



**RADIO SCIENCE
FOR HUMANITY**

A State of the Art of Drone (In)Security (In)Sécurité des drones : un état de l'art

Yves Roudier¹, Tullio Joseph Tanzi²

¹ I3S – CNRS - Université de Nice Sophia Antipolis, yves.roudier@unice.fr

² Institut Mines-Telecom, Telecom ParisTech, tullio.tanzi@telecom-paristech.fr

Keywords (in English and French): Drone, System and Network Security, Safety and Security Requirements, Logical Attacker Models.

Les drones ou UAV constituent aujourd'hui un outil de premier plan dans la collecte d'information à distance [1], dans des lieux d'accès difficile ou dangereux. Collecter l'information joue par exemple un rôle clé dans la gestion des catastrophes naturelles et l'organisation des secours et pour améliorer l'évaluation d'un contexte de crise. Les drones actuels étendent notamment les capacités des équipes de secours dans les tâches de collecte de données dans un contexte difficile. Des drones peuvent par exemple être transportés et déployés pour explorer certaines zones d'inondation afin de trouver un chemin praticable pour rejoindre les sinistrés [2]. Ils étendent ainsi les capacités d'exploration des équipes de secours dans risquer leur propre sécurité [3]. Dans ce domaine également, la présence de fonctions de détection [4] de plus en plus avancées couplée à l'arrivée de mécanismes autonomes intégrera naturellement les prochaines générations de drones aux opérations de recherche en déchargeant les secouristes de ces tâches. Pour concrétiser ces perspectives, deux défis doivent être abordés. Le premier est d'atteindre un degré d'autonomie suffisant pour ces véhicules, tant en termes de navigation que d'interprétation des données détectées. Le second concerne la fiabilité de l'engin et sa robustesse face aux agressions d'origine accidentelles ou malveillantes. Des contraintes juridiques et éthiques nombreuses en ce qui concerne les victimes et les sauveteurs découlent des risques potentiels encourus par l'utilisation d'un drone, en présence de ces deux défis.

Cet article discute des problèmes de sécurité informatique des drones, notamment dans le contexte de plusieurs scénarios humanitaires. Un état de l'art des attaques dans ce domaine est présenté. Nous discutons notamment :

- L'injection de fausses commandes afin de prendre le contrôle de l'UAV. Ces attaques peuvent entraîner des risques graves en ce qui concerne la sécurité des vols par exemple. Au-delà du détournement, un drone peut être accidenté volontairement et est susceptible d'entraîner des dommages et de causer des victimes supplémentaires, notamment du fait du domaine de vol à basse altitude de ces engins ;
- L'accès frauduleux aux données de télémétrie et le piratage des données de télédétection. Les données stockées dans l'engin devront également être protégées afin d'empêcher leur exploitation si le drone est détourné pour une raison quelconque. Les données stockées à bord des drones sont particulièrement sensibles en ce qui concerne les victimes. On a vu par le passé l'utilisation de clichés de personnes identifiables qui ont fait la une des journaux sans leur accord ;
- L'injection de données fabriquées dans le système afin de modifier le cours des opérations de recherche et de sauvetage, et par exemple d'en réduire l'efficacité et de les désorganiser. Ces injections peuvent avoir lieu par envoi de messages fabriqués ou par l'accès direct au drone par interception physique ;
- Le déni de service afin de nuire à ces mêmes opérations, notamment en réduisant les possibilités de communication avec le drone.

On voit que les drones doivent englober les dimensions sécurité et vie privée dès leur conception. Nous faisons également le point sur les techniques permettant d'assurer la sécurité de ces systèmes par le déploiement de mécanismes, notamment cryptographiques, tant au niveau des communications que du stockage des données acquises. Intégrer ces mécanismes requiert aussi de revoir la conception de l'architecture d'un tel système. Un drone constitue avant tout un système communicant qui nécessite aujourd'hui la mise en œuvre d'un centre de contrôle déployé par les unités mobiles sur site ou par la cellule chargée des secours. Les communications entre ce centre de contrôle et les drones doivent être sécurisées afin d'éviter toute interférence indésirable, notamment

empêcher les accès non autorisés aux données sensibles et détecter des anomalies de communication (écrasement de l'UAV, brouillage radio, etc.). Plusieurs études et preuves de concept ont d'ailleurs montré les vulnérabilités des systèmes actuels [5,6,7] dans ce domaine. Pour contrer ces attaques, la source des messages (UAV ou centre de contrôle) doit être authentifiée et l'intégrité des messages être vérifiée. Étant donné que la plupart des communications s'appuie sur différents modules existants de communication axée sur la radio, déployer des mécanismes de sécurité peut nécessiter une couche d'adaptation en interface des fonctionnalités de communication. Les contre-mesures de sécurité peuvent également impliquer des modifications de la télécommande afin d'authentifier les commandes transmises au drone ou de détecter toute tentative d'intrusion. Plusieurs propositions ont aussi suggéré l'utilisation de flottes de drones pour déployer une véritable infrastructure de relais de radio mobile afin d'étendre les capacités de communication disponibles ou mettant en œuvre des communications opportunistes et tolérantes aux délais. Dans ces deux derniers cas de figure, des mécanismes de protection adaptés devraient également être introduits afin d'éviter intrusions et déni de service. Par ailleurs, l'architecture interne d'un drone est également vulnérable à des attaques sur l'intégrité de son programme qui peuvent nécessiter des mécanismes de détection d'intrusion.

Les données recueillies sont aussi susceptibles d'attaques comme décrit plus haut [5,6]. Les drones sont généralement équipés de différents types de capteurs, notamment optiques [8] ou radiométriques, selon leur mission. Ces instruments peuvent être bernés par des attaques spécifiques qui peuvent nécessiter des contre-mesures basées sur la corrélation des données acquises depuis plusieurs capteurs. Ils permettent par ailleurs de détecter sans ambiguïté et localiser des personnes, les compter, évaluer leur âge, etc. L'accès à de telles données doit évidemment être contrôlé. Cela concerne les communications en vol, mais aussi celles stockées dans l'appareil. En effet, en cas de collision ou de panne, ces données ne doivent pas être récupérables par un tiers. Ces données peuvent présenter des aspects commerciaux ou avoir des implications politiques. Elles ne doivent pas être détournées par des tiers et aboutir à une entrave pour les opérations de secours. Le respect de la vie privée, notamment vis-à-vis des victimes, nécessite que toute information acquise lors d'une catastrophe soit contrôlée. Ces objectifs sont exécutés simultanément par l'intermédiaire d'algorithmes cryptographiques assurant la confidentialité et permettant de vérifier l'intégrité de contenus.

Pour finir, le développement et l'intégration des caractéristiques d'autonomie du drone sont essentielles pour déployer cette technologie à plus large échelle sans nécessiter l'intervention de personnels spécialisés et dédiés. D'autre part, dans de nombreuses circonstances, le drone pourra être dans l'incapacité de communiquer avec le centre de contrôle, soit en raison d'interférences, sporadiques ou prolongée, par exemple dans le cas d'exploration du terrain derrière des obstacles ou au-delà de la portée des relais radio ou encore dans un contexte de déni de service volontaire. Les mécanismes de décision autonomes doivent être validés vis-à-vis de scénarios d'attaques qui pourraient modifier le comportement du drone.

L'article sera rédigé en anglais.

References

- [1] Tanzi T. J., Roudier Y. and Apvrille L., (2015), "Towards a new architecture for autonomous data collection", *Int. Arch. Photogramm. Remote Sens. Spatial Inf. Sci.*, vol. XL-3/W3, pp. 363-369.
- [2] F. Lefevre and T. Tanzi, "International Union of Radio Science, International Council for Science (ICSU), Joint Board of Geospatial Information Societies (jBGIS)," in *United Nations office for outer Space Affairs (OOSA)*, 2013.
- [3] T. Tanzi and F. Lefevre, "The Contribution of Radio Sciences to Disaster Management," in *International Symposium on Geo-information for disaster management (Gi4DM 2011)*, Antalya, Turkey, 2011.
- [4] T. Tanzi, M. Chandra, J. Isnard, D. Camara, O. Sebastien, F. Harivelo: Towards "Drone-Borne" Disaster Management: Future Application Scenarios. 06/2016; III-8:181-189. DOI:10.5194/isprs-annals-III-8-181-2016.
- [5] Kim Hartmann and Christoph Steup. The Vulnerability of UAVs to CyberAttacks - An Approach to the Risk Assessment. 5th International Conference on Cyber Conflict, K. Podins, J. Stinissen, M. Maybaum (Eds.), 2013 © NATO CCD COE Publications, Tallinn.
- [6] Alan Kim, Brandon Wampler, James Goppert, Inseok Hwang and Hal Aldridge. Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles. American Institute of Aeronautics and Astronautics.
- [7] Oleg Petrovsky. Attack on the drones: security vulnerabilities of unmanned aerial vehicles. VB2015 (The Virus Bulletin Conference). Wednesday 30 September 2015, Prague, Czech Republic.
- [8] P. Wilkinson and D. Cole, "The Role of the Radio Sciences in the Disaster Management," *Radio Science Bulletin*, vol. 3358, pp. 45-51, 2010.