TECHNICKÁ UNIVERZITA V KOŠICIACH
FAKULTA ELEKTROTECHNIKY A INFORMATIKY

# Konferencia UAV 2023

Kód projektu: 313011V422
„Inteligentné operačné a spracovateľské systémy pre UAV“

ISBN 978-80-553-4389-1

2023

## Zborník z konferencie UAV 2023

**Vydavateľ:** Fakulta elektrotechniky a informatiky
Technická univerzita v Košiciach
Letná 9, 040 01 Košice, Slovenská republika

**Dátum vydania:** máj 2023

**Tlač:** 50 kusov CD

**Jazyk:** slovenský, anglický

**Strán:** 86



 **ISBN: 978-80-553-4389-1**

## O konferencii UAV 2023

Projektová konferencia UAV 2023 bola organizovaná na pôde Technickej univerzity v Košiciach, v rámci prezentačných priestorov Univerzitného vedeckého parku TECHNICOM, v dňoch 11. – 12. 5. 2023, v rámci projektu:

| | |
|---|---|
| **Názov projektu:** | Inteligentné operačné a spracovateľské systémy pre UAV |
| **Kód projektu:** | 313011V422 |
| **Prijímateľ NFP:** | GLOBESY, s.r.o. |
| **Partneri:** | Qintec a.s. |
| | YMS, a.s. |
| | Technická univerzita v Košiciach (TUKE) |
| | Žilinská univerzita v Žiline (UNIZA) |

(ďalej len „projekt UAV“).

Projekt UAV je spolufinancovaný z prostriedkov Európskeho fondu regionálneho rozvoja v rámci Operačného programu Integrovaná infraštruktúra.

EURÓPSKA ÚNIA
Európske štrukturálne a investičné fondy
OP Integrovaná infraštruktúra 2014 – 2020

Riadiaci orgán:

MINISTERSTVO DOPRAVY SLOVENSKEJ REPUBLIKY

V zastúpení na základe splnomocnenia:

VÝSKUMNÁ AGENTÚRA

## Obsah

# Bezpečnostná analýza útokov na UAV

[1]*Peter PEKARČÍK*, [2]*Eva CHOVANCOVÁ*

[1]Katedra počitačov a informatiky, Fakulta elektrotechniky a informatiky, Technická univerzita v Košciach, Slovensko
[2]Katedra počitačov a informatiky, Fakulta elektrotechniky a informatiky, Technická univerzita v Košciach, Slovensko

[1]peter.pekarcik@tuke.sk, [2]eva.chovancova@tuke.sk

*Abstract* – **Bezpilotné lietadlá sú dnes veľmi populárne, a to nielen medzi ľuďmi z oblasti IT, ale aj medzi širokou verejnosťou. Tieto zariadenia dokážu fotografovať alebo nahrávať kamerové záznamy z rôznych perspektív a môžu byť prostriedkom na zábavu. Bezpilotné lietadla sú tiež veľkým zdrojom dát. Tieto dáta získavajú z prostredia, ukladajú a posielajú na iné zariadenia, ako sú smartfóny alebo počítače. Smartfóny alebo počítače tiež posielajú údaje o zmene svojej polohy, alebo ďalšie iné údaje na bezpilotné lietadllá. Ale je prenos dát z bezpilotných lietadiel / na bezpilotnélietadla dostatočne bezpečný? Môžeme dôverovaťprenosu dát medzi riadiacou stanicou a bezpilotným lietadlom alebo sú prenášané dáta vystavené potencion riziku?**

*Keywords* – **bezpečnosť, bezpečnostná analýza, Blesa, Bluesmacking, Bluesnarfing, dron, komunikácia, kybernetický útok, MAVLink, protokol, senzor, simulácia, útok, The 'open sesame bug', UAV**

## I. Úvod

Možno mnohých z Vás zaujala skratka UAV v názve článku a otvorili ste ho len preto, lebo nemáte žiadnu predstavu o čo ide. Možno očakávate predstavenie novej technológie alebo nového prístupu v oblasti IT. Budete ale prekvapení, keď povieme, že UAV sú momentálne veľmi populárne aj medzi ľuďmi, ktorí nemajú nič spoločné s IT. Iniciály UAV sú anglickými iniciálmi zo slovného spojenia unmanned areal vehicle, čo je všeobecné pomenovanie pre bezpilotné lietadlo. Zatiaľ, čo tento odborný názov nie je verejnosti známy, ak použijeme jeho synonymum - "dron", bude väčšine ľudí jasné, o čo ide. UAV sa stali v priebehu posledných rokov veľmi populárnymi. Tieto zariadenia sú vhodné na širokú škálu úloh vrátane fotografovania, nahrávania kamerových záznamov, doručovania zásielok a monitorovania okolia.[1]

Zatiaľ čo popularita dronov komerčne dostupných v štandardných obchodoch s elektornikou vzrástla len v posledných rokoch, profesionálne modely UAV používané na armádne alebo vládne účely boli používané už dávno predtým. Tieto profesionálne drony sú vybavené množstvom rozličných senzorov, ktoré slúžia na zber dát z reálneho sveta. Obdržané dáta sú následne spracované pomocou hardvérových a softvérových komponentov a sú prenesené na riadiacu stanicu alebo na iné zariadenie, s ktorým UAV komunikuje. Takto sa UAV stávajú veľkým zdrojom dát.[2]

Jednou z najdôležitejších otázok pre bežných ľudí je, či je prenos dát dobre zabezpečený. Môžeme dôverovať, že dáta, ktoré boli obdržané od odosielateľa sú dobre zabezpečené? Veľa používateľov UAV nepremýšľa nad týmito otázkami až do momentu, kedy sa oni sami stanú obeťou nejakého kyberútoku. Používatelia majú viac možností, ako môžu zvýšiť bezpečnosť prenosu dát, ale napriek tomu nevyužívajú všetky dostupné mechanizmy na zvýšenie bezpečnosti. To sa ale zmení, ak sa oni sami stanu obeťou niektorého z útokov. V momente, keď to tak je, je ale už neskoro. Naviac, prenášané dáta môžu obsahovať citlivé informácie. Uniknuté dáta sa môžu nekontrolovateľne šíriť a môže byť veľmi obtiažné zabezpečiť, že všetky uniknuté kópie dát budú stiahnuté z obehu.

## II. Prenos dát

Pre odborníkov v počítačovej bezpečnosti je najzaujímavejšou oblasťou výskumu UAV ich komunikácia. Pojem komunikácia (z lat. communicare, v zmysle zdielať, informovať) je proces, v ktorom je správa alebo informácia poslaná jedným účastníkom komunikácie inému účastníkovi.[3]

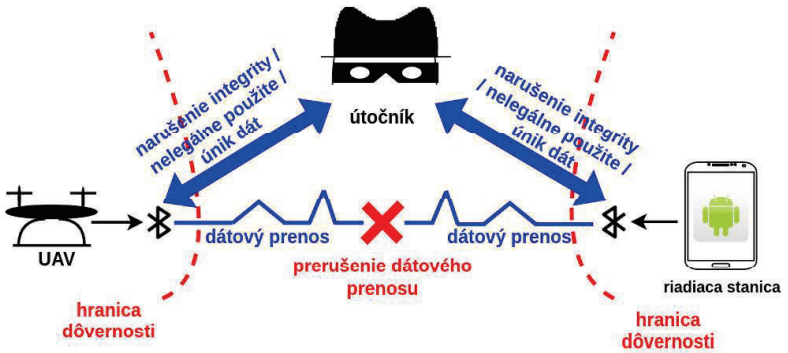
UAV využívajú rôzne protokoly na zabezpečenie korektnej komunikácie medzi riadiacou stanicou a dronom. Väčšina z týchto protokolov bola vyvinutá za účelom armádneho použitia. UAV využívajú napríklad tieto protokoly:

- **MANET protokol** - používaný na statické, proaktívne alebo reaktívne smerovanie
- **Lokalizačné alebo geografické protokoly** - používané pre GPS komunikáciu a RSSI, napríklad na výpočet najkratšej vzdialenosti dvoch bodov
- **Protokoly MAC vrstvy** - používané za účelom dosiahnutia vyššej dynamiky a mobilných scenárov
- **Protokoly na vyhľadávanie najkratšej cesty** - používané na zabezpečenie spoľahlivej komunikácie
- **Protokoly On-Demand** - používané za účelom nemrhania šírkou pásma alebo zdrojom energie pri hľadaní všetkých možných ciest, z ktorých aj tak väčšina nikdy nebude použitá

Ako objekt našej práce sme si zvolili jeden z najpoužívanejších protokolov v oblasti komunikácie malých dronov, MAVLink protokol (skr. z angl. Micro Air Vehicle Link protocol). Ten slúži na zabezpečenie transferu malého množstva dát medzi riadiacou stanicou a UAV tak, aby sa vyhlo vysokým nárokom na ich prenos. Každá MAVLink správa je jednoznačne identifikovateľná pomocou unikátnej hodnoty identifikátora v hlavičke paketu. Tá je logicky definovaná pomocou XML dokumetu, ktorý definuje typ dát, ktoré budú prenášané a poradie v ktorom bude aplikácia interpretovať a spracovavať obdržané dáta. Na definovanie novej správy je potrebné prezentovať ju ako XML súbor, ktorý bude automaticky konvertovaný programom na cieľovom zariadení.[2]

Hlavnou výhodou MAVLink protokolu je podpora rôznych typov transportných vrstiev a rôznych typov medií vďaka jednoduchej štruktúre. MAVLink protokol dokáže prenášať dáta prostredníctvom Bluetooth, Wi-Fi, Ethernet (TCP/IP) alebo kanálov s malým rozsahom šírky pásma, ktoré pracujú na frekvenciách 433 MHz, 868 MHz alebo 915 MHz.[4]

MAVLink protokol je stále vo vývoji, takže nejde o dôkladne zabezpečený protokol. Počas prenosu dáta opúšťajú fyzické zariadenie, prekračujú hranicu dôvernosti a sú prenášané otvoreným priestorom. Možný prenos dát je zobrazený na nasledujúcom obrázku:




Obr. 1 Možný útok na prenos dát

Druhou alternatívou je použitie sieťového rozhania, akým je zvyčajne Wi-Fi alebo Ethernet. Rozhranie prenáša MAVLink správy cez IP sieť. Podporované sú oba protokoly TCP aj UDP a to, ktorý z nich bude použitý závisí od aplikácie.[4]

Existuje potencionálne riziko, že prenášané dáta uniknú, dôjde k narušeniu integrity, zámernému zamedzeniu prístupu k údajom alebo k ilegálnemu použitiu údajov. Ak dáta prenášané prostredníctvom MAVLink protokolu nemajú pre vlastníka veľkú cenu, nemusíme sa zamerať na ich zabezpečenie až tak dôkladne. Problém nastáva, keď je MAVLink protokol využívaný na prenášanie dôverných dát. Ako bolo spomenuté

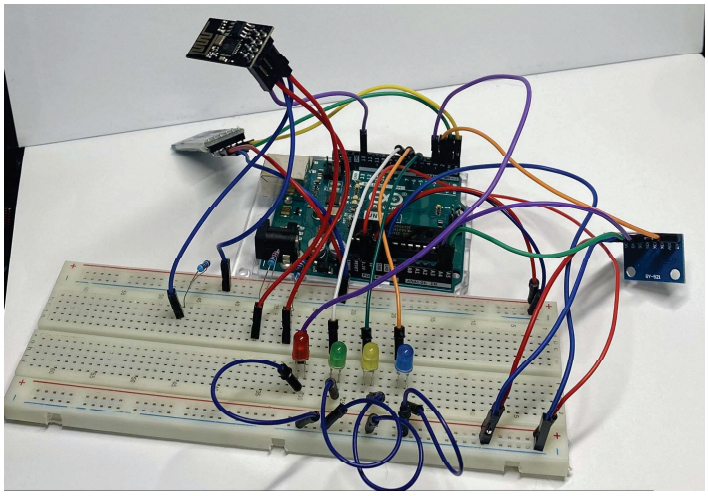
vyššie, ide o nezabezpečený protokol. Preto je potrebné zabezpečiť prenos tak, aby dáta nemohli byť prečítané alebo modifikované útočníkom.

## III. Realizácia útokov

V práci sme vykonali 4 útoky. Tie boli vybrané tak, aby ukázali rôznorodosť útokov na UAV. Zameranie na rôznorodosť ale spôsobilo komplikácie pri ich porovnaní. Fakt, že hodnota úspešnosti jedného útoku je vyššia ako pri inom útoku môže vyvolať dojem, že útok s vyššou úspešnosťou je lepší. Porovnávané útoky majú rôzny zámer a sú založené na odlišných základoch. Napriek tomu ich porovnávame len na základe výslednej úspešnoti. Ideálne by bolo zamerať sa na rôzne vlastnosti, ako je napríklad zámer, komplexnosť implementácie, trvanie od počiatku vykonania útoku až po dosiahnutie cieľa útoku, alebo kvalita zabezpečenia voči danému útoku v praxi. Porovnanie výhod a nevýhod pre každý z tch aspektov, pre každý z týchto útokov by viedlo ku komplexnejšiemu pohľadu na ne a poskytlo by útočníkovi možnosť rozhodnúť sa nad tým, ktorý útok chce vykonať na základe vlastnosti, ktorá je pre neho podstatnejšia. Výsledné hodnoty merania úspešnoti útokov sú prezentované na nasledujúcom diagrame:


Obr. 2 Úspešnosť útokov

Pred opisom dosiahnutých výsledkov pri realizácii prvého útoku je potrebné opísať zariadenia, ktoré boli pri nej použité. Ako riadiaca stanica bol použitý smartfón *HUAVEI Y560-LO1*. Smartfón mal nainštalovaný operačný systém *Android*. Je dôležité, aby sme pri realizácii útokov použili smartfón s operačným systémom *Android* a nie s iným operačným systémom. Ak by sme použili napríklad operačný sysém *iOS*, narazili by sme na problém, že použitý modul *HC-05* s ním nie je kompatibilný.[6]



Obr. 3 Prototyp UAV

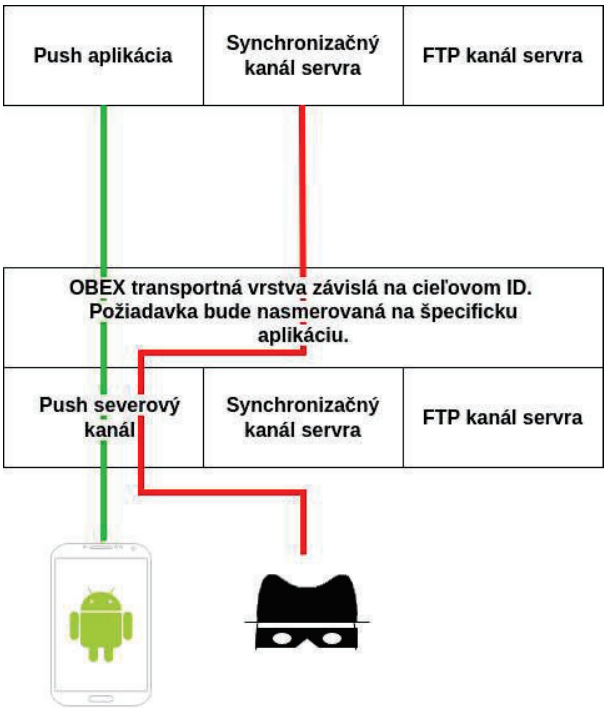
Pri realizácii útokov sme vykonali dátový prenos medzi riadiacou stanicou a skonštruovaným prototypom UAV. Protoyp UAV môžete vidieť na obrázku *Figure 3. Proroyp UAV*. Ako základný provok prototypu bola použitá doska *Arduino UNO*. Na túto dosku boli pripojené senzory, umožňujúce zber dát z reálneho sveta a taktiež prenos dát medzi prototypom a riadiacou stanicou. Ako moduly pre prenos dát boli použité Bluetooth modul *HC-05* a Wi-Fi modul *ESP8266*. Na zber dát bol použitý modul *MPU-6050*. Ide o troj-osový gyroskop a akcelerometer pre Arduino, disponujúci komunikačným modulom *I2C/IIC* a dvoma hlavicami na pripojenie pinov. Tieto tri moduly boli použité s úmyslom priblíženia sa reálným dronom. Všetky spomenuté moduly sú kompatiblilnés *Arduino UNO*.

Po úspešnej konštrukcií prototypu dronu sme vykonali realizáciu prenosu dát medzi našim prototypom a smartfónom. Prv sme realizovali prenos dát bez vykonania útoku. Vďaka tomu sme získali kontrolnú vzorku a ustili sme sa, že prenos dát funguje tak ako má. Potom sme vykonali útoky na dátový prenos. Celkovo sú v práci vykonané štyri útoky: *BlueSnarfing*, *BlueSmacking*, *The 'open sesame' bug* a *The Blesa: spoofingový útok*. Namerané hodnoty úspešnosti útokov sú zobrazenéna diagrame *Vyhodnotenie úspešnosti útokov*.

Prvý stľpec diagramu *Vyhodnotenie úspešnosti útokov* zobrazuje úspešnosť prenosu MAVLink správy. Tento prvý prenos nám slúžil ako kontrolná vzorka. Prenos bol ladený dovtedy, kým nebolo prenesených 100% zo všetkých dát, preto má prvá vzorka takúto úspešnosť.

Druhý stlpec zobrazje úspešnosť útoku *BlueSnarfing*. *BlueSnarfing* je útok na komunikáciu prostredníctom Bluetooth, ktorý používa extrakciu známych názvov súborov počas nadviazania spojenia s *Object Push Profile* v prípade, že komunikujúce zariadenia nepoužívajú autentifikáciu.[6]

V našom prípade sme použili tento fakt na nahranie súboru so škodlivým kódom na UAV. Tento súbor obsahoval XML zdrojový kód známy aj ako *XML bomba*. *XML bomba* je XML kód, ktorý je formatovaný tak, aby sa jedna entita v kóde odkazovala na niekoľko ďalších entít, ktoré sa zasa odkazujú na ďalšie entity. Zdrojový kód *XML bomby* sme napísali tak, aby sme v rekurzii nešli len do jednej úrovne zanorenia, ale hneď niekoľko úrovní. Cieľom tohto útoku bolo spôsobiť pád systému nášho prototypu. Uspenosť útoku bola v meraniach vyhodnotená na 56%. Princíp útoku *BlueSnarfing* je prezentovanýna nasledujúcom obrázku:




Obr. 4 Útok Bluesnarf

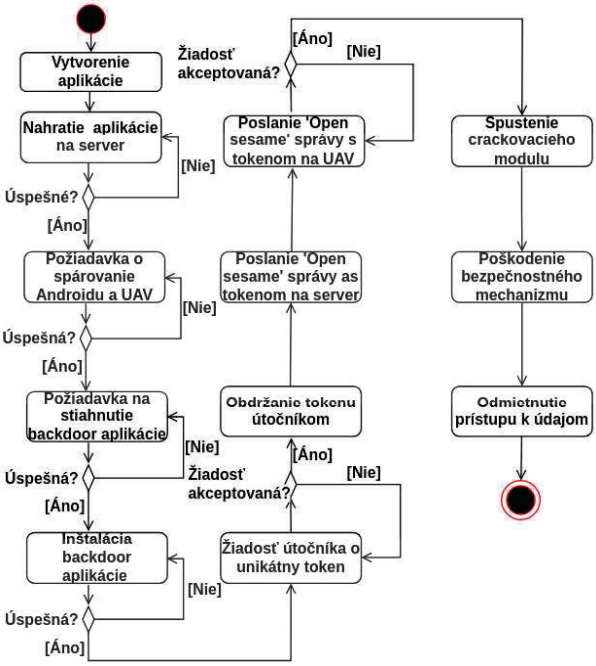
Prostredný stlpec diagramu zobrazuje úspešnosť útoku *BlueSmacking*. Ide o DoS útok,

pri ktorom útočník používa *Logical Link Control and Adaptation Protocol* echo požiadavku o hodnote $600B$ alebo viac. Je pravdepodobné, že práve hodnota $600B$ je optimalizovaná na dosiahnutie čo najlepšej možnej úspešnosti útoku.[7] Utok *BlueSmacking* našťastie oproti útok *BlueSnarfing* poskytuje premennú, ktorá sa dá využiť na optimalizáciu úspešnosti útoku. Modifikácia tejto hodnoty nám poskytla šancu na dosiahnutie najvyššej úspešnosti zo všetkých preskúmaných útokov. Cieľom útoku BlueSmacking je okamžité vyradenie komunikujúceho zariadenia. V našom prípade, po úspešnom vykonaní útoku bolo okamžite znemožnené ovládať prototyp dronu z riadiacej stanice. V prípade skutočného dronu (nie prototypu) by mohol mať tento útok za následok stratu spojenia medzi riadiacou stanicou a dronom, nálsledkom čoho by dron padol. V našich merania mal práve tento útok najvačšiu úspešnosť. Jej hodnota bola $64\%$.

Predposledný útok vykonaný v tejto práci je *The 'open sesame' bug*. Jeho účelom je zabrániť prístupu k zdrojom ako sú napríklad dáta, databázy, aplikácie alebo servre, pomocou zmeny hesla alebo PIN, ktoré chráni zariadenie. Ak útočník pri vykonaní útoku uspeje, dron nebude vyradený z prevádzky, ako to bolo v predchadzajúcom prípade. Útok bude mať ale za následok znemožnenie prístupu k dátam, databáze alebo aplikácii na UAV. *The 'open sesame' bug* môže využívať dva typy útokov - útok hrubou silou alebo slovníkový útok.[8] V tejto práci sme sa rozhodli pre využitie útoku hrubou silou. Táto voľba mohla spôsobiť, že úspešnosť útoku nie je vyššia ako úspešnosť útoku *BlueSnarfing* alebo *BlueSmacking* a je teda len $46\%$. Pri budúcej práci je možné otestovať úspešnosť útoku *BlueSmacking* za pomoci slovníkového útoku.

Posledným vykonaným útokom je *Blesa: spoofingový útok*. Počas *Blesa útoku* sa útočníkové zariadenie vydáva za iné zariadenie, ktoré bolo niekedy v minulosti sparované s dronom, čo utočníkovi umožní podstrčenie falošných dát. Tento fakt ale ovplyvnuje útočníka, ktorý môže vykonať tento útok len na drone, s ktorým bolo útočníkové zariadenie niekedy spárované.[9] Výsledkom tohto útoku je podvrhnutie dát treťou stranou v komunikácii, ktorá by štandardne prebiehala medzi radiacou stanicou a prototypom dronu. Po úspešnom vykonaní útoku, prototyp neobdrží dáta, ktoré sú očakávané, ale dáta podvrhnuté útočníkom. Takto môže útočník prevziať kontrolu nad dronom alebo spôsobiť jeho znefunkčnenie. Uspešnosť *Blesa* bola o niečo vyššia ako úspenosť útoku *The 'open sesame' bug*, konkrétne $48\%$. Na úspešne vykonanie tohto útoku musíme predpokladať, že útočník vykonáva útok zo zariadenia, ktoré už niekedy bolo spárované s prototypom dronu a na základe toho môže útočník podvrhnúť falošné dáta. Tento predpoklad značne limituje utočníka pri pokusoch o vykonanie tohoto útoku. Uspešnosť *útoku Blesa*, jeho priebeh a postup párovanie je závislý od zariadení, ktoré sa párujú. Druhý faktor, ktorý môže ovplyvniť úspešnosť tohto útoku je typ zneužitej zraniteľnosti - útočník si môže zvoliť odmietnutie autentifikácie buď na základe voliteľnej autentifikácie alebo na základe obídenia autentifikácie. Ak útočník chce autentifikáciu obísť, musí prísť na to ako. My sme v práci využili predpoklad, že útočníkové zariadenie a prototyp UAV, na ktorý sa útočí, už niekedy pred útokom mali nadviazané spojenie.

Po úspešnom vykonaní každého z útokov a po úspešnom vyhodnotení ich úspešnosti sme sa pokúsili o návrh ochranných mechanizmov pre tieto útoky. Je dôležité poznamenať, že neexistuje jeden univerzálny ochranný mechanizmus, ktorý by dokázal ochrániť UAV pred všetkými zvolenými útokmi.




Obr. 5 Útok Blesa

## IV. Ochrana pred útokmi

Keď boli implementované všetky 4 útoky bolo naším ďalším cieľom navrhnúť ochranné mechanizmy voči zvoleným útokom. V našej práci sme rozanalyzovali celkovo 14 mechanizmov na ochranu pred útokmi, ktoré boli preskúmané. Tak, ako rôzne útoky zneužívajú rôzne zraniteľnosti systému, tak aj ochranné mechanizmy musia pristupovať ku každému útoku individuálne.

Naš návrh metód ochrany pred útokmi začal s návrhom ochrany pred útokom *BlueSnarfing*. V tomto prípade sme preskúmali možné ochranné mechanizmy ako:

- štandardný antivírusový softvér
- antivírusový softvér špecializovaný na ochranu dronov
- firewall
- povolenie posielania a prijímania len tých dát, ktoré sú zašifrované a podpísané

Ani štandardný antivírusový program, ani antivírusový program špecializovaný na ochranu UAV neposkytujú 100% ochranu pred útokom *BlueSnarfing*. Naopak firewall a posielanie a prijímanie len tých dát, ktoré sú zašifrované a podpísané poskytovalo efektívnu ochranu pre útokom. Dobre implementovaný firewall dokáže efektívne ochrániť dron pred BlueSnarfing útokom. V prípade posielania a prijímania len zašifrovaných a podpísaných dát, môžme nastaviť bezpečnostnú politiku na UAV tak, že povolíme prijímanie dát len z tých zdrojov, ktoré považujeme za dôveryhodné. Za dôveryhodné budeme považovať len tie zdroje, ktoré podpísali odoslanú správu so správnym kľúčom. Týmto spôsobom sme schopní dosiahnúť 100% ochranu.

Ďalším útokom, proti ktorému boli navrhnuté ochranné mechanizmy bol útok *BlueSmack*. V prípade ochrany pred týmto útokom odporúčame:

- pravidelné vykonávanie aktualizácie systému
- dodržiavanie pravidiel bezpečného používania UAV
- používanie aplikácie *Bluetooth Firewall*
- používanie filtrovania sieťovej prevádzky

Všetky spomenuté spôsoby ochrany nám môžu pomôcť pri ochrane pred útokom BlueSmack, ale ani jeden z nich nedokáže garantovať 100% ochranu pred týmto útokom.

Tretím útokom, proti ktorému sme navrhli obranné mechanizmy je útok *The 'open sesame' bug*. V prípade ochrany pred útokom *The 'open sesame' bug* odporúčame:

- pravidelné vykonávanie aktualizácie systému
- odstránenie všetkých potencionálne škodlivých zdrojov z pamate UAV
- povolenie aplikaciám spúšťania v *Trusted Execution Enviroment* móde
- dôsledné dodržiavanie zásad pre správny návrh hesla používateľom

Rovnako, ako tomu bolo v prípade *BlueSmack* aj v prípade *The 'open sesame' bug* musíme poznamenať, že žiaden zo spomínaných spôsobov ochrany negarantuje 100% ochranu pred týmto útokom.

Ako poslednésme navrhli ochranné mechanizmy voči ítoku *Blesa*. V tomto prípade odporúčame:

- pravidelné odstraňovanie sparovaných zariadení
- ovládanie UAV výlučne z jednej riadiacej stanice
- stanovanie úrovne ochrany dát

Bohužiaľ, ani v prípade posledného útoku sme neboli schopní garantovať, že navrhnuté ochranné mechanizmy poskytnú 100% ochranu voči útoku.

Všetky spomenuté metódy ochrany boli verifikované proti špecifickému typu útoku. Môžeme vidieť, že rôzne typy ochrany sú efektívne v zabraňovaní rôznym typom útokom. Ak ale budúł; jednotlivé ochranné mechanizmy implementované samostatne, bude obtiažné zabezpečiť, že každý z nich bude použitý správne. Ideálnym riešením by bolo navrhnutie jedného robustného ochranného mechanizmu špecializovaného na ochranu dronov, ktorý by kombinoval výhody aktuálne dostupných obranných mechanizmov.

## V. ZÁVER

V našom výskume sme vykonali merania úspešnosti štyroch vybraných útokov na prototype UAV. Za útoky sme si zvolili: *Bluesnarfing*, *Bluesmacking*, *The 'open sesame' bug* a *Blesa: spoofingovýútok*. Uspešnosť útoku *Bluesnarfing* sme v našom prípade vyhodnotili na 56%, *Bluesmacking* na 64%, *The 'open sesame' bug* na 46% a *Blesa* na 48%. V praxi ale nemusí znamenať, že útok s vyššou úspešnosťou je aj lepší na implementáciu. Ak chceme tieto útoky hlbšie rozanalyzovať, musíme sa pozrieťna každý jeden z nich ako na komplexnú operáciu, ktorá je charakterizovaná svojími viacerými vlastnosťami, nie len úspešnosťou.

Rovnako je potrebné brať do úvahy, že útoky boli vykonané na prototype dronu, ktorého základným stavebným prvkom bol mikrokontroler Arduino. V záujme dosiahnutia presnejších výsledkov môže byť táto práca rozšírená o overenie úspešnosti útokov na skutočnom drone. Takéto rozšírenie by poskytlo presnejšie a realistickejšie výsledky. Predpokladáme ale, že namerané hodnoty by boli približne rovnaké ako namerané hodnoty na prototype. Naviac, je možné aby bola základná doska prototypu zmenená z mikrokontroléru *Arduino* na iný mikrokontrolér (napr. *Raspberry*). V tomto prípade ale neočakávame zásadný rozdiel v nameraných výsledkoch úspešnosti útokov.

Ďalším cieľom našej práce bol návrh ochranných mechanizmov, ktoré by umožňovali ochranu dronu pred opísanými útokmi. V záujme zabezpečenia nášho UAV sme pristupovali ku každému útoku individuálne a navrhovali sme ochranné mechanizmy. Funkčnosť niektorých ochranných mechanizmov bola potvrdená , ale niektoré z overovaných mechanizmov nedosiahli očakávané výsledky. Pri ďalšom pokračovaní v práci zvažujeme vytvorenie jedného softvéru špecializovaného na ochranu UAV, ktorý bude poskytovať robustný ochranný mechanizmus proti všetkým aktuálne známym typom útokov. V našom budúcom výskume sa pokúsime o návrh jedného ochranného mechanizmu špecializovaného na ochanu UAV. Tento ochranný mechanizmus by mal byť navrhnutý tak, aby neposkytoval ochranu len pred týmito zvolenými útokmi, ale tak, aby umožňoval ľahké doimplementovanie ochrany voči akémukoľvek novému útoku.

Pri ďalšom výskume je potrebné brať do úvahy, že ochrana UAV je veľmi aktuálna téma. Naviac očakávame, že popularita dronov bude v nasledujúcich rokoch ešte viac narastať. Cím viac sa budú UAV používať, tým aj vačšie bude množstvo dát, ktoré je potrebné chrániť. V budúcnosti budú hackeri stále viac motivovaní vo vývoji nových, sofistikovanejších a ťažšie odhaliteľných útokov. Dáta budú mať stále pre používateľa určitú hodnotu. Ak nechceme aby boli zneužité, musíme vo vývoji obranných mechanizmov, držať krok s hackermi. Pokroky v tejto oblasti za posledné roky boli veľmi dynamické. Táto práca ma za cieľ prezentovať aktuálny stav v tejto oblasti.

## POĎAKOVANIE

Táto publikácia bola podporená z operačného programu Integrovaná infraštruktúra v rámci projektu: Inteligentné operačné a spracovateľské systémy pre UAV, kód ITMS2014+: 313011V422 a spolufinancované Európskym fondom regionálneho rozvoja.

## LITERATÚRA


[1] Samuel Novotny and Miroslav Michalko and Jan Perhac and Valerie Novitzka and Frantisek Jakab, *Formalization and Modeling of Communication within Multi-Agent Systems Based on Transparent Intensionla Logic* (2022).

[2] Anis Koubaa and Azza Allouch and Maram Alajlan and Yasir Javed and Abdelfettah Belghith and Mohamed Khaligui, *Micro Air Vehicle Link (MAVLink) in a Nutshell: A Survey* (2016).

[3] Maik Bassi and Iulisloi Zacarias and Carlos Eduardo Tussi Leite and Haijun Wang and Edison Prignaton de Freitas, *A Pratical Deployment of a Communication Infrastructure to Support the Employment of Multiple Surveillance Drones System* (2018).

[4] Ondrej Kainz and Matus Dopiriak and Miroslav Michalko and Frantisek Jakab and Ivana Novakova, *Traffic Monitoring from the Perspective of Unmanned Aerial Vehicle* (2022).

[5] KoubÃ˘a Anis and Akkizch Azza and Alajlan Maram and Javed Yasir and Belghuth Abdelfettah and Khalgui Mohamed, *Micro Air Vehicle Link (MAVLink) in a Nutshell: A Survey* (2016).

[6] *Connecting hc-05 with iPhone SE iOS(v11.0)* (2018).

[7] Moreno Alberto and Okamoto Eiji, *BlueSnarf revisited: OBEX FTP service directory traversal* (2011).

[8] M Thrinatha Reddy, *Man-in-the-Middle Attack and its Countermeasure in Bluetooth Secure Simple Pairing* (2011).

[9] Bas Vergoow and Huub Nagel and Geert Bondt and Bart Custer, *Drone Technology: Types, Payloads, Application, Frequency Spectrum Issues and Future Developments* (2016).

[10] M Thrinatha Reddy, *Man-in-the-Middle Attack and its Countermeasure in Bluetooth Secure Simple Pairing* (2011).