also suspend the Matlab simulator in order to wait for responded results from NS3 to continue.

The rest of the paper is organized as follows: Section II reviews the literature on wireless security and UAV tracking techniques. In Section III, LTA is proposed for the legitimate UAV to track the suspicious flight trajectory via proactive eavesdropping. Simulation results are shown in Section IV, followed by a conclusion in Section V.

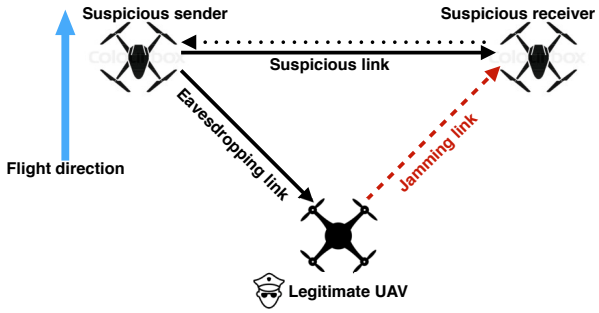

Fig. 1: Two suspicious UAVs follow a collision-free formation flight. A legitimate UAV is employed to track their flight by proactively eavesdropping suspicious UAVs' communication via sending jamming signals.

II. Related work

In this section, we review the literature on UAV tracking strategies. For mobile target tracking with the UAV, the algorithms in the literature can be generally classified to two categories, i.e., *signal-based tracking* and *vision-based tracking*. In the first category, the UAV determines the target's motion based on different aspects of the received wireless signals such as RSS, AOA, or time difference of arrival (TDOA). In [11], main physical and cyber threats from unauthorized UAVs are summarized. The possible ways using ambient radio frequency signals (emitted from the suspicious UAVs), radars, and acoustic sensors for tracking trajectory are also studied. A navigation law is developed for the UAV to track mobile ground units for communication relay establishment without the apriori knowledge on ground unit positions [12]. The navigation law employs two measurements for each ground unit, the RSS and AOA. Koohifar *et al.* [13] study UAVs that are equipped with wireless transceivers locate a moving radio transmitter. A tracking algorithm is developed to predict mobility of the target, and steers the tracking UAVs only based on the signal strength information obtained from the target. The authors in [14] consider a scenario with two non-collocated UAVs where their sensors measure TDOA over a number of emissions from a targeted moving radio transmitter. To track the target's movement using TDOA, the multiple devices need to be precisely synchronized to achieve meaningful TDOA measurements. In [15], an actor UAV is employed to perform networking-related functionalities such as processing or relaying data in multi-UAV systems. An actor UAV tracking strategy is studied, which utilizes a hybrid antenna model to combine the complimentary features of an isotropic omni radio and directional antennas. Their tracking strategy working with the hybrid antenna model is adapted to the constraints of UAV systems such as quick neighbor UAV tracking during flight, varying signal strength depending on the antenna orientation and reorganization requirements in case of topology changes. The authors in [16] focus on a virtual forces based clustering algorithm for neighbor UAV tracking, while maintaining a connected communication network. Particularly, the virtual forces are drawn from the Valence Shell Electron Pair Repulsion model, where forces among electron pairs surrounding a central atom actively position the entities of a system. For tracking the UAV, the virtual forces create wireless interactions among the UAVs and to form a specific topology of the system. A spatially adaptive approach based on molecular geometry is studied for tracking UAVs [17]. The analysis of molecular geometry is used to design a tracking algorithm that adapts the formation of the UAVs to spatially constrained spaces and resolves the chances of flight collision. Different from the tracking strategies solely relying on the received wireless signals, we propose a new tracking algorithm based on the proactive eavesdropping working with the *signal-based tracking* strategies.

In the second category, the UAV tracks the target by using onboard vision sensors, e.g., camera and optical sensor. The literatures [18]–[21] describe the development and evaluation of the vision-based collision detection and tracking algorithm suitable for UAVs. They also consider optical measurements from cameras onboard the UAV to estimate both the relative pose and relative velocities of another UAV or target object. However, the vision sensor is easily affected by weather conditions, such as rain, fog, and smoke.

III. Legitimate Tracking Algorithm

In this section, we present LTA to properly pursue the suspicious UAVs by using the proactive eavesdropping method. In case the eavesdropped packet is not successfully decoded, LTA also utilizes the AOA and RSS of the suspicious UAV's signal to ensure the eavesdropping coverage of the legitimate UAV for the sake of persistent surveillance.

To guarantee that the legitimate jamming and eavesdropping are undetectable by the suspicious UAVs, Signal-to-Interference-plus- Noise Ratio (SINR) of the suspicious link has to be maintained at a certain value δ. We define SNR of the eavesdropping link at t as $\gamma_e(t)$. Moreover, $\gamma_e(t) \geq \delta$ is required by UAV$_L$ to successfully eavesdrop the suspicious transmission, which gives

$$P_L(t) \geq \frac{N_0 \cdot (H_s(t) - H_e(t))}{H_e(t)}, \tag{1}$$

where $H_s(t)$, $H_e(t)$, and N_0 denote channel gain in the suspicious link, channel gain in the eavesdropping link, and power of white Gaussian noise, respectively. Therefore, the jamming power can be initialized by

$$P_L^0(t) = \frac{N_0 \cdot (H_s(t) - H_e(t))}{H_e(t)}. \tag{2}$$

Let P_L^{max} denote the maximum jamming power of UAV$_L$. $P_L^0(t)$ is examined by UAV$_L$ if $0 \leq P_L^0(t) \leq P_L^{max}$ can hold. Otherwise, it indicates that the required jamming power is much higher than the available specific power, i.e., the quality of the eavesdropping link is too poor to decode the suspicious packet. In this case, UAV$_L$ eavesdrops without sending jamming signals to interfere suspicious transmission for the purpose of power efficiency. Note that the modulation level at UAV$_{ST}$ is adapted to the jamming power $P_L(t)$ at UAV$_L$ [22], [23]. Specifically, UAV$_{ST}$ increases the modulation level to transmit data with an increasing $P_L(t)$ so that the SINR of the suspicious link at time slot t is maintained at δ. Furthermore, the optimal jamming power denoted by $P_L^\star(t)$ is able to be derived by convex optimization techniques, e.g., interior-point method, according to [24].

The proactive eavesdropping method is presented in Algorithm 1. In addition, since $P_L^\star(t)$ can be solved by linear optimization techniques, e.g., linear programming, the power consumption of executing the proactive eavesdropping is much smaller than the jamming power of UAV$_L$, and is comparatively negligible.

Due to terrestrial propagation environment and antenna gain, the RSS at UAV$_L$, denoted by $\phi_L(t)$, can be given by [25]

$$\phi_L(t) = \frac{G_{ST} G_L P_{ST}(t) H_{ST}^2(t) h_L^2(t)}{d^4(t)}, \tag{3}$$

where $P_{ST}(t)$ denotes the transmit power of UAV$_{ST}$. G_{ST} is the transmit antenna gain (i.e., UAV$_{ST}$), and G_L is the receive antenna gain (i.e., UAV$_L$). $H_{ST}(t)$ and $h_L(t)$ define the heights of UAV$_{ST}$ and UAV$_L$ at time t, respectively.

Algorithm 1 Proactive Eavesdropping Method

1: **Input:** $P_L^0(t) = \frac{N_0 \cdot (H_s(t) - H_e(t))}{H_e(t)}$, and δ.
2: UAV$_{ST}$ transmits the packet over the suspicious link.
3: UAV$_L$ overhears the packet in the eavesdropping link, where the SNR is $\gamma_e(t)$.
4: UAV$_L$ sets its jamming power to $P_L^0(t)$.
5: **if** $0 \leq P_L^0(t) \leq P_L^{max}$ **then**
6: $P_L^\star(t)$ is derived [24], where the SINR of the suspicious link at time slot t is maintained at δ.
7: **else**
8: $P_L^\star(t) \leftarrow 0$.
9: **end if**
10: **Output:** $P_L^\star(t)$.

Suppose that $\theta(t)$ is the AOA of the eavesdropping signal at UAV$_L$ at time t. The distance between UAV$_{ST}$ and UAV$_L$ at t_1 and t_2 is given by $d(t_1)$ and $d(t_2)$, respectively, which can be obtained by in-flight RSS measurement [26]. Hence, the distance of UAV$_{ST}$'s flight from t_1 to t_2, denoted by Δd_{ST}, can be given by

$$\Delta d_{ST} = \sqrt{d^2(t_1) + d^2(t_2) - 2d(t_1)d(t_2)\cos(\theta(t_2) - \theta(t_1))}. \tag{4}$$

Assume that the coordinates of UAV$_L$ at t_1 and t_2 in the three-dimensional space are $(x_L(t_1), y_L(t_1), z_L(t_1))$ and $(x_L(t_2), y_L(t_2), z_L(t_2))$, respectively. Then, we have

$$(x_L(t_2), y_L(t_2), z_L(t_2)) \rightarrow \begin{cases} x_L(t_2) = x_L(t_1) + \Delta d_{ST} \\ y_L(t_2) = y_L(t_1) + \Delta d_{ST} \\ z_L(t_2) = d(t_2)\sin(1 - \theta(t_2)) \end{cases} \tag{5}$$

In particular, when the packet is successfully eavesdropped, the coordinates of UAV$_{ST}$, denoted by $(x_{ST}(t), y_{ST}(t), z_{ST}(t))$, can be known to UAV$_L$. In this case, UAV$_L$ is able to derive the next waypoint of its flight, which is

$$(x_L(t_2), y_L(t_2), z_L(t_2)) \rightarrow \begin{cases} x_L(t_2) = x_L(t_1) + [x_{ST}(t_2) - x_{ST}(t_1)] \\ y_L(t_2) = y_L(t_1) + [y_{ST}(t_2) - y_{ST}(t_1)] \\ z_L(t_2) = z_L(t_1) + [z_{ST}(t_2) - z_{ST}(t_1)] \end{cases}$$

Furthermore, Algorithm 2 presents the legitimate tracking scheme that comprehensively considers the outcome of the proactive eavesdropping, and the in-flight measurement of AOA and RSS. Specifically, if the suspicious packet is successfully eavesdropped by UAV$_L$, i.e., $\gamma_e(t) \geq \delta$, UAV$_L$ is able to derive its next waypoint based on (5). Otherwise, UAV$_L$ measures the AOA and RSS of the suspicious transmission in order to obtain $\theta(t)$ and $\phi_L(t)$ at t_1 and t_2. According to (3), the distance between UAV$_{ST}$ and UAV$_L$ at t_1 and t_2 can be given by applying

$$d(t) = \sqrt[4]{G_{ST} G_L P_{ST}(t) H_{ST}^2(t) h_L^2(t) / \phi_L(t)}. \tag{6}$$

Therefore, Δd_{ST} can be obtained by (4). Given (5), the next waypoint of UAV$_L$ is updated by substituting Δd_{ST} and $\theta(t_2)$. In terms of computational complexity, LTA requires $O(T)$ time in the worst case, where T is the total number of time slots, as the proactive eavesdropping could be conducted in Algorithm 2. Note that the proposed LTA is general and can track any flight trajectory of the suspicious UAVs with the optimized jamming power of UAV$_L$.

Algorithm 2 Legitimate Tracking Algorithm

Initialize: $\phi_L(t) = 0$, $\theta(t) = 0$, $\Delta d_{ST} = 0$, $f_0, P_{ST}(t), G_{ST}, G_L$.
if $\gamma_e(t) \geq \delta$ **then**
  UAV$_L$ carries out the proactive eavesdropping method in Algorithm 1 $\rightarrow$ $(x_{ST}(t_1), y_{ST}(t_1), z_{ST}(t_1))$;
  $(x_{ST}(t_2), y_{ST}(t_2), z_{ST}(t_2))$.
  The next waypoint of UAV$_L$'s flight is updated by $x_L(t_2) \rightarrow x_L(t_1) + [x_{ST}(t_2) - x_{ST}(t_1)]$;
  $y_L(t_2) \rightarrow y_L(t_1) + [y_{ST}(t_2) - y_{ST}(t_1)]$;
  $z_L(t_2) \rightarrow z_L(t_1) + [z_{ST}(t_2) - z_{ST}(t_1)]$.
else
  Measure AOA of the eavesdropping signal at t_1 and $t_2 \rightarrow \theta(t_1)$ and $\theta(t_2)$.
  Measure RSS of the eavesdropping signal at t_1 and $t_2 \rightarrow \phi_L(t_1)$ and $\phi_L(t_2)$.
  $d(t_1)$ and $d(t_2) \leftarrow$ (3).
  The $\Delta d_{ST} \leftarrow$ (4).
  The next waypoint of UAV$_L$'s flight is updated $\leftarrow$ (5).
end if

IV. Performance Evaluation

In this section, we firstly develop a new co-simulation framework, JAMSIM, which combines the complementary features of a constrained optimization solver, i.e., Matlab, and a network simulator, i.e., NS3. Next, we evaluate the eavesdropping and tracking performance of the proactive eavesdropping algorithm working with the legitimate tracking algorithm based on JAMSIM.

A. Development of JAMSIM

For evaluating performance of LTA, we develop a new co-simulation framework, JAMSIM, which combines the complementary features of a constrained optimization solver, i.e., Matlab, and a network simulator, i.e., NS3. Our use of MATLAB is also because solving $P_L^\star(t)$ in the proposed proactive eavesdropping method can be readily implemented by using the MATLAB CVX toolbox. In addition, it is convenient to generate fast changing airborne wireless channels in MATLAB to simulate the proactive eavesdropping method. However, tracking the suspicious UAV's trajectory based on AOA and RSS has to be evaluated using a discrete event-driven simulator [27], e.g., NS3. To achieve a meaningful simulation, JAMSIM is developed to evaluate proactive eavesdropping and legitimate tracking performance in parallel.

Figure 2 shows the coding diagram of JAMSIM, which presents function interactions between NS3 and Matlab. Specifically, in NS3, the flight trajectory and the data packets of the suspicious UAVs are generated. Meanwhile, the mobility and channel models of the UAVs are configured in Matlab to derive $\gamma_e(t)$ which is imported to the simulation in NS3. Based on LTA, the next waypoint of UAV$_L$'s flight can be obtained. To ensure the eavesdropping coverage of UAV$_L$ for persistent surveillance, the next waypoint of UAV$_L$'s flight is used to update the mobility model in NS3 for eavesdropping the next data packet.

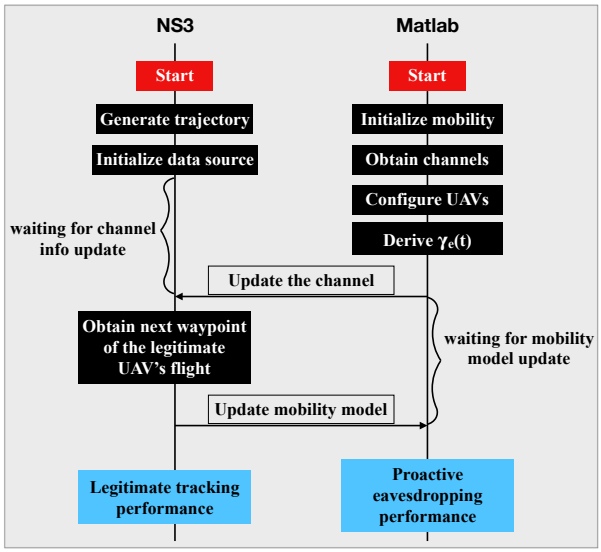

Fig. 2: The coding diagram of JAMSIM.

In terms of configurations in JAMSIM, the patrolling speed of UAV$_L$ is set to 10 m/s. The total number of data packets transmitted by UAV$_{ST}$ is 100. UAV$_{ST}$ sends the flight information to UAV$_{SR}$ every time slot. Meanwhile, UAV$_L$ eavesdrops the suspicious packet and decides to jam its transmission. In addition, the suspicious link, eavesdropping link, and jamming link are assumed to be block-fading, i.e., the channels remain unchanged during each transmission block, and may change from block to block.

B. Trajectory tracking performance

We evaluate trajectory tracking error of LTA. In particular, we define the tracking error as a distance between the actual next waypoint of UAV$_L$, which is obtained by LTA, and its expected next waypoint (i.e., ground truth), which is calculated by the coordinates of UAV$_L$ plus the moving distance of UAV$_{ST}$ along its heading.

Figure 3 shows the flight tracking performance of the proposed legitimate tracking algorithm when δ in PES is set to 10 dB and 20 dB, respectively. A numerical comparison

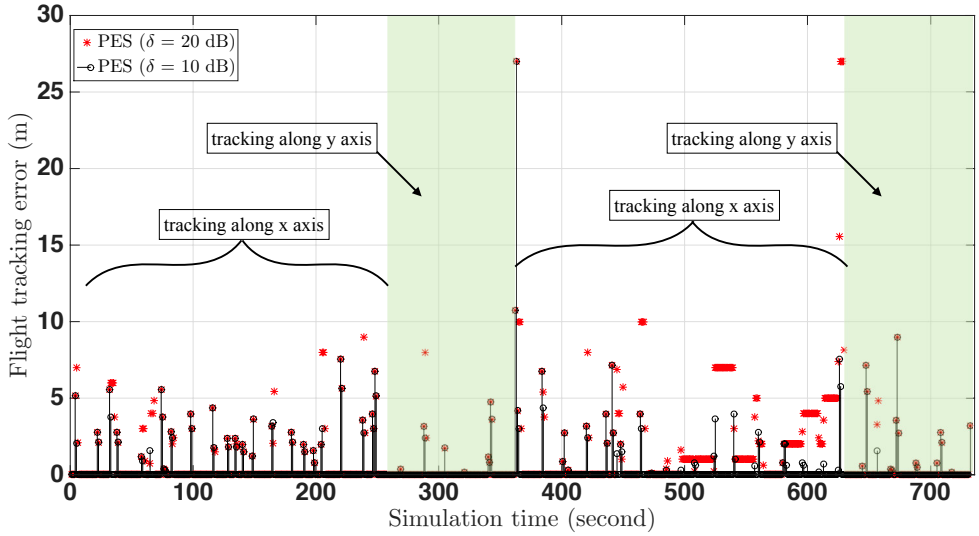

Fig. 3: Tracking error of the proposed LTA.

of tracking error is provided in Figure 3. Specifically, the average tracking error on "(δ = 20 dB)" and "(δ = 10 dB)" is around 1.23 and 0.45 meters, respectively. In particular, the suspicious UAVs fly horizontally at the first 240 seconds, and from 380 to 620 seconds, while UAV_L tracks their flight along the x-axis. During the other time, the suspicious UAVs fly vertically, and UAV_L tracks the flight along the y-axis. The maximum tracking error is 27.5 meters, which appears at the starting point when UAV_{ST} changes their heading from horizontal to vertical.

To observe the performance difference more clearly, Figure 4 shows the flight trajectories of the UAVs using proposed legitimate tracking algorithm when δ in PES is set to 20 dB. It can be observed that the trajectory of UAV_L generally matches the one of the suspicious UAVs, which confirms that UAV_L using the tracking algorithm is able to pursue the suspicious UAVs in the case that the packet eavesdropped by PES is not successfully decoded. Figure 5 presents the flight trajectories with δ = 10 dB in PES, where the suspicious flight can be tracked more accurately than the one with δ = 20 dB. The reason is that a lower δ in PES leads to a larger number of successfully eavesdropped packets on UAV_{ST}.

In fact, although the flight trajectory of the suspicious UAVs in our simulation is fixed, it should be noted that the proposed tracking algorithm is general and can support any flight trajectory since the flight tracking is based on the eavesdropped packet, AOA and RSS of the suspicious transmitter's signal.

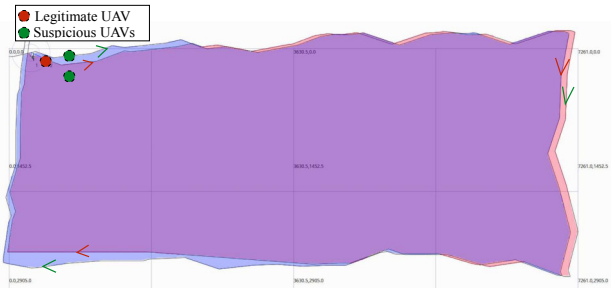

Fig. 4: Tracking flight trajectory, where δ = 20 dB.

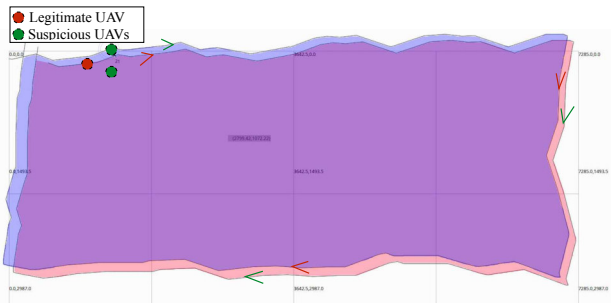

Fig. 5: Tracking flight trajectory, where δ = 10 dB.

V. Conclusion

This paper focuses on the legitimate UAV surveillance, where the legitimate UAV tracks suspicious UAVs' flight for preventing intended crimes and terror attacks. To enhance tracking accuracy, the legitimate UAV proactively eavesdrops suspicious UAVs' communication via sending jamming signals. The legitimate tracking algorithm is studied to comprehensively utilize the eavesdropped packets, angle-of-arrival and received signal strength of the suspicious transmitter's signal. Moreover, we developed a new co-simulation framework, JAMSIM, to evaluate the wireless surveillance performance of PES working with LTA in UAV communications.

ACKNOWLEDGEMENTS

This work was partially supported by National Funds through FCT/MCTES (Portuguese Foundation for Science and Technology), within the CISTER Research Unit (CEC/04234); also by the Operational Competitiveness Programme and Internationalization (COMPETE 2020) through the European Regional Development Fund (ERDF) and by national funds through the FCT, within project POCI-01-0145-FEDER-029074 (ARNET).

REFERENCES

[1] N. H. Motlagh, M. Bagaa, and T. Taleb, "UAV-based IOT platform: A crowd surveillance use case," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 128–134, 2017.

[2] L. Gupta, R. Jain, and G. Vaszkun, "Survey of important issues in UAV communication networks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1123–1152, 2016.

[3] (2017, April) Homeland security in united states. [Online]. Available: https://en.wikipedia.org/wiki/Homeland_security

[4] C. C. Haddal and J. Gertler, "Homeland security: Unmanned aerial vehicles and border surveillance." DTIC Document, 2010.

[5] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[6] R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 1023–1043, 2015.

[7] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[8] K. Li, R. C. Voicu, S. S. Kanhere, W. Ni, and E. Tovard, "Energy efficient legitimate wireless surveillance of UAV communications," *IEEE Transactions on Vehicular Technology*, 2019.

[9] J. Xu, K. Li, L. Duan, and R. Zhang, "Proactive eavesdropping via jamming over HARQ-based communications," in *IEEE Global Communications Conference (GLOBECOM)*, 2017.

[10] X. Wang, D. Li, C. Guo, X. Zhang, S. S. Kanhere, K. Li, and E. Tovar, "Eavesdropping and jamming selection policy for suspicious UAVs based on low power consumption over fading channels," *Sensors*, vol. 19, no. 5, p. 1126, 2019.

[11] I. Guvenc, F. Koohifar, S. Singh, M. L. Sichitiu, and D. Matolak, "Detection, tracking, and interdiction for amateur drones," *IEEE Communications Magazine*, vol. 56, no. 4, pp. 75–81, 2018.

[12] A. Chamseddine, O. Akhrif, G. Charland-Arcand, F. Gagnon, and D. Couillard, "Communication relay for multiground units with unmanned aerial vehicle using only signal strength and angle of arrival," *IEEE Transactions on Control Systems Technology*, vol. 25, no. 1, pp. 286–293, 2017.

[13] F. Koohifar, A. Kumbhar, and I. Guvenc, "Receding horizon multi-UAV cooperative tracking of moving RF source," *IEEE Communications Letters*, 2016.

[14] N. Okello, F. Fletcher, D. Musicki, and B. Ristic, "Comparison of recursive algorithms for emitter localisation using TDOA measurements from a pair of UAVs," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 47, no. 3, pp. 1723–1732, 2011.

[15] K. Li, M. I. Akbaş, D. Turgut, S. S. Kanhere, and S. Jha, "Reliable positioning with hybrid antenna model for aerial wireless sensor and actor networks," in *Wireless Communications and Networking Conference (WCNC)*. IEEE, 2014, pp. 2904–2909.

[16] M. R. Brust, M. I. Akbas, and D. Turgut, "VBCA: A virtual forces clustering algorithm for autonomous aerial drone systems," *arXiv preprint arXiv:1607.05048*, 2016.

[17] J. Rentrope and M. I. Akbaş, "Spatially adaptive positioning for molecular geometry inspired aerial networks," in *Proceedings of the 6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications*. ACM, 2017, pp. 1–8.

[18] A. Chakrabarty, R. Morris, X. Bouyssounouse, and R. Hunt, "Autonomous indoor object tracking with the parrot AR. drone," in *International Conference on Unmanned Aircraft Systems (ICUAS)*. IEEE, 2016, pp. 25–30.

[19] M. Izadi, A. K. Sanyal, R. Beard, and H. Bai, "GPS-denied relative motion estimation for fixed-wing UAV using the variational pose estimator," in *Annual Conference on Decision and Control (CDC)*. IEEE, 2015, pp. 2152–2157.

[20] L. Mejias, S. McNamara, J. Lai, and J. Ford, "Vision-based detection and tracking of aerial targets for UAV collision avoidance," in *International Conference on Intelligent Robots and Systems (IROS)*. IEEE, 2010, pp. 87–92.

[21] Z. Li, N. Hovakimyan, V. Dobrokhodov, and I. Kaminer, "Vision-based target tracking and motion estimation using a small UAV," in *International Conference on Decision and Control (CDC)*. IEEE, 2010, pp. 2505–2510.

[22] K. Li, W. Ni, X. Wang, R. P. Liu, S. S. Kanhere, and S. Jha, "Energy-efficient cooperative relaying for unmanned aerial vehicles," *IEEE Transactions on Mobile Computing*, vol. 15, no. 6, pp. 1377–1386, 2016.

[23] K. Li, W. Ni, X. Wang, R. P. Liu, S. S. Kanhere, and S. Jha, "EPLA: Energy-balancing packets scheduling for airborne relaying networks," in *IEEE International Conference on Communications (ICC)*, 2015, pp. 6246–6251.

[24] X. Wang, K. Li, S. S. Kanhere, D. Li, X. Zhang, and E. Tovar, "PELE: Power efficient legitimate eavesdropping via jamming in uav communications," in *International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE, 2017, pp. 402–408.

[25] N. Ahmed, S. S. Kanhere, and S. Jha, "Utilizing link characterization for improving the performance of aerial wireless sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 8, pp. 1639–1649, 2013.

[26] C. Luo, S. I. McClean, G. Parr, L. Teacy, and R. De Nardi, "UAV position estimation and collision avoidance using the extended kalman filter," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 6, pp. 2749–2762, 2013.

[27] Z. Pan, Q. Xu, C. Chen, and X. Guan, "NS3-MATLAB co-simulator for cyber-physical systems in smart grid," in *Chinese Control Conference (CCC)*. IEEE, 2016, pp. 9831–9836.