Analysis and design of stealthy cyber attacks on unmanned aerial systems

Abstract

Cyber security has emerged as one of the most important issues in unmanned aerial systems for which the functionality heavily relies on onboard automation and intervehicle communications. In this paper, potential cyber threats and vulnerabilities in the unmanned aerial system's state estimator to stealthy cyber attacks are identified, which can avoid being detected by the monitoring system. Specifically, this paper investigates the worst stealthy cyber attack that can maximize the state estimation error of the unmanned aerial system's state estimator while not being detected. First, the condition that the system is vulnerable to the stealthy cyber attacks is derived, and then an analytical method is provided to identify the worst stealthy cyber attack. The proposed cyber attack analysis methods are demonstrated with illustrative examples of an onboard unmanned aerial system navigation system and an unmanned aerial system tracking application. 

Indexed keywords

Air navigation, Crime, Estimation, Navigation systems, State estimation, Analytical method, Cyber security, Cyber threats, Cyber-attacks, Inter vehicle communications, Monitoring system, State Estimators, Unmanned aerial systems, Computer crime

Cardenas, A., Amin, S., Sastry, S. Research challenges for the security of control systems (2008) 3rd USENIX Workshop on Hot Topics in Security. Cited 237 times. USENIX Association, Berkeley, CA, July, Paper 6

Cárdenas, A.A., Amin, S., Sastry, S. Secure control: Towards survivable cyber-physical systems (2008) Proceedings - International Conference on Distributed Computing Systems, art. no. 4577833, pp. 495-500. Cited 398 times. ISBN: 978-076953173-1 doi: 10.1109/ICDCS.Workshops.2008.40

Clapper, J.R., Young, J.J., Cartwright, J.E., Grimes, J.G. (2007) Unmmaned Systems Roadmap 2007-2032. Cited 193 times. U.S. Dept. of Defense Secretaries of the Military Depts. Memo, Dec

Donley, M.B., Schwartz, N.A. (2009) United States Air Force Unmanned Aircraft Systems Flight Plan 2009-2047. Cited 57 times. U.S. Air Force, TR, May

Herwitz, S.R., Berthold, R., Dunagan, S., Sullivan, D., Fladeland, M., Brass, J.A. UAV homeland security demonstration (2004) Collection of Technical Papers - AIAA 3rd "Unmanned-Unlimited" Technical Conference, Workshop, and Exhibit, 1, art. no. AIAA 2004-6473, pp. 396-400. Cited 7 times. ISBN: 1563477173; 978-156347717-1

Avižienis, A., Laprie, J.-C., Randell, B., Landwehr, C. Basic concepts and taxonomy of dependable and secure computing (2004) IEEE Transactions on Dependable and Secure Computing, 1 (1), pp. 11-33. Cited 2885 times. doi: 10.1109/TDSC.2004.2

Saltzer, J.H., Schroeder, M.D. The Protection of Information in Computer Systems (1975) Proceedings of the IEEE, 63 (9), pp. 1278-1308. Cited 1086 times. doi: 10.1109/PROC.1975.9939

Ahmed, T., Tripathi, A.R. Security policies in distributed CSCW and workflow systems (2010) IEEE Transactions on Systems, Man, and Cybernetics Part A:Systems and Humans, 40 (6), art. no. 5464271, pp. 1220-1231. Cited 18 times. doi: 10.1109/TSMCA.2010.2046727

Ding, S.X. Model-based fault diagnosis techniques: Design schemes, algorithms, and tools (2008) Model-based Fault Diagnosis Techniques: Design Schemes, Algorithms, and Tools, pp. 1-473. Cited 1463 times. http://www.springerlink.com/openurl.asp?genre=book&isbn=978-3-540-76303-1 ISBN: 978-354076303-1 doi: 10.1007/978-3-540-76304-8

(2011) Flying Operations of Remotely Piloted Aircraft Unaffected by Malware. Cited 3 times. U.S. Air Force Space Command Release 021011, Oct. [retrieved 2014] www.afspc.af.mil/news/story.asp?id=123275647

Warner, J.S., Johnston, R.G. (2003) GPS Spoofing Countermeasures. Cited 34 times. Los Alamos National Lab., TR LAUR-03-6163, Los Alamos, NM

Nicol, D.M., Sanders, W.H., Trivedi, K.S. Model-based evaluation: From dependability to security (2004) IEEE Transactions on Dependable and Secure Computing, 1 (1), pp. 48-64. Cited 343 times. doi: 10.1109/TDSC.2004.11

Ten, C.-W., Manimaran, G., Liu, C.-C. Cybersecurity for critical infrastructures: Attack and defense modeling (2010) IEEE Transactions on Systems, Man, and Cybernetics Part A:Systems and Humans, 40 (4), art. no. 5477189, pp. 853-865. Cited 200 times. doi: 10.1109/TSMCA.2010.2048028

Gligor, V.D. A Note on Denial-of-Service in Operating Systems (1984) IEEE Transactions on Software Engineering, SE-10 (3), pp. 320-324. Cited 62 times. doi: 10.1109/TSE.1984.5010241

Amin, S., Schwartz, G.A., Shankar Sastry, S. Security of interdependent and identical networked control systems (2013) Automatica, 49 (1), pp. 186-192. Cited 95 times. doi: 10.1016/j.automatica.2012.09.007

Zhu, Q., Başar, T. Robust and resilient control design for cyber-physical systems with an application to power systems (2011) Proceedings of the IEEE Conference on Decision and Control, art. no. 6161031, pp. 4066-4071. Cited 99 times. ISBN: 978-161284800-6 doi: 10.1109/CDC.2011.6161031

Gupta, A., Langbort, C., Başar, T. Optimal control in the presence of an intelligent jammer with limited actions (2010) Proceedings of the IEEE Conference on Decision and Control, art. no. 5717544, pp. 1096-1101. Cited 125 times. ISBN: 978-142447745-6 doi: 10.1109/CDC.2010.5717544

Mo, Y., Sinopoli, B. False data injection attacks in control systems (2010) First Workshop on Secure Control Systems. Cited 111 times. Team for Research in Ubiquitous Secure Technology (TRUST) Center and the Idaho National Laboratory (INL), April, Paper 7

Liu, Y., Ning, P., Reiter, M.K. False data injection attacks against state estimation in electric power grids (2009) Proceedings of the ACM Conference on Computer and Communications Security, pp. 21-32. Cited 710 times. ISBN: 978-160558352-5 doi: 10.1145/1653662.1653666

Teixeira, A., Amin, S., Sandberg, H., Johansson, K.H., Sastry, S.S. Cyber security analysis of state estimators in electric power systems (2010) Proceedings of the IEEE Conference on Decision and Control, art. no. 5717318, pp. 5991-5998. Cited 231 times. ISBN: 978-142447745-6 doi: 10.1109/CDC.2010.5717318

Amin, S., Litrico, X., Sastry, S., Bayen, A.M. Cyber security of water scada systems-part I: Analysis and experimentation of stealthy deception attacks (2013) IEEE Transactions on Control Systems Technology, 21 (5), art. no. 6303885, pp. 1963-1970. Cited 141 times. doi: 10.1109/TCST.2012.2211873

Mo, Y., Garone, E., Casavola, A., Sinopoli, B. False data injection attacks against state estimation in wireless sensor networks (2010) Proceedings of the IEEE Conference on Decision and Control, art. no. 5718158, pp. 5967-5972. Cited 182 times. ISBN: 978-142447745-6 doi: 10.1109/CDC.2010.5718158

Sandberg, H., Teixeira, A., Johansson, K. On security indices for state estimators in power networks (2010) 1st Workshop on Secure Control Systems. Cited 182 times. Team for Research in Ubiquitous Secure Technology (TRUST) Center and the Idaho National Laboratory (INL), Paper 8

Pasqualetti, F., Dorfler, F., Bullo, F. Attack detection and identification in cyber-physical systems (2013) IEEE Transactions on Automatic Control, 58 (11), art. no. 6545301, pp. 2715-2729. Cited 659 times. doi: 10.1109/TAC.2013.2266831

Javaid, A.Y., Sun, W., Devabhaktuni, V.K., Alam, M. Cyber security threat analysis and modeling of an unmanned aerial vehicle system (2012) 2012 IEEE International Conference on Technologies for Homeland Security, HST 2012, art. no. 6459914, pp. 585-590. Cited 84 times. ISBN: 978-146732708-4 doi: 10.1109/THS.2012.6459914

Rudinskas, D., Goraj, Z., Stankunas, J. Security analysis of uav radio communication system (2009) Aviation, 13 (4), pp. 116-121. Cited 9 times. doi: 10.3846/1648-7788.2009.13.116-121

Kim, A., Wampler, B., Goppert, J., Hwang, I., Aldridge, H. Cyber attack vulnerabilities analysis for unmanned aerial vehicles (2012) AIAA Infotech at Aerospace Conference and Exhibit 2012. Cited 54 times. ISBN: 978-160086939-6

Goppert, J., Liu, W., Shull, A., Sciandra, V., Hwang, I., Aldridge, H. Numerical analysis of cyberattacks on unmanned aerial systems (2012) AIAA Infotech at Aerospace Conference and Exhibit 2012. Cited 8 times. ISBN: 978-160086939-6

Goppert, J., Shull, A., Sathyamoorthy, N., Liu, W., Hwang, I., Aldridge, H. Software/hardware-in-the-loop analysis of cyberattacks on unmanned aerial systems (2014) Journal of Aerospace Information Systems, 11 (5), pp. 337-343. Cited 9 times. http://arc.aiaa.org/doi/pdf/10.2514/1.I010114 doi: 10.2514/1.I010114

Hwang, I., Kim, S., Kim, Y., Seah, C.E. A survey of fault detection, isolation, and reconfiguration methods (2010) IEEE Transactions on Control Systems Technology, 18 (3), art. no. 5282515, pp. 636-653. Cited 786 times. doi: 10.1109/TCST.2009.2026285

Chetouani, Y. Using the Kalman filtering for the Fault Detection and Isolation (FDI) in the nonlinear dynamic processes (2008) International Journal of Chemical Reactor Engineering, 6, art. no. A43. Cited 10 times.

Xue, W., Guo, Y.-Q., Zhang, X.-D. Application of a bank of Kalman filters and a Robust Kalman filter for aircraft engine sensor/actuator fault diagnosis (2008) International Journal of Innovative Computing, Information and Control, 4 (12), pp. 3161-3168. Cited 39 times.

Malladi, D.P., Speyer, J.L. A generalized Shiryayev sequential probability ratio test for change detection and isolation (1999) IEEE Transactions on Automatic Control, 44 (8), pp. 1522-1534. Cited 96 times. doi: 10.1109/9.780416

Nikiforov, I.V. A Generalized Change Detection Problem (1995) IEEE Transactions on Information Theory, 41 (1), pp. 171-187. Cited 115 times. doi: 10.1109/18.370109

Dionne, D., Michalska, H., Oshman, Y., Shinar, J. Novel adaptive generalized likelihood ratio detector with application to maneuvering target tracking (2006) Journal of Guidance, Control, and Dynamics, 29 (2), pp. 465-474. Cited 17 times. doi: 10.2514/1.13447

Gertler, J.J. Survey of Model-Based Failure Detection and Isolation in Complex Plants (1988) IEEE Control Systems Magazine, 8 (6), pp. 3-11. Cited 723 times. doi: 10.1109/37.9163

Strang, G. (1976) Linear Algebra and Its Applications, pp. 311-330. Cited 53 times. Thomson Brooks/Cole, Pacific Grove, CA

Boyd, S., Vandenberghe, L. (2004) Convex Optimization, pp. 215-231. Cited 31331 times. Cambridge Univ. Press New York

Titterton, D., Weston, J. (2004) Strapdown Inertial Navigation Technology, pp. 377-418. Cited 162 times. AIAA Reston VA

(2011) Concept of Operations for the Next Generation Air Transportation System. Cited 489 times. Ver. 3.2. Joint Planning and Development Office TR

Oh, S., Hwang, I., Sastry, S. Distributed multitarget tracking and identity management (2008) Journal of Guidance, Control, and Dynamics, 31 (1), pp. 12-29. Cited 9 times. http://pdf.aiaa.org/getfile.cfm?urlX=%2D%3CWI%277D%2FQKS%2B%29SPOJV%40%20%20%0A&urla=%26%2A%22L%20%23%20%2AC%0A&urlb=%21%2A%20%20%20%0A&urlc=%21%2A0%20%20%0A&urld=%21%2A0%20%20%0A&urle=%27%2B2%28%27%21%40JJU%40%20%20%0A doi: 10.2514/1.26237

Bar-Shalom, Y., Li, X.R., Kirubarajan, T. (2001) Estimation with Applications to Tracking and Navigation, pp. 277-293. Cited 5383 times. Wiley, New York

Seah, C.E., Hwang, I. Stochastic linear hybrid systems: Modeling, estimation, and application in air traffic control (2009) IEEE Transactions on Control Systems Technology, 17 (3), pp. 563-575. Cited 54 times. doi: 10.1109/TCST.2008.2001377