MOKSLAS – LIETUVOS ATEITIS
SCIENCE – FUTURE OF LITHUANIA

2009, 1 tomas, Nr. 6
2009, Vol. 1, No. 6

Transporto inžinerija
Transport Engineering

Aviacijos technologijos
Aviation Technologies

BEPILOČIŲ ORLAIVIŲ RADIJO RYŠIO SISTEMŲ ANALIZĖ

Darius Rudinskas[1], Jonas Stankūnas[2]

Vilniaus Gedimino technikos universitetas
El. paštas: [1]darius.rudinskas@vgtu.lt; [2]jonas.stankunas@vgtu.lt

Santrauka. Straipsnyje nagrinėjami radijo ryšiu perduodamos informacijos saugumo klausimai. Ypač svarbi radijo ryšiu perduodamos informacijos apsauga, kuriant bepiločius orlaivius (toliau tekste – BO) ir kitas nuotolinio valdymo transporto priemones. Straipsnyje pateikiama bepiločių orlaivių ryšių sistemos struktūra, galimos grėsmės informacijos perdavimui, saugumui bei integralumui, radijo ryšio sistemos apsaugos būdai ir priemonės.

Reikšminiai žodžiai: bepilotis orlaivis, saugumas, radijo ryšio sistema.

Įvadas

Bepiločiai orlaiviai naudojami skirtingiems tikslams: kariniams, aplinkos stebėjimui, transportui, ryšių centrai, įstatymų vykdymo priežiūrai (UAVNET 2006). BO valdymui, telemetrijos ir kitų duomenų perdavimui naudojama radijo ryšio sąsaja. Naudojantis radijo ryšiu neišvengiamai susiduriama su grėsmėmis: radijo ryšio, perduodamų duomenų, valdymo informacijos praradimu arba tyčine išorine intervencija. Norint išvengti šių nepageidaujamų pasekmių, būtina imtis informacijos apsaugos priemonių (Rudinskas *et al.* 2008). Darbe analizuojamos BO radijo ryšio sistemos problemos, potencialios grėsmės ir galimi sprendimo būdai.

Sistemos aprašymas

BO priklausomai nuo paskirties ir konfigūracijos gali komunikuoti su antžemine stotimi ar kitais bepiločiais skraidymo aparatais, taip pat gali priimti duomenis iš skirtingų informacijos šaltinių (GPS, meteorologinių stočių, duomenų centrų) (Torun 1999). Apibendrinta radijo ryšio schema matyti 1 pav.

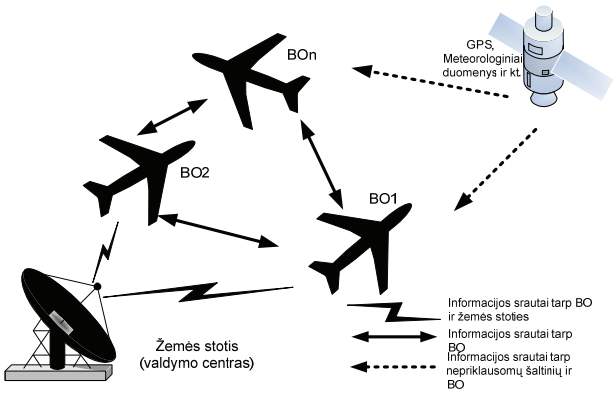
Orlaivio ryšių sistema „žemė-oras" naudojama informacijos perdavimui tarp žemės kontrolės stoties ir BO. Šie ryšio kanalai naudojami BO perduodant valdymo komandas, telemetrijos duomenis ar kitą informaciją.

Radijo ryšio saugumo pažeidimo grėsmės

Radijo ryšiu perduodant informaciją susiduriama su dviejų tipų grėsmėmis: nuo žmogaus veiklos nepriklausančios grėsmės ir nuo žmogaus veiklos priklausančios grėsmės (2 pav.).

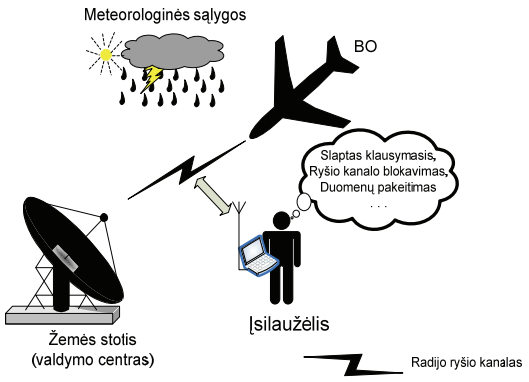
Vienas iš paminėtų grėsmių tipų yra nuo žmogaus veiklos nepriklausančios grėsmės – natūralūs gamtos reiškiniai, kurie turi įtakos radijo ryšio kokybei, bet ne perduodamos informacijos saugumui. Tai yra BO skrydžio metu besikeičiančios oro sąlygos (2 pav.).

Nuo žmogaus veiklos priklausančios grėsmės yra šios: ryšių kanalo klausymasis, informacijos pakeitimas arba sugadinimas, ryšių kanalo blokavimas (2 pav.).



1 pav. Informacijos srautai tarp skirtingų sistemų

Fig. 1. Information flows between different systems



2 pav. Potencialios grėsmės

Fig. 2. Potential treats

ISSN 2029-2341 print / ISSN 2029-2252 online
DOI: 10.3846/mla.2009.6.26

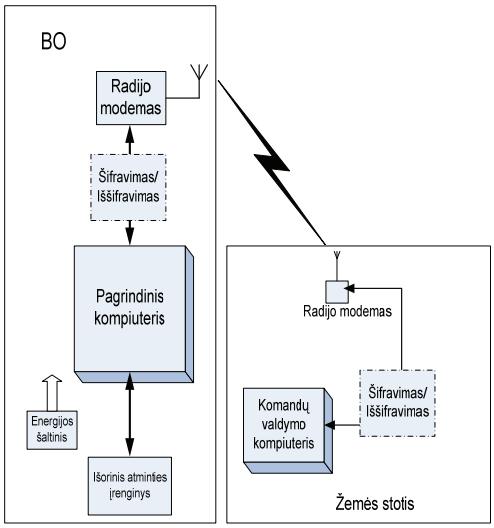
Nepaisant BO paskirties, reikia imtis informacijos apsaugos priemonių. Tai daryti būtina, nes kaip buvo minima anksčiau, perduodamos informacijos sugadinimas gali turėti tiesioginės įtakos BO veikimui arba surinkta informacija gali būti panaudota kitų išpuolių prieš BO metu.

Informacijos apsaugos priemonės

Įsilaužėliui bandant manipuliuoti perduodamais duomenimis, juos paslepiant, pakeičiant valdymo komandas ar duomenis apie orlaivio techninę būklę, atsiranda grėsmė BO saugumui ir misijos sėkmei. Manipuliacijos gali būti atliekamos pakeičiant ar blokuojant duomenis jų perdavimo metu. Todėl orlaivyje turi būti integruota atitinkama realiu laiku veikianti atakų ir kitokius neteisėtus duomenų pakeitimus stebinti įranga.

Nepaisant to, kad BO saugai svarbi informacija yra apsaugoma, įsilaužėlis vis dar gali sumažinti BO saugumo ribas. Be to, įsilaužėlis gali pasyviai klausytis radijo ryšio kanalo, taip nesukeldamas tiesioginio pavojaus BO funkcionalumui kaupti informaciją ateities atakoms.

Informacijos apsaugai naudojamos fizinės ir loginės (programinės) apsaugos priemonės (Torun 1999). Fizinės apsaugos priemonės yra techninė apsauga, fizinė duomenų kaupyklų apsauga bei kontroliuojama prieiga prie jų. Loginės apsaugos priemonės apima labai plačią priemonių sritį: tai informacijos kodavimas, sudėtingi duomenų perdavimo protokolai bei šifravimo algoritmai. Visos informacijos apsaugos priemonės gali būti integruojamos į radijo ryšio sistemą. Apibendrinta BO radijo ryšio sistema matyti 3 pav.



3 pav. Apibendrinta bepiločio orlaivio radijo ryšio funkcinė schema

Fig. 3. Structure summary of UAV radio communication system

Siekiant sumažinti minėtas grėsmes, siūlomos šios saugumo rekomendacijos ir priemonės:

- Radijo kanalo patikimumo užtikrinimas – radijo ryšio kokybė skrendant priklauso nuo daugelio faktorių: radijo ryšiui naudojamų dažnių, atstumo, išorinio triukšmo intensyvumo, orlaivio padėties erdvėje. Siekiant užtikrinti radijo ryšio kokybę ir patikimumą tikslinga naudoti dubliuojančius imtuvus, kurių antenų poliarizacijos plokštumos yra statmenos viena kitai. Esant nepakankamai radijo signalo kokybei, imtuvas automatiškai signalą priima iš tos antenos, kurią pasiekia reikiamos kokybės signalas. Naudojant aukšto dažnio (GHz bangų ruožas) imtuvus, priimamo signalo poliarizacija yra ypač aktuali, todėl reikiamos antenos padėties užtikrinimui rekomenduojama naudoti dubliuojančius imtuvus, kurių antenos išdėstytos skirtingose orlaivio vietose ir yra statmenos viena kitai (Viero *et al.* 2007). Kitas svarbus momentas yra medžiagos, iš kurių pagamintas BO korpusas. Jei korpusas gaminamas iš metalo lakšto ar anglies pluošto, kurie yra geri elektromagnetinių bangų ekranai, o įrengti antenas korpuso išorėje nėra galimybės, būtina įrengti elektromagnetinėms bangoms laidžius „langus" (pavyzdžiui, stiklo pluoštas);
- Integralumas – BO radijo ryšio kanalas turi būti apsaugotas nuo neautorizuoto duomenų pakeitimo, pavyzdžiui, valdymo komandų ar telemetrijos duomenų pakeitimas. Vadinasi iš BO priimti duomenys turi būti identiški jo sukurtiems duomenims (Robinson *et al.* 2007a);
- Autentiškumas – BO turi būti apsaugotas nuo neautorizuotos antžeminės stoties siunčiamų klaidinančių duomenų srauto. Siekiant užkirsti kelią išorės atakoms, duomenis gavęs BO privalo turėti galimybę patikrinti tiek duomenų šaltinio, tiek ir pranešimo autentiškumą. Norint išvengti klaidinančių antžeminių stočių, BO gali būti integruoti skirtingi autentiškumą patvirtinantys sprendimai, pavyzdžiui, daugumos balsavimo sistema, kartu galinti nustatyti ir duomenų galiojimą (Lazos *et a* . 2005);
- Konfidencialumas – ne visa BO perduodama informacija yra skirta viešam naudojimui – tai BO valdymo komandos, telemetriniai duomenys ir kt. Perduodamos informacijos konfidencialumo užtikrinimas bus aptartas detaliau;
- Kanalo trikdžių mažinimas – įsilaužėlis gali rengti radijo kanalo tarp BO ir antžeminės stoties slopi-

nimą, siekdamas blokuoti arba suvėlinti BO saugai svarbios informacijos perdavimą. Dėl to kanalo slopinimas turi būti nustatomas kiek galima anksčiau. Galimus sprendimus, kaip apsisaugoti nuo ryšio kanalo slopinimo, aprašo M. Li ir kt (2007: 1307–1315);

– Ankstyvas ir tikslus manipuliacijų nustatymas – visos su duomenimis atliekamos neteisėtos manipuliacijos turi būti nustatomos kiek galima greičiau ir tiksliau. Šiam tikslui pasiekti reikia integruoti įsilaužimų nustatymo sistemą, taip pat pats BO turi kaupti įrašus apie visus incidentus.

Konfidencialumo užtikrinimas

Paprasčiausia yra perdavinėti duomenis, naudojant paprastus atviro teksto protokolus, kurie sudaryti iš informacinių bitų laukų: pradžios, duomenų, kontrolinės sumos ir pabaigos bitų (4 pav.).

Šis duomenų perdavimo metodas yra paprastas, bet ne saugus. Taip pat daugeliu atvejų naudojami radijo modemai neturi integruotų informacijos apsaugos priemonių (Confidential… 2005). Siekiant užtikrinti tiek BO, tiek ir antžeminės stoties perduodamos informacijos integralumą, autentiškumą ir konfidencialumą, reikia naudoti kriptografines apsaugos priemones.

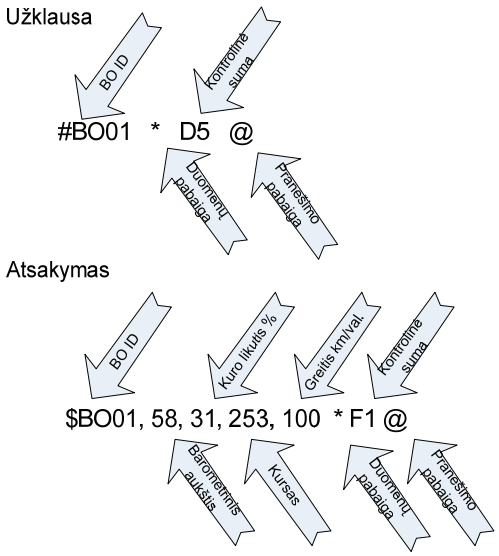
Visos kriptografijos priemonės gali būti integruojamos į ryšio kanalą kaip aparatinė įranga, kaip įterptinis įrankis (3 paveiksle punktyrinės linijos), arba gali būti pagrindiniame BO kompiuteryje įdiegtos programinės priemonės. Ryšio kanale yra paprasta įdiegti aparatines šifravimo priemones, kurios pasižymi didele šifravimo sparta, tačiau tai sukuria ir sunkumų. Pirma, tai yra fizinis įrenginys, kuriam reikalingas energijos šaltinis ir taip pat papildomas svoris. Antra, atliekant skirtingų protokolų konvertavimo procedūras prarandamas laikas, kuris gali turėti įtakos BO saugumui. Programinės priemonės neturi prieš tai aptartų aparatinės įrangos trūkumų, tačiau šifravimo laikas tiesiogiai priklauso nuo pagrindinio procesoriaus technologijos (8, 16, 32 ar daugiau bitų), spartos, atminties talpos ir papildomos integruotos programinės įrangos.

Didžiausią saugumo lygį perduodamai informacijai suteikia asimetrinio šifravimo technologijos. Vienas iš tokių technologinių sprendimų yra skaitmeninio parašo technologija (Li *et al.* 2007, Robinson *et al.* 2007b). Naudojant asimetrinės kriptografijos priemones reikia turėti didelius skaičiavimo ir ryšių pajėgumus, kas yra sunkiai įgyvendinama BO, nes jie turi ribotą energijos šaltinį (bateriją ar kurą). Todėl BO tikslingiau naudoti simetrinio šifravimo technologijas, kurios pasižymi didele duomenų šifravimo sparta bei nesudėtingais realizacijos algoritmais, kurie jau būna realizuoti ryšių įrangoje.

Konfidencialumo užtikrinimui gali būti naudojamos standartinės bevieliuose tinkluose naudojamos priemonės. Viena iš galimų priemonių yra progresyvus šifravimo standartas (AES) (FIPS… 2009). AES turi kelias skirtingas modifikacijas, pvz., AES skaitiklio režimas (*Counter mode AES-CTR*), AES-CCM, AES-CBC-MAC. Naudojamas šifravimo rakto ilgis neturi būti trumpesnis nei 32 bitai.

Naudodami kriptografinius sprendimus galime apsaugoti ne tik perduodamus duomenis, bet ir pagalbinę informaciją (informacijos šaltinį bei gavėją, kontrolinę sumą, pranešimo santrauką). Geriausia yra šifruoti visą duomenų paketą (5 pav.).

Šifravimo procesui reikalingi dideli matematinių skaičiavimų pajėgumai, kurie kartais sunkiai realizuojami sistemoje. Yra sprendimai, kurie leidžia mažoms įterptinėms sistemoms turėti kriptografijos galimybes. Pavyzdžiui, sumaniųjų kortelių technologijoje taikomi duomenų šifravimo sprendimai (ZK-Crypt… 2009).



4 pav. Paprasto protokolo užklausos ir atsakymo žinučių struktūra

Fig. 4. Structure of simple questions and answers messages protocols

$BO01, 58, 31, 253, 100 * F1 @ - Nešifruotas pranešimas

»hвx/tμЦCs"vsЇThЁ¦f©ħцx~¦kђJъ - Šifruotas pranešimas

5 pav. Tiesiog tekste ir AES128 algoritmu šifruotas pranešimas

Fig. 5. Open text message and AES128 ciphered message

Siekiant užtikrinti perduodamos informacijos saugumą, pirmiausia reikia išnagrinėti integruotas apsaugos priemones. Daugelis radijo ryšio sistemų turi integruotas informacijos apsaugos priemones, tačiau paprastai jos yra nustatytos pagal gamyklinius parametrus ir juos būtina pakeisti individualiai konkrečiai ryšio sistemai skirtais parametrais.

Išvados

1. Saugiam bepiločių orlaivių naudojimui būtina užtikrinti perduodamos informacijos saugumą.
2. Mažiausiomis sąnaudomis perduodama informacija apsaugoma taikant duomenų šifravimo principus.
3. Informacijos apsaugos lygis ir duomenų šifravimo priemonės parenkamas atsižvelgiant į bepiločių orlaivių panaudojimo sritį.

Literatūra

FIPS PUB 197: the official AES standard [online] 2009. [cited 25 March 2009]. Available from Internet: <http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.

Li, M.; Koutsopoulos, I.; Poovendran, R. 2007. Optimal jamming attacks and network defense policies in wireless sensor networks, in *IEEE INFOCOM*: 1307–1315.

Lazos, L.; Poovendran, R. 2005. SeRLoc: robust localization for wireless sensor networks, *ACM Transactions on Sensor Networks* 1(1): 73–100. doi:10.1145/1077391.1077395

Confidential & Proprietary [online] 2005. MaxStream, Inc: X stream-PKG-R™ RS232/485 RF Modem – Product Manual. Avi v4. 2B. Available from Internet: <www. maxstream.net>.

Robinson, R. M.; Li, S.; Lintelman, K. *et al*. 2007a. Challenges for IT infrastructure supporting secure network-enabled commercial airplane operations, in *AIAA Infotech@Aerospace Conference.*

Robinson, R.; Li, M.; Sampigethaya, K., *et al*. 2007b. Impact of public key enabled applications on the operation and maintenance of commercial airplanes, in *AIAA ATIO*.

Rudinskas, D.; Stankunas, J. 2008 Analysis of design problems of integrated health management systems in the small aircrafts, in *Proc. of the 8th International Conference on RRDPAE_2008. Brno.*

Torun, E. 1999. UAV Requirements and design consideration, in *RTO MP-44: RTO SCI Symposium on "Warfare Automation: Procedures and Techniques for Unmanned Vehicles"*. Ankara, Turkey.

UAVNET homepage [online], 2006. [cited 25 March 2009]. Available from Internet: < http://www.uavnet.com/>.

Viero, T.; Rounioja, K.; Sipila, T., *et al.* 2007. Dual antenna receivers for high data rate terminals, *Wireless Personal Communications* 43(2): 281–293. doi:10.1007/s11277-006-9221-8

ZK-Crypt Homepage [online] 2009. [cited 25 March 2009]. Available from Internet: <http://www.fortressgb.com/apage/39649.php >.

ANALYSIS OF UNMMANNED AIR VEHICLES COMMUNICATION SYSTEMS

D. Rudinskas, J. Stankunas

Abstract

The analyzed questions of information security transferable by the radio connection link are presented in this article.

This safety it is especially important for design of unmanned air vehicles (UAV) and for other remote control vehicles.

Also questions about UAV communication systems structure, security treats of radio connection system, possible menaces for secure information transferring, security and integrity are discussed in our presentation.

Keywords: Unmanned Air Vehicles, security, radio communication system.