Politecnico di Torino

Politecnico di Torino
Collegio di Ingegneria Informatica, del Cinema e Meccatronica

Corso di Laurea Magistrale in Ingegneria Informatica
A.a. 2023/2024
Sessione di Laurea: ottobre 2024

Soluzioni per la sicurezza informatica di aeromobili a pilotaggio remoto

Relatori:
Prof. Tiziano Bianchi
Ing. Michele Festa

Candidato:
Andrea Martinengo

Abstract

Il seguente progetto di tesi si propone di affrontare il tema della sicurezza informatica applicato ad un settore in forte crescita, come quello del mercato dei droni. L'aumento dell'impiego di questi velivoli, favorito dalla loro versatilità, che li rende utilizzabili in qualsiasi settore (agricoltura, mappature, emergenze, sicurezza, logistica, fotografia…), unito al loro pilotaggio da remoto, fa sorgere numerosi problemi legati alla sicurezza dei dati, delle comunicazioni e delle procedure legate al controllo degli stessi.

La presente tesi nasce dal personale interesse per l'argomento della cybersecurity, unito a uno dei maggiori campi di azione di SIPAL, il settore dell'aeronautica. La tesi è, infatti, realizzata in stretta collaborazione con SIPAL, azienda leader nel settore della consulenza aeronautica, che mi ha fornito supporto per la realizzazione dell'elaborato, in particolar modo nella fase sperimentale.

Durante il periodo di svolgimento di questa tesi, sono stati affrontati dapprima i temi legati alle normative vigenti che i vari paesi adottano per far fronte al problema della sicurezza digitale di un drone: l'attenzione si è focalizzata al settore civile, che vede ancora importanti lacune, piuttosto che al settore militare, dove le norme sono ben definite, secretate e specifiche per ogni velivolo. Questa differenza, che si può riscontrare sia nell'ambito legislativo, con la mancanza di linee guide specifiche, che nell'ambito tecnico, con l'assenza di protocolli di cybersecurity riguardanti i droni, è il punto focale dell'elaborato. A seguito della disamina legislativa, si farà una descrizione delle principali minacce informatiche, rilevanti per lo scenario analizzato, affiancata da un elenco di noti attacchi effettuati contro i droni.

Dopodiché, ci si concentrerà sulla parte applicativa, analizzando un protocollo di recente introduzione e ancora in fase di testing, ma con enormi potenzialità per quel che riguarda l'autenticazione dei messaggi relativi, in particolare, alla posizione. Tale sezione verrà arricchita con un'analisi dei dati relativi ai consumi del software preso in considerazione, per poi concludersi con uno sguardo alle tendenze future.

Sommario

Introduzione

Obiettivi e motivazioni

Alla base di questo studio vi è la cybersecurity legata al mondo degli UAV (Unmanned Aerial Vehicle), con maggior enfasi sul mondo dei droni allo stato attuale. In particolare, si pone l'attenzione sulle tecnologie attualmente in campo e sulla mancanza di tecniche basiche di protezione, per quanto riguarda l'ambito civile.

L'idea di questa tesi nasce da una volontà di unire il mio percorso di studi, legato alla cybersecurity, con l'ambito nel quale ho incominciato a lavorare, in concomitanza con l'inizio della tesi, ovvero lo sviluppo di software di volo per i droni.

L'obiettivo della tesi è quello di approfondire la tematica della sicurezza informatica in un settore, come quello degli UAV, sul quale, specialmente in ambito civile, non c'è ancora stata particolare attenzione. L'argomento verrà valutato sia in un contesto teorico che in un contesto pratico, analizzando un recente algoritmo di autenticazione.

L'elaborato è diviso in quattro sezioni: la prima riguardante la normativa attualmente in vigore, in Italia così come all'estero; la seconda sezione è incentrata sulle tematiche legate alla sicurezza informatica, intese sia come tecniche attualmente in campo che come minacce informatiche contro gli UAV; nella terza sezione ci si concentra su OSNMA, funzione inclusa in Galileo Open Service, che fornice l'autenticazione dei dati per tutti i ricevitori abilitati, in relazione alle potenziali soluzioni, in termini di applicazione, del quadro delle soluzioni di sicurezza informatica in campo avionico, in particolare riguardo il funzionamento degli UAV. A questo scopo, è presente una parte sperimentale, nella quale si analizza il funzionamento dell'algoritmo di OSNMA su una Orange Pi, paragonabile a un computer di bordo equipaggiato su un drone civile. Infine ci sarà un rapido sguardo a quelli che sono i trend futuri e i possibili sviluppi del settore, legati alle innovazioni tecnologiche che stiamo vivendo.

Breve storia

Negli ultimi anni gli UAV sono diventati sempre più popolari. Le ragioni sono molteplici; tra i principali vantaggi nel loro utilizzo vi sono il potenziamento delle funzionalità dei droni, il miglioramento della durata delle batterie, della stabilizzazione, della navigazione, della tecnologia dei sensori. Tuttavia, mentre il numero di droni si espande e le loro funzionalità tecnologiche si evolvono, l'uso dei droni comporta preoccupazioni e sfide che non devono essere sottovalutate, legate, ad esempio, alla cybersecurity, alla privacy e alla sicurezza pubblica. Gli UAV, secondo il regime internazionale, regionale e nazionale del diritto dell'aviazione, sono considerati aeromobili; poiché non esiste un quadro di cybersecurity specifico per gli UAV, dovrebbe applicarsi il quadro di cybersecurity dell'aviazione civile.

Un drone è un aeromobile senza piloti o passeggeri a bordo. Possono essere a guida automatica, quindi programmati per seguire una determinata rotta, oppure pilotati da remoto (RPAV). Il primo aeromobile senza pilota risale al 1917, quando il Regno Unito sviluppò un piccolo drone radio comandato, progettato per essere usato nella Prima Guerra Mondiale; nel 1918, gli Stati Uniti replicarono l'esperimento su un siluro aereo, il

Kettering Bug, ma entrambi questi progetti si limitarono alle fasi di test. Nel 1935 il termine “drone” entrò a far parte del lessico, grazie ai numerosi modelli prodotti dal Regno Unito, come il **DH.82B Queen Bee**. Questi modelli avevano scopi di esercitazioni di tiro e addestramento. Nella guerra del Vietnam, furono introdotti per la prima volta i droni da ricognizione, da parte degli Stati Uniti, e dopo di essa, il loro utilizzo venne esteso ad altri settori, oltre a quello militare, e i droni diventarono sempre più sofisticati, in grado di volare per lunghi periodi e ad energia solare, per affrontare il problema del rifornimento di carburante. [1]

I droni ora hanno molte funzioni, che vanno dal monitoraggio del cambiamento climatico allo svolgimento di operazioni di ricerca dopo disastri naturali, alla fotografia, alle riprese e alla consegna di merci. Ma il loro utilizzo più noto resta quello da parte dei militari per la ricognizione, la sorveglianza e gli attacchi mirati. Dopo gli attacchi terroristici dell'11 settembre, gli Stati Uniti hanno aumentato notevolmente l'uso dei droni. Sono utilizzati principalmente per la sorveglianza in aree e terreni in cui le truppe non possono andare in sicurezza.

Tuttavia, i droni sono usati anche come armi e sono stati accusati di aver ucciso presunti militanti. Il loro utilizzo nei conflitti attuali e in alcuni paesi ha sollevato interrogativi sull'etica di questo tipo di armi, soprattutto quando provocano la morte di civili, a causa di dati imprecisi o a causa della loro vicinanza a un "bersaglio".

Infine, meritevole di menzione è la recente guerra tra Russia e Ucraina, che ha visto un ingente investimento sugli UAV in campo militare, in entrambi gli schieramenti.

Utilizzi di un UAV

Con il termine UAV ci riferiamo soltanto al drone in sé, inteso come un veicolo in grado di volare comandato da remoto o totalmente autonomo. Con il termine UAS (Unmanned Aircraft System) invece, ci riferiamo all’insieme dell’UAV e della stazione di controllo, pilota compreso. Infine, il termine RPAS (Remotely Piloted Aircraft System) viene usato per quegli UAV con delle funzionalità avanzate, per il quale sono richieste competenze più specifiche rispetto agli standard.

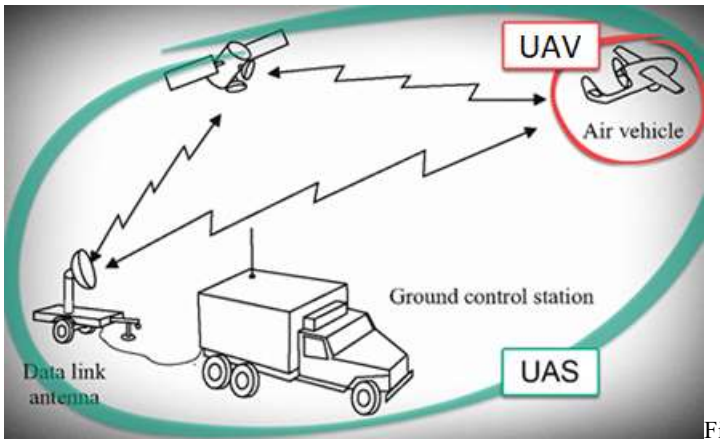


Fig. 1 Configurazione generica UAS

In generale, secondo il rapporto fornito da PwC [2], gli UAV vengono utilizzati nei seguenti settori: agricoltura, energia, servizi pubblici, sicurezza, intrattenimento, media, infrastrutture, assicurazioni, telecomunicazioni, trasporti e logistica.

Come affermato da un recente rapporto di *globenewswire.com* [3], il mercato degli UAV conterà 91.23 miliardi di dollari entro il 2030. Il mercato divide gli UAV per classe, per modalità operativa, per soluzione, applicazione e per utente finale.

Le classi possono essere Micro UAV (sotto i 2kg), Mini UAV (tra 2 e 20kg), Small UAV (tra 20 e 50kg) e Tactical UAV, come MALE e HALE. In quest'ultima categoria si prevede la maggiore crescita dovuta alla crescente richiesta di tali velivoli di India, Giappone, Cina e Australia.

Per modalità operativa, invece, troviamo completamente autonomo, semi-autonomo e da pilotati totalmente da remoto; il segmento con la maggiore crescita prevista è quello dei droni completamente automatici, grazie alla crescente presenza di FPS (Flight Planning System) e CDS (Command Delivery System).

Per soluzione, si classificano in aerostrutture e meccanismi, sistemi di sicurezza, software operativo, fonti di alimentazione e sistemi di gestione generici. A causa dell'aumento degli attacchi informatici contro gli UAV, si prevede una maggiore crescita del settore relativo ai sistemi di sicurezza.

Per applicazione, il mercato suddivide gli UAV in sicurezza perimetrale e gestione delle frontiere, missioni di combattimento e supporto al combattimento, consapevolezza situazionale, gestione delle catastrofi e primi soccorritori, rilevamento, mappatura e monitoraggio, gestione dell'agricoltura di precisione, gestione delle centrali elettriche, gestione degli asset e delle operazioni, logistica medica d'emergenza. La logistica medica di emergenza registrerà la crescita più rapida durante il periodo di previsione, anche grazie allo scoppio di pandemie, che necessitano forniture di attrezzature mediche avanzate.

In base all'utente finale, il mercato è suddiviso in governo e difesa, energia, petrolio e gas, costruzioni e miniere, agricoltura, silvicoltura e conservazione della vita selvatica, infrastrutture pubbliche e sicurezza interna, ospedali e servizi medici di emergenza, trasporti e logistica e gestione degli eventi. Il segmento degli ospedali e dei servizi medici di emergenza registrerà il tasso di crescita più elevato durante il periodo di previsione, grazie alla crescente adozione di esperimenti e test sui veicoli aerei senza pilota (UAV) per varie applicazioni mediche in tutto il mondo.

Normativa applicabile

Italia

In Italia l'utilizzo dei droni è regolamentato dal "Regolamento sui Sistemi Aeromobili a Pilotaggio Remoto" emanato dall'Ente Nazionale per l'Aviazione Civile (ENAC) nel 2015, aggiornato nel 2021 [4].

Il regolamento si applica a tutti i droni di peso superiore a 250g e richiede la registrazione dell'operatore del drone e del drone stesso. La registrazione avviene attraverso una piattaforma online gestita da ENAC.

In Italia, il regolamento sui droni non affronta specificamente la sicurezza informatica dei droni, ma esistono leggi e regolamenti che si applicano all'uso dell'informatica e alla sicurezza informatica in generale.

Direttiva sulla sicurezza delle reti e delle informazioni

La direttiva sulla sicurezza delle reti e delle informazioni (NIS) è una direttiva dell'Unione Europea che stabilisce le regole per garantire la sicurezza delle reti e dei sistemi informativi. La direttiva NIS si applica agli operatori di servizi essenziali e ai fornitori di servizi digitali, compresi gli operatori di droni che forniscono servizi tramite Internet. Gli operatori di droni che rientrano nel campo di applicazione della direttiva NIS devono attuare adeguate misure di sicurezza per prevenire le minacce informatiche e segnalare gli incidenti di sicurezza alle autorità competenti.

Quadro di sicurezza informatica per le infrastrutture critiche

Il governo italiano ha emanato un quadro di sicurezza informatica per le infrastrutture critiche, che include disposizioni relative alla protezione dei sistemi di controllo industriale, compresi i droni utilizzati per il monitoraggio delle infrastrutture critiche. Il quadro stabilisce le linee guida per la valutazione e la gestione dei rischi informatici, l'implementazione dei controlli di sicurezza e la segnalazione degli incidenti di sicurezza.

Diritto penale

Il Codice penale italiano include disposizioni relative alla criminalità informatica, tra cui l'accesso non autorizzato ai sistemi informatici, il furto di dati e la diffusione di malware o virus. Gli operatori di droni che commettono crimini informatici possono essere perseguiti e puniti penalmente.

UE

L'Unione Europea ha adottato una normativa comune sulla sicurezza dei droni, il Regolamento UE 2019/947. Questo regolamento richiede la registrazione dei droni, la certificazione degli operatori, l'uso di sistemi di geolocalizzazione e limiti sul peso e sulla velocità dei droni. [5]

Il regolamento stabilisce inoltre diverse categorie di operazioni con droni in base al peso, alle caratteristiche e agli scopi del drone e definisce requisiti e restrizioni specifici per ciascuna categoria. Le categorie sono:

Categoria aperta

La categoria aperta copre le operazioni meno rischiose e più comuni, in cui l'aeromobile rimane entro il campo visivo del pilota e non vola sopra le persone.

- La categoria aperta è suddivisa in tre sottocategorie (A1, A2 e A3), che si differenziano in base al rischio dell'operazione, al peso e alle caratteristiche dell'UAV utilizzato. In generale, le operazioni in categoria aperta richiedono solo una registrazione dell'UAV e del pilota, l'adesione a norme di base sulla sicurezza aerea e il rispetto delle distanze di volo e degli spazi aerei previsti dalla normativa.
    - La sottocategoria A1 è applicabile agli UAV leggeri (massa al decollo inferiore o uguale a 250 grammi) e alle operazioni a basso rischio. In questa sottocategoria, l'UAS può essere operato senza restrizioni sulla distanza dal pilota o dalle persone non coinvolte nell'operazione, purché venga rispettata la distanza minima di 5 metri dalle persone coinvolte nell'operazione e il volo avvenga solo su aree autorizzate.
    - La sottocategoria A2 si applica agli UAV che pesano meno di 4 kg e che sono operati a distanze di sicurezza maggiori rispetto alla sottocategoria A1. Per volare in questa categoria, l'UAV deve soddisfare requisiti tecnici specifici, come la capacità di evitare le persone, e il pilota deve aver superato un corso di formazione.
    - La sottocategoria A3 si applica agli UAV che pesano meno di 25 kg e che sono operati in spazi aerei meno popolati e con limitazioni sulle operazioni sull'acqua e sulle persone. In questa sottocategoria, l'UAV deve rispettare le distanze di volo e le restrizioni sui luoghi di operazione previste dalla normativa.

In generale, la categoria aperta consente un utilizzo semplice e accessibile degli UAV per le attività ricreative e commerciali a basso rischio, con una regolamentazione proporzionata al livello di rischio dell'operazione.

Categoria specifica

La categoria specifica si applica alle operazioni che rappresentano un rischio elevato per la sicurezza pubblica o che richiedono autorizzazioni e requisiti specifici.

- Le operazioni in categoria specifica sono soggette a una valutazione del rischio specifica, che tiene conto delle caratteristiche dell'operazione e del tipo di UAV utilizzato. A seconda della valutazione del rischio, l'operatore può dover ottenere un'autorizzazione specifica dalle autorità competenti, ad esempio per volare in aree urbane, vicino a infrastrutture critiche, in spazi aerei controllati o per operazioni di sorveglianza.
- La categoria specifica prevede anche l'obbligo di utilizzare UAV conformi a specifiche tecniche e di ottenere certificazioni per le attrezzature e il personale, in funzione del tipo di operazione e del rischio associato. Inoltre, l'operatore deve rispettare le norme sulla privacy e sulla protezione dei dati personali durante l'utilizzo dell'UAV.

Questa categoria si applica a operazioni più complesse e ad alto rischio, come quelle utilizzate per il trasporto di materiali pericolosi, l'osservazione aerea o le operazioni di ricerca e salvataggio.

Categoria certificata

La categoria certificata si applica alle operazioni di alto rischio e alle operazioni fuori dalla vista del pilota.

- Le operazioni in categoria certificata richiedono un elevato livello di certificazione e di autorizzazione, e sono soggette a un rigoroso processo di valutazione del rischio. Queste operazioni comprendono, ad esempio, voli oltre la linea di vista, voli in spazi aerei controllati, operazioni in aree urbane o vicino a infrastrutture critiche.
- Per effettuare operazioni in categoria certificata, l'operatore deve ottenere un certificato di aeronavigabilità per l'UAV, una certificazione per l'equipaggio e per le attrezzature, oltre ad autorizzazioni specifiche dalle autorità competenti. Inoltre, l'operatore deve aderire a rigide norme di sicurezza, che comprendono l'utilizzo di sistemi di sorveglianza e di comunicazione a distanza, nonché l'implementazione di misure di sicurezza specifiche per la zona di volo.
- In generale, la categoria certificata si applica a operazioni altamente specializzate e critiche per la sicurezza pubblica, come le operazioni di ricerca e salvataggio, le missioni di sicurezza nazionale o le operazioni di soccorso in caso di calamità naturali.

Oltre a questi requisiti, il regolamento stabilisce anche regole relative all'uso di droni per la fotografia aerea e la videografia, l'uso di sistemi di visuale in prima persona (First-Person View) e la protezione della privacy e dei dati personali.

In Europa, la sicurezza informatica dei droni è regolata da una combinazione di leggi, regolamenti e linee guida a livello UE e nazionale. Le principali normative relative alla sicurezza informatica dei droni in Europa sono:

1. Regolamenti dell'Agenzia dell'Unione europea per la sicurezza aerea (EASA): l'obiettivo di EASA è assicurarsi che l'aviazione, nell'ambito UE, sia sicura, protetta e resiliente. EASA ha sviluppato regolamenti per i sistemi aerei senza pilota (UAS), compresi i droni. Questi regolamenti riguardano la progettazione, la produzione, il funzionamento e la manutenzione dei droni e includono disposizioni per la sicurezza informatica. Ad esempio, l'EASA richiede che i droni dispongano di adeguate caratteristiche di sicurezza per impedire l'accesso non autorizzato e che l'operatore implementi misure di sicurezza informatica per proteggere i dati e le comunicazioni. [6]
2. Regolamento generale sulla protezione dei dati (GDPR): il GDPR è un regolamento che si applica a tutti gli stati membri dell'Unione Europea e stabilisce le regole per la raccolta, l'elaborazione e l'archiviazione dei dati personali. Il GDPR si applica ai droni che raccolgono ed elaborano dati personali e richiede agli operatori di droni di implementare adeguate misure di sicurezza informatica per proteggere i dati personali da accessi non autorizzati e violazioni dei dati. [7]
3. Direttiva sulla sicurezza delle reti e delle informazioni (NIS): vedi sopra.
4. Linee guida dell'Agenzia dell'Unione europea per la sicurezza informatica (ENISA): l'ENISA ha pubblicato linee guida per la sicurezza informatica dei droni, che forniscono raccomandazioni agli operatori e ai produttori di droni su come migliorare la sicurezza informatica dei droni. Le linee guida trattano argomenti come la valutazione del rischio, la progettazione e lo sviluppo sicuri, il funzionamento e la manutenzione sicuri e la risposta agli incidenti. [8]

5. Linee guida dell'Agenzia europea per la difesa (EDA): l'EDA ha pubblicato linee guida per la sicurezza informatica dei sistemi aerei a pilotaggio remoto (RPAS), che forniscono raccomandazioni per le forze armate e altre organizzazioni di sicurezza su come migliorare la sicurezza informatica degli RPAS. Le linee guida trattano argomenti analoghi a quelle dell'ENISA. [9]

Questi regolamenti e linee guida mirano a promuovere l'uso sicuro e protetto dei droni e a proteggere le infrastrutture critiche e i dati personali dalle minacce informatiche. Gli operatori di droni devono essere a conoscenza di queste normative e implementare adeguate misure di sicurezza per prevenire attacchi informatici e violazioni dei dati.

L'Unione europea (UE) ha fornito una serie di linee guida per la sicurezza informatica dei droni, note come linee guida dell'Agenzia dell'Unione Europea per la Sicurezza Aerea (EASA). Queste linee guida mirano a garantire il funzionamento sicuro e protetto dei droni, che vengono sempre più utilizzati per varie applicazioni come la fotografia aerea, il rilevamento e i servizi di consegna. Seguono alcune delle linee guida chiave per la sicurezza informatica dei droni nell'UE [10]:

1. **Valutazione del rischio**: gli operatori devono condurre una valutazione del rischio delle loro operazioni per identificare eventuali rischi di sicurezza informatica che potrebbero influire sulla sicurezza del drone e di altri utenti dello spazio aereo.
2. **Controllo degli accessi**: gli operatori devono garantire che solo il personale autorizzato abbia accesso ai sistemi del drone, compresi i suoi sistemi di controllo e comunicazione.
3. **Protezione dei dati**: gli operatori devono proteggere tutti i dati raccolti dal drone durante le sue operazioni da accessi non autorizzati o furto. Dovrebbero inoltre garantire che i dati siano archiviati in modo sicuro ed eliminati quando non sono più necessari.
4. **Comunicazioni sicure**: gli operatori devono utilizzare protocolli di comunicazione sicuri per garantire che i segnali di controllo del drone non vengano intercettati o interrotti da parti non autorizzate.
5. **Aggiornamenti del software**: gli operatori devono aggiornare regolarmente il software del drone per affrontare eventuali vulnerabilità o bug che potrebbero essere sfruttati dai cyber aggressori.
6. **Sicurezza fisica**: gli operatori devono garantire che il drone sia fisicamente sicuro, ad esempio utilizzando strutture di stoccaggio sicure quando non in uso e proteggendo il drone durante il trasporto.
7. **Segnalazione degli incidenti**: gli operatori devono segnalare alle autorità competenti eventuali incidenti di sicurezza informatica, come accessi non autorizzati o violazioni dei dati.

Queste linee guida sono progettate per fornire un quadro per gli operatori di droni per garantire che le loro operazioni siano sicure e protette dalle minacce informatiche. Seguendo queste linee guida, gli operatori di droni possono aiutare a proteggere sia i loro droni che altri utenti dello spazio aereo da potenziali attacchi informatici.

Le linee guida italiane (ENAC) sono del tutto simili a quelle fornite dall'UE e sono progettate per garantire il funzionamento sicuro e protetto dei droni in Italia.

Resto del mondo

La normativa sulla sicurezza digitale dei droni può variare a seconda del paese e della giurisdizione in cui il drone viene utilizzato. Tuttavia, in linea di massima, la maggior parte dei paesi ha una serie di regole e normative che regolano l'uso dei droni, anche in relazione alla sicurezza informatica.

USA

L'agenzia federale dell'aviazione (FAA) richiede che tutti i droni commerciali registrati siano dotati di un numero di identificazione unico e che gli operatori dei droni commerciali abbiano una certificazione FAA Part 107. Inoltre, FAA richiede che i droni commerciali vengano utilizzati solo in aree designate e in conformità con le norme di sicurezza, che includono restrizioni sul volo in prossimità di aeroporti, strutture crittografiche e di sicurezza nazionale. [11]

Canada

Transport Canada ha stabilito regolamenti per il funzionamento dei droni ai sensi del Canadian Aviation Regulations. Questi regolamenti richiedono che gli operatori di droni ottengano un certificato di pilota, registrino il loro drone e rispettino i requisiti operativi e tecnici, come volare sotto i 400 piedi e non sorvolare le persone. [12]

Australia

L'Autorità per la sicurezza dell'aviazione civile (CASA) ha stabilito regolamenti per il funzionamento dei droni ai sensi dei regolamenti per la sicurezza dell'aviazione civile. I droni devono essere registrati e il loro utilizzo è soggetto a limiti di peso, altezza massima di volo e distanza di volo. Inoltre, i droni non possono essere utilizzati sopra persone non coinvolte nell'operazione e non possono essere utilizzati per attività commerciali senza una licenza commerciale. [13]

Cina

La Cina richiede la registrazione dei droni e ha stabilito limiti di peso, altezza massima di volo e distanza di volo. Inoltre, i droni devono essere dotati di dispositivi di identificazione elettronica e possono essere utilizzati solo per attività non commerciali senza autorizzazione. [14]

Giappone

Il Giappone richiede la registrazione dei droni e ha stabilito limiti di peso, altezza massima di volo e distanza di volo. Inoltre, i droni devono essere dotati di dispositivi di identificazione elettronica e non possono essere utilizzati in alcune aree proibite come aeroporti e centri urbani densamente popolati. [15]

Regno Unito

Nel Regno Unito, i droni devono essere registrati e il loro utilizzo è soggetto a limiti di peso, altezza massima di volo e distanza di volo. Inoltre, i droni devono essere dotati di dispositivi di identificazione elettronica e non possono essere utilizzati sopra persone non coinvolte nell'operazione. [16]

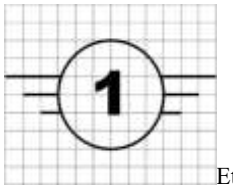
Requisiti di sicurezza per droni

I costruttori di droni hanno l'obbligo di garantire la sicurezza dei loro prodotti in ambito cybersecurity. Ciò significa che devono prevedere misure di sicurezza adeguate, per prevenire intrusioni e altre minacce informatiche che potrebbero compromettere la sicurezza dei dati, la privacy degli utenti o, ancor peggio, la sicurezza dei sistemi in cui i droni sono utilizzati.

In particolare, i costruttori di droni dovrebbero adottare le seguenti misure: [17]

1. **Crittografia dei dati**: i droni devono utilizzare un sistema di crittografia avanzato per proteggere i dati che vengono trasferiti tra il drone e il sistema di controllo. Ciò garantirà che le informazioni trasmesse siano accessibili solo a persone autorizzate.
2. **Sicurezza del firmware**: i costruttori di droni dovrebbero verificare che il firmware dei loro prodotti sia sicuro e non presenti vulnerabilità che possano essere sfruttate dagli hacker per prendere il controllo del drone o per accedere ai dati.
3. **Autenticazione degli utenti**: i droni dovrebbero richiedere una corretta autenticazione degli utenti prima di permettere l'accesso alle funzionalità di controllo. Ciò significa che solo le persone autorizzate dovrebbero essere in grado di pilotare il drone.
4. **Aggiornamenti del software**: i costruttori di droni dovrebbero fornire aggiornamenti regolari del software per correggere eventuali vulnerabilità di sicurezza scoperte dopo il rilascio del prodotto.
5. **Privacy**: i droni dovrebbero rispettare la privacy degli utenti e non essere in grado di raccogliere o trasferire informazioni personali senza il consenso dell'utente.
6. **Conformità normativa**: i costruttori di droni dovrebbero conformarsi alle norme e alle regolamentazioni di cybersecurity in vigore nei paesi in cui i loro prodotti sono venduti o utilizzati.
7. **Collaborazione con gli utenti**: i costruttori di droni dovrebbero lavorare a stretto contatto con i loro utenti per identificare e risolvere eventuali problemi di sicurezza che potrebbero emergere nel corso dell'uso del prodotto.

Gli obblighi dei fabbricanti, dei distributori e degli importatori sono elencati nel Regolamento delegato (UE) 2019/945 della Commissione, del 12 marzo 2019, relativo ai sistemi aeromobili senza equipaggio e agli operatori di paesi terzi di sistemi aeromobili senza equipaggio.



Etichetta di identificazione di drone Classe C1.

I droni solo classificati secondo la MTOM, sigla che sta per "Maximum Take Off Mass" e che indica la massa massima dal decollo del drone in configurazione operativa: [18]

- **Classe C0**
    - MTOM inferiore a 250 g.
    - Utilizzati per scopi ricreativi e di svago.
    - Nessun requisito formale di licenza.
    - Dotati di sistemi di limitazione della velocità e dell'altitudine.
- **Classe C1**
    - MTOM compreso tra 250 g e 900 g.
    - Utilizzati per riprese fotografiche e video.
    - Registrazione del pilota e del drone.
    - Sistemi di identificazione remota.
    - Dotati di Geo-Fencing.
- **Classe C2**
    - MTOM compreso tra 900 g e 4 kg.
    - Utilizzati per attività commerciali, come l'ispezione di infrastrutture e la mappatura.
    - Formazione e licenza specifica per i piloti.
    - Dotati di sistema di rilevamento e prevenzione delle collisioni.
    - Le zone operative sono definite con limitazioni rigorose.
- **Classe C3**
    - MTOM compreso tra 4 kg e 25 kg.
    - Utilizzati per l'agricoltura di precisione o l'osservazione aerea.
    - Formazione approfondita e licenza specifica per i piloti.
    - Autorizzazioni specifiche per operazioni in aree popolate o vicino a infrastrutture critiche.
- **Classe C4**
    - MTOM superiore a 25 kg.
    - Utilizzati per operazioni militari o per il trasporto di merci.
    - Formazione avanzata e certificazioni specifiche per tipo di operazione.

- Pianificazione rigorosa delle operazioni, con valutazioni del rischio
- Autorizzazioni specifiche e protocolli di sicurezza per operazioni complesse

La convenzione di Budapest

La Convenzione di Budapest obbliga gli Stati membri a criminalizzare gli atti commessi nel cyberspace, suddividendoli in quattro categorie:

1. Reati contro la riservatezza, l'integrità e la disponibilità dei dati e dei sistemi informatici.
2. Criminalità informatica.
3. Reati causati della natura delle informazioni in esso contenute.
4. Reati legati alla violazione del diritto d'autore e dei diritti connessi.

Nella prima categoria, la convenzione sopra citata include:

- Accesso illegale inteso come accesso deliberato e non autorizzato a tutto o parte di un sistema informatico. Le parti in causa possono richiedere che il reato sia commesso mediante una violazione della sicurezza, con l'intento di ottenere dati informatici o con qualsiasi altro intento fraudolento, o in relazione a un sistema informatico collegato a un altro sistema informatico.
- Intercettazione illecita di dati, ossia l'intercettazione intenzionale e non autorizzata, mediante dispositivi tecnici, della trasmissione non pubblica di dati informatici verso, da o all'interno di un sistema informatico, comprese le emissioni elettromagnetiche del sistema informatico che trasmette tali dati informatici. Le parti possono richiedere che il reato sia commesso con intento fraudolento o in relazione a un sistema informatico collegato a un altro sistema informatico.
- Violazione dell'integrità dei dati intesa come distruzione, cancellazione, danneggiamento, modifica o eliminazione deliberata e illegale di dati informatici. Una parte può riservarsi il diritto di richiedere che il comportamento debba comportare un danno grave.
- Violazione dell'integrità del sistema, ossia interferenza deliberata, non autorizzata e alterante il funzionamento del sistema informatico mediante l'introduzione, la trasmissione, la distruzione, la cancellazione, il danneggiamento, la modifica o l'eliminazione di dati informatici.
- Uso improprio di dispositivi inteso come attività deliberata e non autorizzata consistente nella produzione, vendita, acquisizione con l'intenzione di utilizzare, importare, distribuire o condividere in altro modo.

La seconda categoria è quella dei reati informatici, e quindi della contraffazione e della frode informatica. La contraffazione informatica è l'introduzione e la modifica, la cancellazione o l'eliminazione deliberata e non autorizzata di dati informatici, con conseguente creazione di dati non autentici, che l'autore intende far riconoscere o utilizzare a fini leciti come autentici, indipendentemente dal fatto che siano compresi o

comprensibili e che possano essere letti direttamente. Una parte può richiedere che la responsabilità penale si riferisca a un atto fraudolento o a un'analoga intenzione fraudolenta.

Si considera frode informatica la perdita intenzionale e illecita di beni da parte di un'altra persona mediante l'introduzione, la modifica, la cancellazione o l'eliminazione di dati informatici o qualsiasi interferenza con il funzionamento di un sistema informatico, con l'intenzione di ottenere vantaggi economici per sé o per un'altra persona.

La terza categoria riguarda gli atti relativi alla produzione, all'offerta, alla condivisione, all'acquisizione e al possesso illeciti e deliberati di materiale pedopornografico per mezzo di un sistema informatico.

La quarta categoria riguarda la violazione del diritto d'autore e dei diritti correlati con l'uso di un sistema informatico. In modo simile, gli atti contro la sicurezza del cyberspazio sono definiti dal diritto dell'Unione europea, la cosiddetta direttiva sugli attacchi ai sistemi informatici. La direttiva 2013/40 obbliga gli Stati membri dell'Unione Europea a punire tali reati come crimini.

Temi della sicurezza informatica

In questa sezione, faremo una panoramica sulle principali tematiche legate alla sicurezza informatica, per poi declinarle, nello specifico, al mondo dei droni.

I principi della sicurezza informatica si possono riassumere in alcuni concetti chiave:

Autenticità

L'autenticità è la capacità di verificare la propria identità è conforme a ciò con cui ci stiamo dichiarando; in questo modo, si ha la certezza che ogni dato in input proviene da una sorgente autenticata, cioè fidata.

Non ripudio

Il non ripudio è una prova formale, utilizzabile in sede giuridica, riguardo a chi ha creato una determinata informazione. Tramite procedure di autenticazione, ogni azione performata dell'utente è soggetta al non-ripudio.

Autorizzazione

Con il termine autorizzazione, si intende verificare se un utente (autenticato) ha i diritti per eseguire certe operazioni. Anche conosciuta come controllo di accesso, l'autorizzazione va a braccetto con l'autenticazione, poiché sono concetti inseparabili l'uno dall'altro.

Integrità

L'integrità è la capacità di proteggersi da modifiche, o distruzioni, non autorizzate. Il non rispetto di questa proprietà compromette la validità dell'informazione, e con essa la sicurezza dell'intero scambio di dati.

Confidenzialità

La confidenzialità è fondamentale quando vogliamo preservare le restrizioni sull'informazione, proteggendoci da qualsiasi tipo di divulgazione al di fuori dell'ambiente controllato.

Tracciabilità e Responsabilità

In supporto al non ripudio, la tracciabilità serve a legare un'entità a una determinata azione, in maniera univoca.

Tutte queste proprietà astratte trovano applicazioni in ogni campo dove si verifica uno scambio di dati in maniera digitale. Non sempre vi è la necessità di applicarle e rispettarle tutte, molto dipende dagli obiettivi che si vogliono raggiungere: ci concentreremo su una comunicazione che coinvolge un drone e una generica stazione di controllo (Ground Station). In questo scenario, le uniche proprietà che tralasciamo sono il non ripudio e la tracciabilità, poiché non pertinenti allo studio.

Protezione dei dati personali

La protezione dei dati personali coinvolge le proprietà di confidenzialità ed integrità, ed è un aspetto fondamentale quando si utilizzano droni che possono raccogliere e trattare informazioni sensibili. Le principali tematiche da tenere in conto legati al drone in volo sono:

- **Consenso e finalità**
  - È obbligatorio ottenere il consenso delle persone interessate prima di raccogliere e trattare i loro dati personali con un drone. I dati devono essere raccolti solo per scopi specifici e legittimi, e non devono essere utilizzati in modo incompatibile da quanto dichiarato.
- **Limitazione della raccolta**
  - La quantità e il tipo di dati personali raccolti dovrebbero essere limitati, nella quantità e nel tempo, al minimo necessario per raggiungere lo scopo dichiarato.
    - Bisogna evitare la raccolta di informazioni non pertinenti o eccessive, come informazioni sensibili o non rispettose della privacy delle persone.
    - I dati personali raccolti dal drone devono essere conservati solo per il periodo necessario per raggiungere gli scopi dichiarati. Una volta scaduto il periodo di conservazione, i dati devono essere eliminati in modo sicuro e irreversibile
- **Sicurezza dei dati**
  - I dati personali raccolti dal drone devono essere adeguatamente protetti per prevenire l'accesso non autorizzato, l'alterazione, la divulgazione o la perdita dei dati. Ciò può includere l'adozione di misure di sicurezza come crittografia dei dati, autenticazione degli accessi, trasmissione sicura e protezione fisica dei dispositivi di archiviazione.
- **Trasmissione dei dati**
  - Quando i dati personali vengono trasmessi dal drone, ad esempio a un server o a un'infrastruttura di controllo a terra, devono essere adottate misure per garantire la sicurezza della trasmissione. Ciò può includere l'uso di connessioni criptate e protocolli di sicurezza robusti per prevenire l'intercettazione o l'accesso non autorizzato ai dati durante la trasmissione.

Tecniche di autenticazione

In questo ambito, troviamo l'applicazione concreta delle proprietà di autenticazione e di autorizzazione, che come abbiamo detto sono strettamente connesse tra di loro.

User authentication

Per controllare l'accesso all'UAS e alle sue funzionalità, vengono impiegate tecniche di autenticazione degli utenti. Queste possono includere nomi utente e password o metodi più avanzati come l'autenticazione biometrica (impronta digitale, riconoscimento facciale) o l'autenticazione a due fattori (2FA).

Controllo degli accessi in base al ruolo

Role Based Access Control (RBAC) viene comunemente utilizzato per l'autorizzazione negli UAS. Vengono definiti diversi ruoli, come piloti, supervisori o personale di manutenzione, e a ciascun ruolo vengono concessi permessi e diritti di accesso specifici in base alle proprie responsabilità. La RBAC garantisce che solo le persone autorizzate possano eseguire determinate azioni o accedere a funzionalità UAS sensibili.

Geofencing

Tecnica utilizzata per definire il perimetro virtuale nelle aree geografiche. I sistemi UAS possono utilizzare il geofencing per limitare o controllare il movimento dei droni in luoghi specifici. Ciò può includere no-fly zone, spazio aereo limitato o aree in cui le operazioni con i droni sono vietate dai regolamenti. Il geofencing aiuta a prevenire i voli non autorizzati e migliora la sicurezza e la protezione.

Infrastruttura a chiave pubblica

Public Key Infrastructure (PKI) è un sistema che utilizza tecniche crittografiche per gestire certificati digitali e coppie di chiavi pubblica-privata. La PKI può essere usata per scambiare in modo sicuro le chiavi, verificare l'identità delle parti e stabilire canali di comunicazione sicuri tra droni.

Aggiornamenti sicuri del firmware e del software

I sistemi UAS, così come ogni dispositivo elettronico, devono aggiornare regolarmente il firmware e il software per affrontare le vulnerabilità della sicurezza e migliorare la funzionalità. Vengono impiegati meccanismi di aggiornamento sicuri, come la firma e la verifica del codice, per garantire che solo gli aggiornamenti autorizzati e autenticati siano installati sull'UAS, impedendo modifiche non autorizzate.

Sicurezza delle comunicazioni

Per rispettare una qualsiasi delle proprietà sulla sicurezza informatica, nella comunicazione tra drone e Ground Station, non si può prescindere dall'usare una connessione definita sicura, nelle sue varie declinazioni:

Certificati digitali

Gli UAS possono utilizzare certificati digitali per stabilire l'autenticità e l'integrità della comunicazione tra il drone e la Ground Station. I certificati vengono emessi da autorità di certificazione attendibili e vengono utilizzati per verificare le identità sia dell'UAS che della GS. Il formato più comune su cui i certificati si basano è lo standard X509, grazie anche alla sua versatilità.

Crittografia

Tecniche di crittografia vengono utilizzate per proteggere i dati sensibili archiviati sull'UAS e/o trasmessi tra il drone e la GS. La crittografia dei dati garantisce che, anche qualora persone non autorizzate ottenessero l'accesso ai dati, non possono comprenderne il contenuto senza la chiave di crittografia. Queste tecniche contribuiscono in maniera decisiva sulla confidenzialità dell'informazione.

Protocolli di comunicazione sicuri

Protocolli come Transport Layer Security (TLS) o Secure Shell (SSH) possono essere usati per crittografare e proteggere i dati scambiati tra il drone e la GCS. Questi protocolli aumentano l'integrità e la confidenzialità della comunicazione, poiché si basano su standard prestabiliti, rendendo vane le più comuni tecniche di sniffing e spoofing.

Al fine di integrare queste tematiche al mondo delle comunicazioni satellitari, Galileo Open Service ha iniziato lo sviluppo di un algoritmo di autenticazione dei dati per i loro utenti. Si tratta di un servizio che mira a fornire informazioni robuste su posizione, velocità e tempo dei sistemi supportati da Galileo. OSNMA (Open Service Navigation Message Authentication) autentica i dati attraverso il messaggio di navigazione I/NAV, come parte del segnale E1-B. OSNMA è in fase di test pubblico per tutto il 2024, per permettere di avere un primo feedback dagli utenti per scopi di testing.

Questa tecnica fornisce una prima forma di protezione dei dati di navigazione da falsificazioni e manipolazioni, di cui abbiamo discusso prima. Tra i principali settori di applicazione di OSNMA troviamo il trasporto, anche dei sistemi a guida autonoma, le infrastrutture critiche e la finanza, proteggendo le transazioni finanziarie da frodi.

Sistemi di rilevamento delle intrusioni

I sistemi di rilevamento delle intrusioni (IDS) permettono di monitorare il traffico di rete e identificare qualsiasi attività dannosa o non autorizzata all'interno di una rete. Lo scopo principale è quello di rilevare e rispondere a potenziali violazioni della sicurezza o attacchi in tempo reale.

Un IDS agisce analizzando i pacchetti di rete, i registri di sistema e i file di log per rilevare anomalie che possono indicare tentativi di accesso non autorizzati, attività dannose o violazioni delle policy. Sono in grado di rilevare un'ampia gamma di minacce, inclusi attacchi basati sulla rete (come port scanning, attacchi DOS o propagazione di malware) e attacchi basati su host (come tentativi di accesso non autorizzato o exploit a livello di sistema). In particolare, possono essere applicati su un drone per aumentarne: la sicurezza del volo, rilevando tentativi di accesso non autorizzato o hacking ai sistemi interni del drone e intrusioni in spazi aerei riservati, la protezione dei dati e altri comportamenti anomali rispetto al funzionamento usuale. Inoltre, possono contribuire alla prevenzione di collisioni con altri oggetti nello spazio aereo, a valle di un'integrazione tra IDS e sistemi di controllo, sensori e componenti interne al drone.

Ci sono due principali tipologie di IDS:

Network IDS

Un Network IDS è un sistema che permette di monitorare l'intera infrastruttura di rete, analizzando, in tempo reale, ogni pacchetto in entrata e in uscita. Essi possono essere posizionati in livelli diversi della rete, a seconda della strategia adottata.

Gli svantaggi di questo approccio consistono nella necessità di hardware aggiuntivo e nella grande mole di dati da analizzare e gestire, senza però intaccare le prestazioni del sistema.

Host IDS

Un Host IDS lavora sui singoli dispositivi anziché sull'intera rete, ottenendo degli *snapshot* che permettono di comparare i dispositivi in diversi istanti di tempo, per identificare eventuali intrusioni. Agiscono ad un livello più specifico rispetto ai NIDS.

Gli svantaggi derivano dal fatto che la rilevazione avviene sempre dopo l'attacco effettivo (after-the-fact), richiedendo quindi un monitoring costante degli snapshot e dei log files.

Gestione delle chiavi crittografiche

Nella comunicazione tra droni, la gestione delle chiavi è un aspetto cruciale per garantire la sicurezza e la privacy delle informazioni scambiate. Ci sono diversi approcci possibili per gestire le chiavi nella comunicazione tra droni, e la scelta dipenderà dalle specifiche esigenze di sicurezza e dai protocolli adottati.

Di seguito elencati i metodi per lo scambio di chiavi più comuni:

Algoritmi di crittografia

I droni possono utilizzare algoritmi di crittografia asimmetrica o simmetrica per cifrare le comunicazioni. Nell'approccio asimmetrico, ogni drone possiede una coppia di chiavi, una pubblica e una privata. La chiave pubblica può essere condivisa tra i droni per crittografare i dati trasmessi, mentre la chiave privata viene utilizzata per decriptare i dati ricevuti. Nell'approccio simmetrico, tutti i droni condividono una chiave segreta che viene utilizzata sia per la crittografia che per la decrittazione.

Scambio di chiavi

Prima di iniziare una comunicazione, i droni possono utilizzare protocolli di scambio di chiavi, come il protocollo Diffie-Hellman, per stabilire una chiave di sessione condivisa. Questa chiave viene quindi utilizzata per cifrare e decifrare i dati scambiati durante la comunicazione.

Certificati digitali

I droni possono utilizzare certificati digitali per autenticare l'identità di altri droni o entità nella rete. Un certificato digitale è un documento elettronico che viene emesso da un'autorità di certificazione affidabile e contiene informazioni sull'identità del drone, nonché la chiave pubblica associata. Questo permette ai droni di verificare l'autenticità delle chiavi pubbliche degli altri partecipanti alla comunicazione.

Gestione delle chiavi centralizzata

In alcuni casi, una terza entità di fiducia può svolgere il ruolo di gestore delle chiavi centralizzato. Questa entità sarà responsabile della generazione, distribuzione e revoca delle chiavi per i droni coinvolti nella comunicazione. Un approccio centralizzato può semplificare la gestione delle chiavi, ma richiede una certa fiducia nella terza entità.

Open Service Navigation Message Authentication

OSNMA [19] è una funzione di autenticazione dei dati per gli utenti mondiali del Galileo Open Service a livello mondiale, liberamente accessibile a tutti e senza alcun impatto sugli utenti e sulle prestazioni del sistema operativo.

OSNMA fornisce ai ricevitori la certezza che il messaggio di navigazione Galileo ricevuto provenga dal sistema stesso e non sia stato modificato, aumentando così la probabilità di rilevare attacchi di spoofing a livello di dati e contribuendo in modo significativo alla sicurezza della soluzione. OSNMA sarà integrato dal Servizio di Autenticazione Commerciale (CAS), che offrirà l'autenticazione del raggio d'azione nella banda di frequenza E6 Commercial Authentication Service (CAS), che offrirà l'autenticazione della portata nella banda di frequenza E6 (al di fuori dell'ambito di questo studio). I bit OSNMA, che sono per lo più imprevedibili, possono essere sfruttati anche dai ricevitori per fornire un certo livello di protezione contro gli attacchi di replay del segnale.

OSNMA (Open Service Navigation Message Authentication) è una funzione, inclusa in Galileo Open Service, che fornice l'autenticazione dei dati per tutti i ricevitori abilitati. OSNMA autentica i dati per le informazioni relative alla posizione, che provengono da Open Service e sono contenute in un Navigation Message (I/NAV), nella componente E1B del segnale. I dati di autenticazione vengono inseriti in un campo dell'E1 I/NAV Message, fino ad ora tenuto riservato. Nelle comunicazioni broadcast, la protezione delle informazioni, e quindi la loro integrità, è un aspetto necessario per garantire che le informazioni trasmesse non siano state manomesse o non abbiano subito modifiche non autorizzate. L'intento di OSNMA è quello di fornire un metodo standard, efficiente e innovativo, in quanto ad oggi non ne esistono estesi al mondo delle comunicazioni civili.

OSNMA adatta un protocollo di autenticazione broadcast leggero e standard, già esistente, denominato TESLA (Timed-Efficient Stream Loss-Tolerant Authentication), per trasmissioni ottimali sulla rete Galileo. Questa ottimizzazione permette di stabilire un canale monodirezionale condivisa dai satelliti Galileo, insieme alla possibilità di autenticare i satelliti che non trasmettono dati OSNMA recuperando i dati dei satelliti abilitati, con un meccanismo di cross-autenticazione.

Rispetto ad altri protocolli studiati, OSNMA riduce l'overhead sia di computazione che di comunicazione, migliorando l'integrità dei dati scambiati. Sfruttando i campi precedentemente riservati, il messaggio non subisce alterazioni e quindi le performance del sistema non vengono intaccate. Inoltre, questo design permette la retrocompatibilità, in quanto i ricevitori che non supportano OSNMA possono semplicmeente ignorare i dati presenti in quei campi. Un ricevitore abilitato differisce da uno standard per la capacità di recuperare i messaggi OSNMA, all'interno del Navigation Message, e processarli, per verificarne l'autenticità.

Inizialmente, il sistema Galileo genera il Codice di Autenticazione del Messaggio (MAC o bit OSNMA) e lo allega al messaggio di navigazione. Questo viene trasmesso sulla banda Galileo E1 con una chiave, che viene inviata con un ritardo di qualche secondo per autenticare il MAC. L'ordine della chiave generata viene invertito prima dell'invio del messaggio di navigazione.

Una volta che il ricevitore GNSS rileva questo segnale, i dati di navigazione vengono demodulati. Quindi il ricevitore deve recuperare il MAC dal messaggio di navigazione e deve decodificarlo per ottenere le coordinate di navigazione. Il processo di decodifica richiede che la chiave inviata dal sistema Galileo venga autenticata dal ricevente. L'autenticazione avviene riferendo la chiave ricevuta ad una precedente, già verificata, oppure potrebbe fare riferimento ad una chiave root per verificare la stessa. Una volta verificato, il ricevitore rigenera la chiave MAC con i dati, che dovrebbero corrispondere al MAC originale. In questo modo le coordinate di navigazione vengono identificate in modo sicuro dall'OSNMA nel sistema di navigazione Galileo.

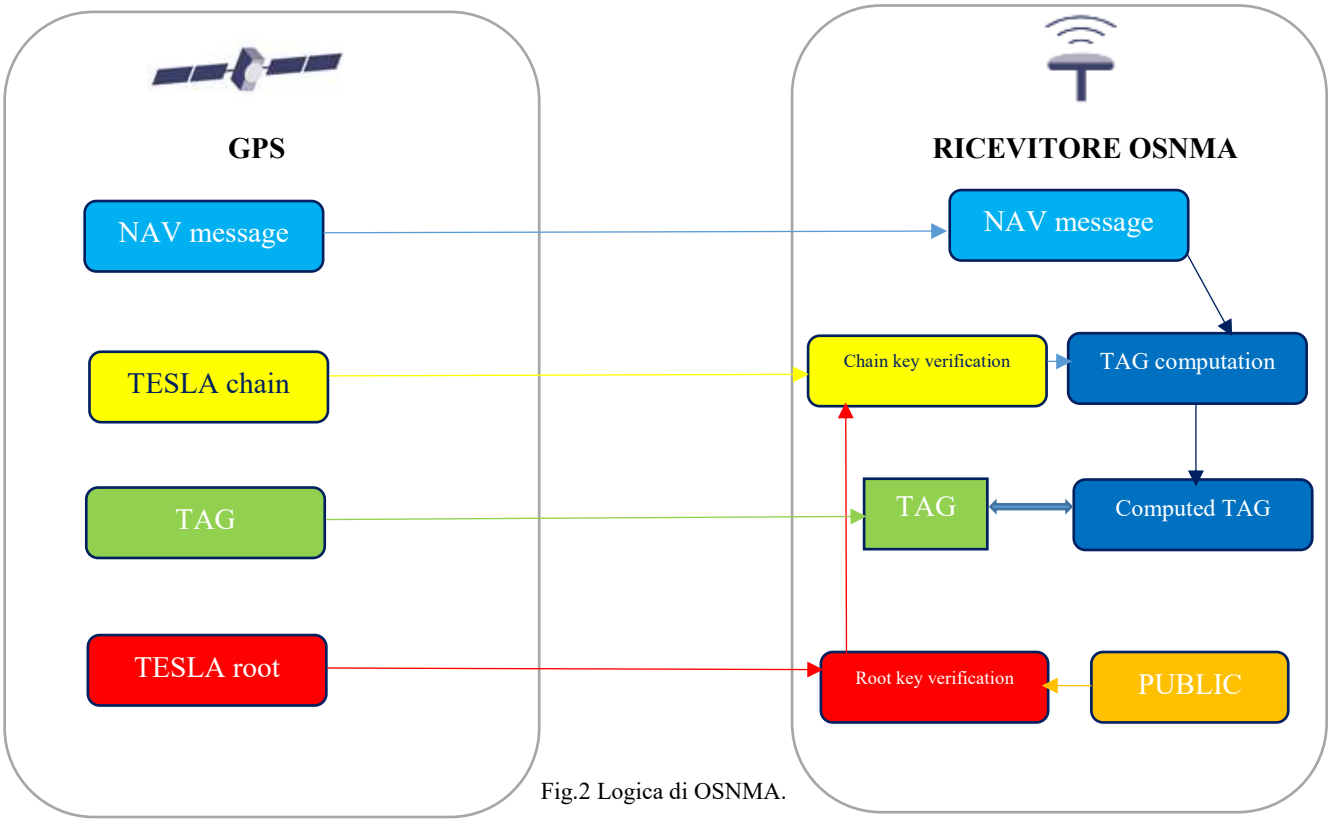


Fig.2 Logica di OSNMA.

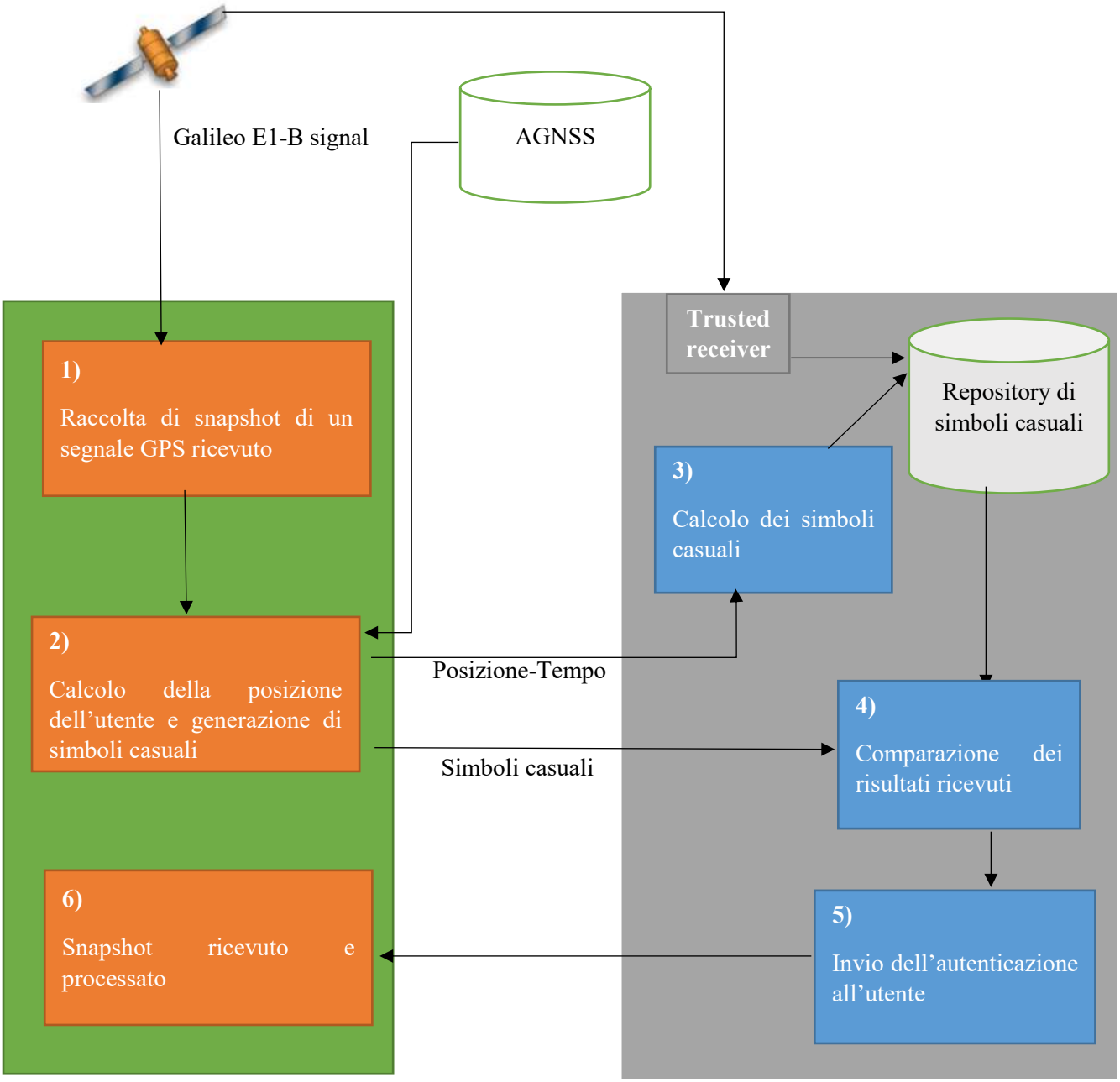


Fig.3 Esempio di comunicazione client server OSNMA.

TESLA Protocol

[20] TESLA (Timed Efficient Stream Loss-tolerant Authentication) è un protocollo di sicurezza che fornisce l'autenticazione di pacchetti broadcast e multicast in maniera efficiente e resistente alle failure, come una perdita di pacchetti. Il funzionamento è basato sulla sincronizzazione temporale libera, ovvero senza bisogno che né il sender né il receiver abbiano una sincronizzazione esatta, ma è sufficiente una finestra temporale con un range di tolleranza. Il sender utilizza una serie di chiavi per firmare i pacchetti, le quali vengono rivelate dopo un certo intervallo di tempo, impedendo ad un attaccante di falsificare i pacchetti stessi. La serie di chiavi utilizzata è parte di una catena (key chain) nella quale ogni chiave dipende (e può essere derivata) dalla precedente, ma non viceversa: ciò garantisce che, qualora ci sia una compromissione di una chiave, questa non può essere usata per ottenere le precedenti.

La prima fase è quella della generazione della chiave, partendo da una chiave segreta K_n, e ogni chiave viene determinata secondo una funzione F non invertibile:

$$Ki\text{-}1=F(K_i)$$

Dopodiché, la finestra temporale è divisa in intervalli di ugual dimensione, ciascuno associato a una chiave K_i. A questo punto, il sender è pronto ad inviare un pacchetto, includendo un Message Authentication Code (MAC) generato a partire dalla chiave K_i. Nel pacchetto è inclusa anche la chiave K_{i-d}, dove d indica il delay necessario per garantire che, nel momento in cui la chiave viene divulgata, i pacchetti autenticati con essa siano già stato ricevuti dai destinatari corretti.

Il receiver memorizza in un buffer il pacchetto fino alla divulgazione della chiave corrispondente; quando ciò avviene, procede alla verifica del MAC usando proprio la chiave appena rilasciata. Contestualmente, si possono verificare anche le chiavi precedenti a partire dalla chiave K_{i-d}.

I vantaggi principali di TESLA sono l'efficienza, in termini di computazione e overhead di comunicazione, resistenza ai malfunzionamenti, come la perdita di pacchetti e infine la scalabilità, poiché il processo di autenticazione non richiede un'interazione con ogni receiver.

Gli unici svantaggi riguardano la sincronizzazione temporale, che sebbene non sia precisa, può risultare problematica in alcuni contesti. Inoltre, viene usato un approccio TOFU (Trust On First Use) con la prima chiave rivelata, di conseguenza è richiesto un meccanismo sicuro di distribuzione delle chiavi a monte di tutto il processo.

La descrizione completa del protocollo TESLA è contenuta nella RFC 4082.

Merkle Tree

OSNMA fa uso del Merkle Tree. Il Merkle Tree, o più comunemente Hash Tree, che viene usato per verificare l'integrità di enormi quantità di dati, in modo sicuro e efficienti. Trovano maggiore utilizzo nell'ambito della blockchain, nelle comunicazioni peer-to-peer o anche nei file system.

Un Merkle Tree è formato da tre tipi di nodi:

- Nodi foglia, ovvero il nodo più basso di tutta la catena, che rappresenta l'hash di un singolo blocco di dati. Solitamente, questi blocchi sono computati con algoritmi di hash come SHA-256
- Nodi intermedi, ovvero tutti i nodi tra la foglia e la radice (root), che vengono calcolati come hash dei due nodi figli in una struttura gerarchica
- Nodo radice, noto come Merkle Root, che identifica da solo l'intero dataset.

La costruzione di un Merkle Tree parte dall'hash di ogni blocco di dati, che andranno a formare i nodi foglia. Successivamente, i nodi foglia vengono accoppiati per formare il nodo successivo, e in caso di disparità dei nodi foglia, si procede alla duplicazione di un nodo. Questo processo viene ripetuto fino a che non si ottiene un singolo nodo, la root.

I vantaggi di questo approccio riflettono quelli di TESLA e consistono nell'efficienza computazionale, dato che non vi è bisogno di processare l'intero dataset, e la scalabilità, dovuta alla sua natura gerarchica; infine risultano particolarmente interessanti per preservare l'integrità, in quanto è facile risalire ad alterazioni nella catena.

Per verificare che un nodo sia parte del Tree corretto, si ricorre a un Merkle Proof, che include l'hash del nodo stesso e quello di ciascun nodo fino alla root.

Per questi motivi, Merkle Tree è una struttura idonea a verificare l'integrità in maniera efficace su qualsiasi tipologia di dato, in particolare negli ambienti dove questa verifica è critica e richiede di essere eseguita in tempi brevi.

Struttura

La struttura di seguito riportata è stata estratta dall'ICD ufficiale di OSNMA, versione 1.1 di ottobre 2023 [21]

HKROOT Message

HKROOT è lungo 15 Byte ed è trasmesso ogni 30 secondi, ovvero ad ogni E1-B I/NAV subframe. Il messaggio è composto da 1 Byte di NMA Header seguito da 14 Byte di DSM, a sua volta diviso in DSM Header (1B) e DSM Block (13B).

NMA Header	**DSM Field**		
NMA Header	**DSM Header**	**DSM Block *n***	Total (Bits)
8	8	104	120

NMA Header

Questo messaggio ha lo scopo di definire lo status del servizio NMA.

NMA Header				
NMAS	CID	CPKS	*Reserved*	Total
2	2	3	1	8

L'ultimo bit è riservato per utilizzi futuri.

- **NMA Status** descrive lo stato generale dello stato di OSNMA, con un valore compreso tra 0 e 3
  - 00: Reserved
  - 01: Test
  - 10: Operational
  - 11: Don't use
- **Chain ID** rappresenta la chain attualmente utilizzata. Il valore viene incrementato ogni volta che a nuova key chain entra in vigore. Dopo 3, il contatore viene ripristinato
- **Chain and Publik Key status** descrive lo stato della chiave pubblica e della key chain attualmente utilizzata, con un valore compreso tra 0 e 7
  - 000: Reserved
  - 001: Nominal
  - 010: End Of Chain (EOC)
  - 011: Chain Revoked (CR)
  - 100: New Public Key (NPK)
  - 101: Publick Key Revoked (PKREV)
  - 110: New Merkle Tree (NMT)
  - 111: Alert Message (AM)

DSM (Digital Signature Message)

Esistono due tipi diversi di DSM:

- **DSM-PKR**, che fornisce la chiave pubblica per verificare la chiave root della TESLA chain
- **DSM-KROOT**, che fornice una KROOT con firma digitale per una TESLA chain.

DSM Header

Questo messaggio, della dimensione di 1B, fornisce informazioni sul blocco DSM trasmesso nel subframe corrispondente.

DSM Header		
DSM ID	DSM Block ID	Total
4	4	8

Un Digital Signature Message è identificato da un DSM ID, mentre ogni blocco ad esso associato è identificato a sua volta da un Block ID univoco.

- **DSM ID**: identifica un numero variabile di blocchi, che va da 0 a 15,

- **DSM Block ID (BID)**: identifica la posizione del blocco all'interno del DSM, con un valore incrementale da 0 a 15

DSM-PKR

DSM PKR						
NB_{dp}	MID	ITN	NPKT	NPK	Padding	Total (Bits)
4	4	1024	4	*l*	*l*	L_{dp}

La lunghezza totale risulterà sempre un multiplo di 104, ovvero la dimensione del blocco DSM. Se necessario, verrà aggiunto un padding alla fine del blocco.

- **Number of DSM-PKR Blocks (NBDP)**

NB_{DP} value	Blocks	Total DSM-PKR length
0-6	*Reserved*	n/a
7	13	1352
8	14	1456
9	15	1560
10	16	1664
11-15	*Reserved*	n/a

- **MID** identifica quale foglia del Merkle Tree viene fornita.

MID value	Merkle Tree Leaf
0..n	$M_{0..n}$

- **Intermediate Tree Nodes (ITN)** fornisce informazioni sui 4 nodi del Merkle Tree necessari ad autenticare il messaggio identificato dal MID. I nodi sono inviati nell'ordine della tabella sopra.
- **New Public Key Type (NPKT)** rappresenta l'algoritmo di firma associato alla chiave pubblica fornita nel blocco DSM-PKR.

MID value	Merkle Tree Leaf
0	*Reserved*
1	ECDSA P-256
2	*Reserved*
3	ECDSA P-521
4	OSNMA Alert Message
5-15	*Reserved*

- **New Publick Key ID (NPKID)** rappresenta l'ID della nuova chiave pubblica. Se NPKT vale 4, il valore di NPKID è 0, per poi andare in ordine incrementale.
- **New Publick Key** è il campo che contiene la nuova chiave pubblica, fornita mediante compressione di ECDSA.

Key Type	NPK size
ECDSA P-256	264
ECDSA P-521	536

DSM-KROOT

Fornisce la root della key chain attualmente in vigore, al fine di autenticare ogni chiave appartenenti alla stessa catena. Inoltre, sono fornite le funzioni di crittografia, la dimensione delle chiavi e dei tag, e altri parametri a seconda della catena.

DSM-KROOT																
NB_{dk}	PKID	CIDKR	*res*	HF	MF	KS	TS	MACTL	*res*	WN_k	$TOWH_k$	α	KROOT	DS	P_{dk}	Tot
4	4	2	2	2	2	4	4	8	4	12	8	48	l_k	l_{ds}	l_{pdk}	l_{DK}

- **Number of DSM-KROOT Blocks (NBDK)** identifica il numero di blocchi, che corrisponde ciascuno a 104 bits di un DSM.

NB_{DK} value	Blocks	Total DSM-KROOT length
0	*Reserved*	n/a
1	7	728
2	8	832
3	9	936
4	10	1040
5	11	1144
6	12	1248
7	13	1352
8	14	1456
9-15	*Reserved*	n/a

- **Public Key ID (PKID)** rappresenta l'ID della chiave pubblica usata per verificare la firma digitale di DSM-KROOT.
- **KROOT Chain ID (CIDKR)** identifica la catena di appartenenza del KROOT.
  - CIDKR e CID di NMA header potrebbero essere differenti, nel caso di rinnovamento di una catena.
- **Hash Function:** identifica la funzione MAC utilizzata per autenticare i navigation data.

MF value	Hash function
0	HMAC-SHA-256
1	CMAC-AES
2	*Reserved*
3	*Reserved*

- **Key Size (KS)** identifica la dimensione della chiave utilizzata, in bit.

KS value	Key Length
0	96
1	104
2	112
3	120
4	128
5	160
6	192
7	224
8	256
9-15	*Reserved*

- **Tag Size (TS)** identifica la dimensione del tag, in bit.

TS value	Tag Length

0-4	*Reserved*
5	20
6	24
7	28
8	32
9	40
10-15	*Reserved*

- **MAC Look-up Table (MACLT)** corrisponde alla entry della look-up table che specifica la sequenza Authentication Data e Key Delay (ADKD) dei messaggi MACK. Una look-up table può identificare fino a 256 sequenze.
- **KROOT Week Number e Time of Week (WNK e TOWHK)** sono i parametri conformo al Galileo System Time (GST), associati ad una KROOT.
- **Random Pattern α** è un pattern casuale inserito nel processo di hash della catena.
- **KROOT** è la root key associata a un Kroot time, firmata e inserita nella catena nel DSM-KROOT.
- **Digital Signature (DS)** è la firma digitale di DSM-KROOT.
- **DSM-KROOT Padding (P_{dk})** se necessario, viene aggiunto per raggiungere la dimensione del blocco multipla di un blocco DSM.

MACK Message

Il MACK Message è lungo 60 Byte ed è trasmesso ogni 30 secondi, esattamente come per i Data Message. Ognuno di questi messaggi contiene diversi MAC troncati, detti tag, con una TESLA key e information data associati.

MACK Message				
MACK Header	Tag & Info	Key	Padding	Total (Bits)

MACK Header

MACK Header			
Tag_0	MACSEQ	COP	Total (Bits)
l_t	12	4	l_{MH}

- **Tag_0** è ottenuto troncando un MAC con ADKD = 0. La size l_t è dichiarata nel campo Tag Size in DKM-ROOT.
- **MACSEQ** permette al ricevitore di autenticare il campo Tag-Info quando ADKD è identificato come flessibile nella MAC Look-up Table.
- **Data Cut-Off Point (COP)** usato per l'encoding del parametro Data Cut-Off.
- **Tags & Info:** il numero di tag associabile ad ogni messaggio è variabile e dipende dalle dimensioni della key e del tag stesso.

Tag & Info						
Tag 1		**Tag 2**		**..**	**Tag_{n-1}**	
Tag	Tag-Info	Tag	Tag-Info	..	Tag	Tag-Info

l_t	16	l_t	16	..	l_t	16

- **Tag Info** contiene le informazioni necessarie per generare un tag e identificare gli Authentication Data corrispondenti.

Tag Info			
PRN_d	ADKD	COP	Total (Bits)
8	4	4	16

  - **PRN_d** identifica il satellite, autenticati dal suo tag, che trasmette i dati.
    -

PRN_d value	**Meaning**
0	*Reserved*
1-36	Galileo SV_{ID} 1-36
37-254	*Reserved*
255	Informazioni non specifiche del satellite

  - **ADKD**

ADKD value	**Authenticated Data**
0	Ephemeris, Clock and Status
1-3	*Reserved*
4	Timing parameters
5-11	*Reserved*
12	Slow MAC
13-15	*Reserved*

  - **COP** il valore 0 indica un dummy tag, mentre i restanti valori i restanti 15 bit indicano la massima latenza, T_{COP}, tra il tag e i dati autenticati associati.

Risultati sperimentali

Hardware

Nella fase di testing, mi sono avvalso di una Macchina Virtuale, creata con VirtualBox, con sistema operativo Linux. In particolare, è stato usato Ubuntu in versione 20.04, ma si potrebbe usare una qualsiasi versione, in quanto non vi sono particolari richieste da parte del software.

La board, che mi è stata fornita dall'azienda proprio per provare questo software, è una Orange Pi Zero LTS, le cui specifiche sono riportate in Fig.2. I vari settaggi significativi per il test sono:

- Linux versione 14.04
- GCC versione 8.4

Per il resto, nessuna specifica è stata modificata, essendo la board già utilizzata per altri progetti interni all'azienda.

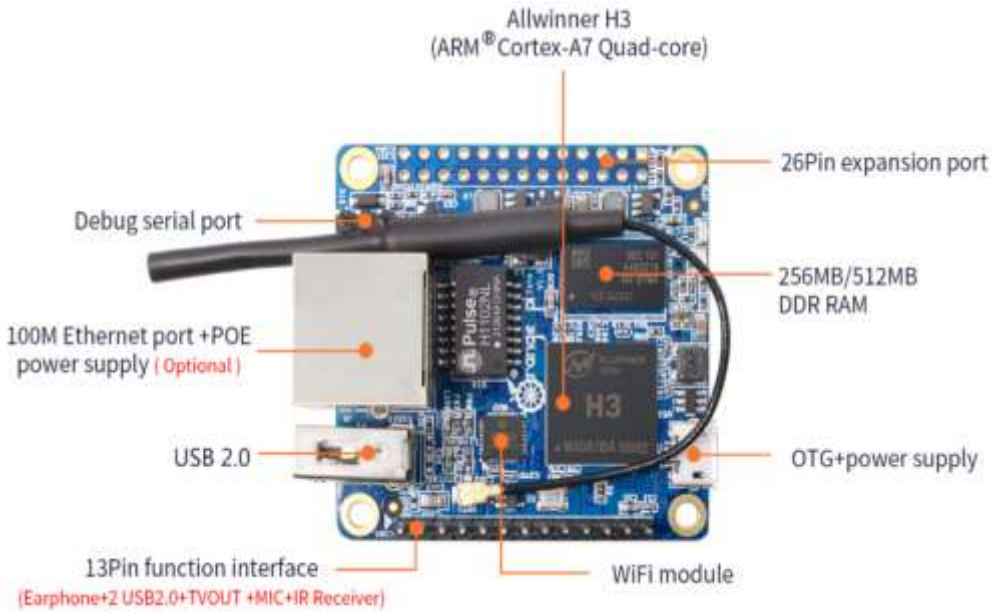


Fig. 2 Informativa Orange Pi 0

Infine, la connessione tra board e PC è stata realizzata inizialmente mediante Ethernet, infine tramite seriale, come vedremo in seguito.

Per dare una valutazione generale delle prestazioni, dei consumi e overhead sul sistema dell'algoritmo, ho preso in considerazione tre parametri, riguardanti ciascuno di questi aspetti tempistico-occupazionali. Il primo parametro è il classico CPU usage, che indica la percentuale di CPU utilizzata dal processo *galmon-osnma*, considerando trascurabili gli altri processi in esecuzione sulla board. Il secondo parametro è stato il memory usage, che indica la percentuale di memoria utilizzata, partendo da un 10% di consumo in idle. L'ultimo parametro riguarda il system load, una metrica più generale, misurata su differenti intervalli di tempo, che indica il sovraccarico sul sistema.

Tutte queste misurazioni sono state fatte su un numero crescente di thread, lanciati al momento di esecuzione dell'applicativo, tenendo come limite superiore 100. Questi test sono stati effettuati al fine di sperimentare l'utilizzo della board per connettersi a più feed contemporaneamente, per simulare la ricezione di messaggi provenienti da sorgenti diverse, valutando il sovraccarico della macchina in tale condizione.

La board utilizzata, che monta un processore quad core, riesce a gestire un numero ragionevole di thread in esecuzione, che si attesta intorno ai 10, come verificato dal system load.

Software

OSNMA, essendo ancora in fase di test, è in continua evoluzione, così come le chiavi riconosciute e distribuite dal sito EUSPA (European Union Agency for Space Programme). Al momento del test, sono state usate le versioni aggiornate a gennaio 2024, è possibile pertanto che, per testare il programma in futuro, sia doveroso chiedere nuovamente l'invio dei file.

Dopo essersi registrati come tester nel sito di EUSPA, la chiave pubblica per accedere a tutti i servizi offerti da Galileo viene fornita in tre file separati:

- OSNMA_Merkle_Tree.xml
- OSNMA_PublickKey.crt
- Digital Certificates.crl

OSNMA è disponibile open source su Github sia in linguaggio Rust (https://github.com/daniestevez/galileo-osnma) che in Python (https://github.com/Algafix/OSNMA). Così come le chiavi pubbliche, entrambe le alternative vengono spesso aggiornate, in accordo con le nuove linee guida presenti nell'ultimo ICD.

Per eseguire i test è stata scelta la versione di Rust, in modo da avere un eseguibile compilato su una VM e poi trasferito sulla board.

Una volta clonato il repository, è stato necessario cross-compilare il codice, compatibilmente con l'architettura presente sulla board. Il compilatore scelto è stato *gnueabif*, mentre l'istruzione

cargo build --target arm-unknown-linux-gnueabihf --config target.arm-unknown-linux-gnueabihf.linker=\"arm-linux-gnueabihf-gcc\"

è stata necessaria per generare l'eseguibile correttamente.

Per fornire l'accesso a internet alla board, ci sono due alternative:

- Abilitare il modulo WiFi nella board
- Condividere, tramite Ethernet, la propria connessione

Tutta la comunicazione tra Macchina Virtuale e board è avvenuta tramite protocollo SSH.

Per ottenere una chiave pubblica in formato pem, come si aspetta il software Rust in input, è bastato eseguire il comando:

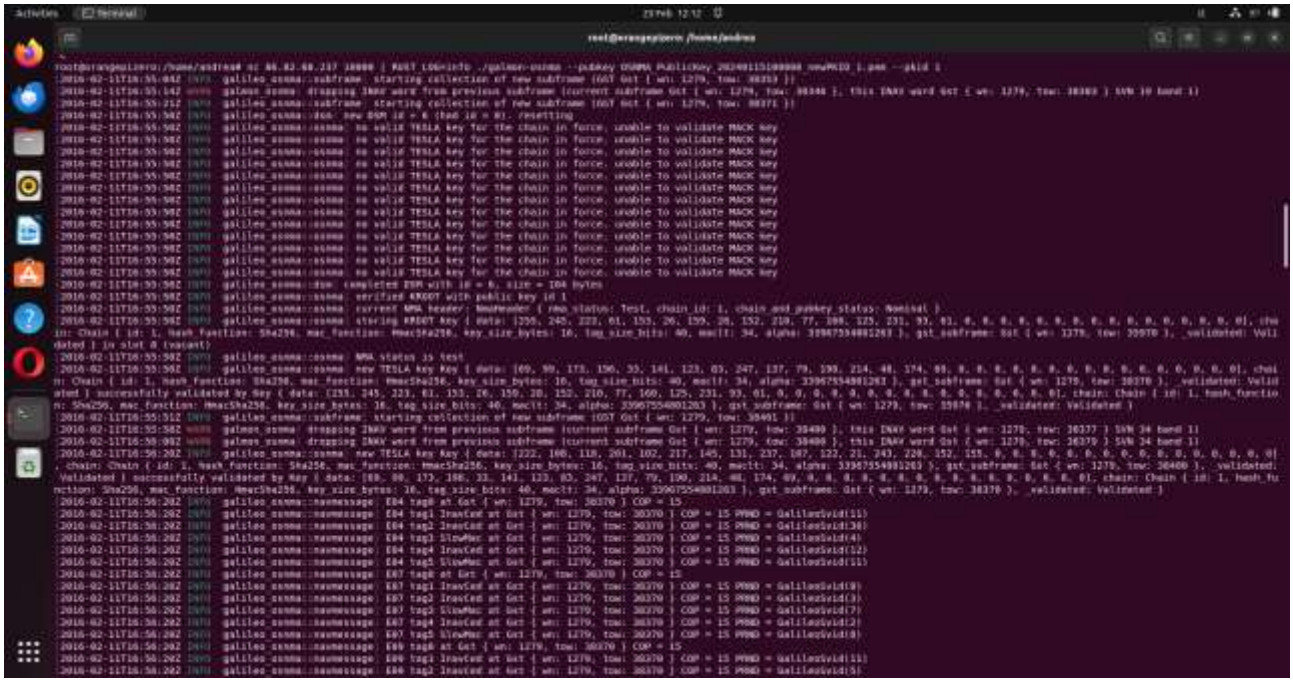
openssl x509 -pubkey -noout -in OSNMA_PublicKey_20240115100000_newPKID_1.crt > pubkey.pem

Per ottenere i dati di autenticazione di Galileo, è stato usato un live feed, fornito da Bert Hubert, autore di *galmon* (Galileo Monitoring), raggiungibile all'indirizzo 86.82.68.237 alla porta 10000. I dati di input sono in una codifica BERT, che viene interpretata dal programma *galmon-osnma*, lanciato con il comando seguente:

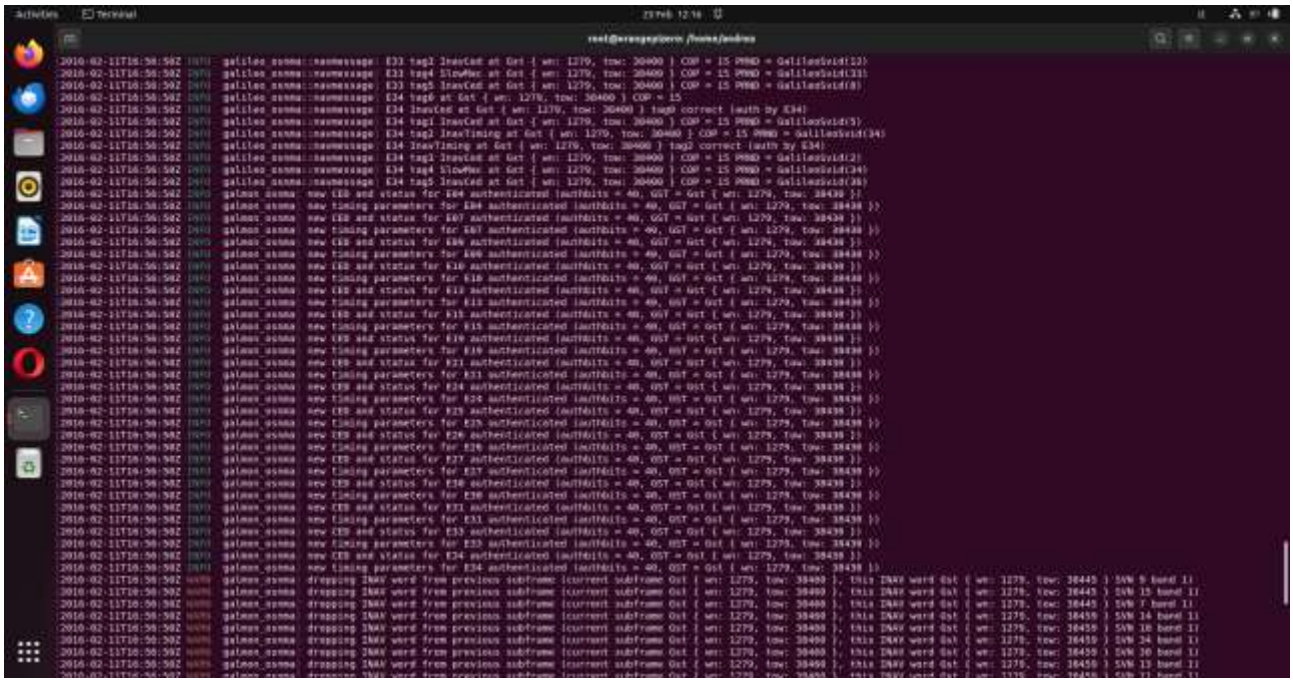
nc 86.82.68.237 10000 | ./galmon-osnma –pubkey OSNMA_PublicKey_20240115100000_newPKID_1.pem --pkid 1

dove *pubkey* è la chiave generata precedentemente e *pkid* è il suffisso, incrementale ad ogni nuovo rilascio, del file pem.

A questo punto, il software è pronto per leggere i vari messaggi di autenticazione sulla rete:



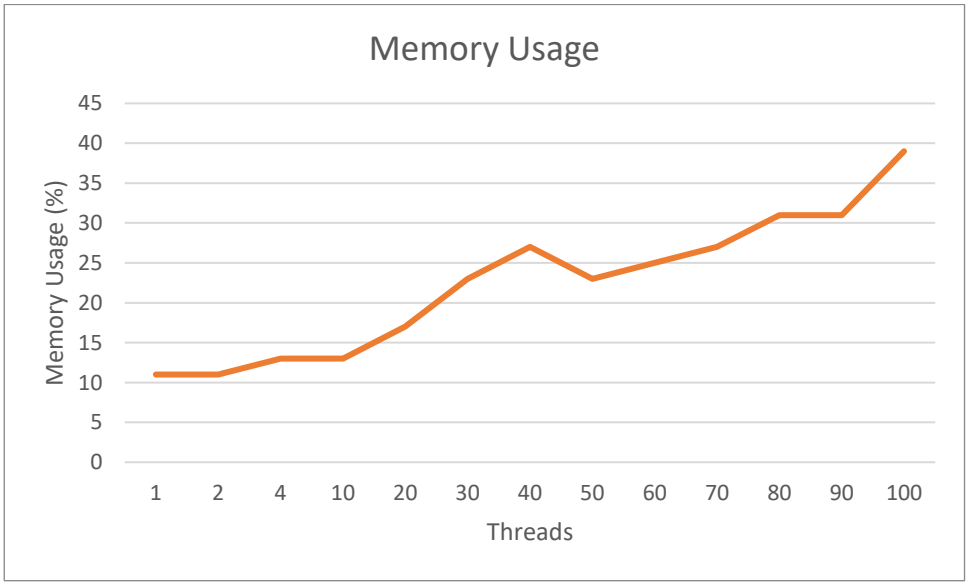
Il primo messaggio significativo è quello relativo allo store della KROOT key, provenienti dal modulo *dsm* che permette di autenticare la TESLA chain, necessaria a ricevere i messaggi dai vari satelliti Galileo (E02.. E36). Dopodiché, i messaggi di autenticazione arrivano dal modulo *navmessage*, con relativi numero di finestra *wn* e time of the week *tow*. Questi ultimi vengono aggiornati periodicamente (ogni 15 secondi) e autenticati alla ricezione. In caso di arrivo di messaggi con un *tow* precedente, questi vengono scartati e un warning viene generato.



Il significato dei parametri *wn* e *tow* è connesso al protocollo TESLA, che, come abbiamo discusso prima, si basa sulla firma di un messaggio con una chiave simmetrica, che dovrebbe essere mantenuta segreta, e pubblicata dopo un breve ritardo e concatenarla in modo che la chiave simmetrica possa essere utilizzata per derivare chiavi simmetriche precedenti.

Overload e Memory Usage

L'utilizzo della memoria presenta un andamento anomale in corrispondenza all'esecuzione di circa 50 thread, questo potrebbe essere dovuto all'architettura dell'Orange Pi Zero, che, a una certa soglia di occupazione della memoria, fa intervenire la partizione di Swap. Si tratta tuttavia di un algoritmo che, come previsto, non richiede un uso intensivo della memoria.



Per quanto riguarda l'overload del processo sul sistema, mi sono basato su due parametri: oltre alla classica CPU usage, ho voluto monitorare un altro parametro chiamato system load, ovvero una metrica per misurare le performance del sistema tenendo conto dei task in esecuzione sulla CPU. Tale metrica è espressa come numero medio di processi in stato di esecuzione negli ultimi 1, 5 oppure 15 minuti. Il sistema si definisce sovraccarico se il system load è superiore al numero di core presenti, nel nostro caso 4. Orange Pi Zero è già sovraccarica dopo circa 10 esecuzioni parallele.

```
root@orangepizero:~# echo 60 && /etc/update-motd.d/30-sysinfo
60
System load:   46.98 24.62 14.36        Up time:        1:46 hour
ocal users:    2
Memory usage:  25 % of 494MB    IP:             192.168.137.2 192
43.236
CPU temp:      80°C
Usage of /:    20% of 7.1G

root@orangepizero:~#
```

I risultati possono essere ottenuti con il comando */etc/update-motd.d/30-sysinfo*, che fa parte dei messaggi all'accensione, oppure con *top*, entrambi forniscono i dati di nostro interesse. La tabella Fig.3 è relativa ad un minuto di esecuzione. Una media più alta indica un utilizzo maggiore delle risorse.

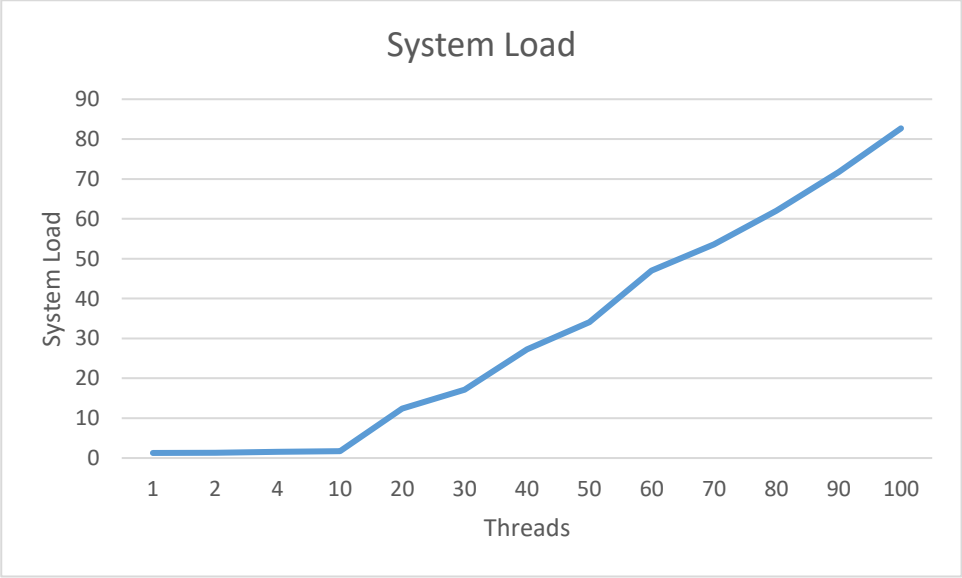
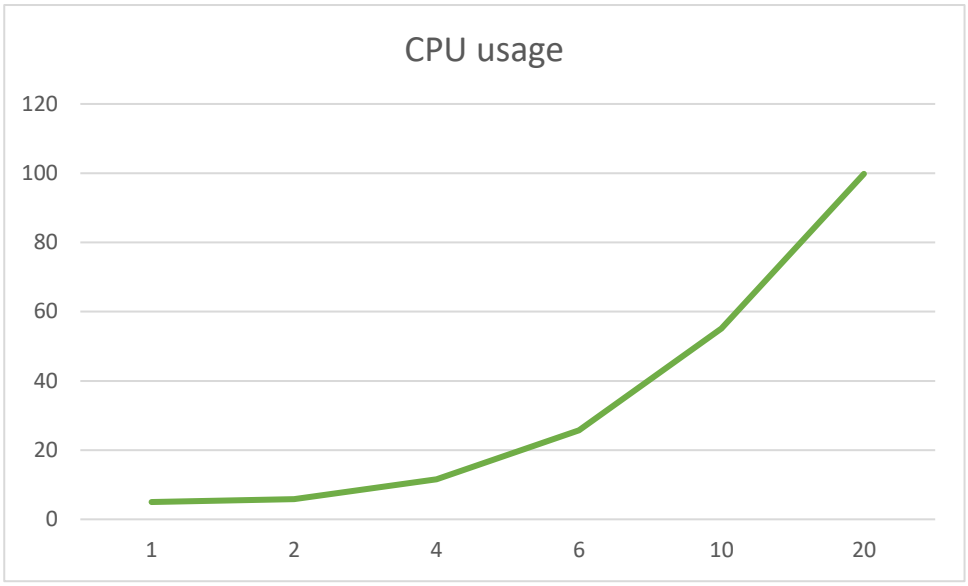


Fig.3 Overload del sistema

Si può notare come lo stress del sistema cresca in maniera lineare con l'aumentare delle istanze di *galmon-osnma* eseguite, anche se, di fatto, il sistema diventa sovraccarico già intorno ai 20 e inutilizzabile dopo i 70 thread in esecuzione.

Di seguito, infine, è mostrata l'utilizzo della CPU.



Si può notare che dopo i 10 thread di esecuzione, la CPU raggiunge velocemente la soglia di 100% di utilizzo.

Durante l'esecuzione di questi test, la scheda è risulta irraggiungibile via SSH, a causa di un servizio (OpenSSH) che non parte all'avvio del sistema. È stato necessario, per continuare con le misurazioni, accedere alla Orange Pi tramite interfaccia seriale in Fig.4, creare la cartella /var/run/sshd e far partire manualmente il

servizio ssh.

Fig.4

Conclusioni e sviluppi futuri

Conclusioni

A fronte dei risultati ottenuti nella parte sperimentale, è possibile trarre alcune conclusioni, riassumendo tutti i punti toccati fino a qui.

L'assenza di specifici protocolli, nel campo dei droni civili, può presentare svariate problematiche, in diverse componenti del drone stesso, oltre che nel suo comportamento in volo. Tali velivoli, essendo dotati di sistemi a pilotaggio remoto, sono suscettibili a tutte le minacce già note nella letteratura ICT. È importante dunque, integrare delle contromisure, ad oggi manualmente, nel sistema fisico. Nello scegliere tra le varie soluzioni, bisogna considerare il nostro sistema target, ovvero un drone, nel quale la componentistica hardware non presenta prestazioni di alto livello, almeno nell'ambito civile. Di conseguenza, dopo una panoramica sulle principali soluzioni possibili, ci si è concentrati su OSNMA. Open Service Message Navigation Authentication (OSNMA) è la soluzione, proposta da Galileo, al problema dell'autenticazione dei segnali di geolocalizzazione nel sistema Galileo; la caratteristica che lo rende molto interessante, soprattutto in ambito civile, è la possibilità di essere usato su un sistema general purpose, senza particolari necessità hardware.

In questa tesi abbiamo preso come riferimento a OrangePi Zero, una board dalle prestazioni non eccellenti, ma comunque adatte ad essere installata su un computer di bordo, che può quindi simulare fedelmente un comparto hardware montato su un drone. I risultati ottenuti dimostrano come OSNMA possa essere effettivamente utilizzabile e implementabile su buona parte dei dispositivi oggi in commercio. Tuttavia, è auspicabile un impegno maggiore, da parte delle case produttrici, nel produrre dispositivi che già implementano un meccanismo di autenticazione, seppur basilare, ma di facile comprensione da parte dell'utente finale.

Sviluppi futuri

In ultima analisi, diamo uno sguardo a quelli che possono essere i trend più innovativi nel settore. Le nuove tendenze, in particolare in ambito cybersecurity dei droni, possono essere dettate non solo dall'introduzione di nuove tecnologie emergenti, ma anche dalle minacce, sempre più diffuse e sofisticate, che possono emergere in qualsiasi momento.

AI

La prima tematica che viene in mente, sempre più popolare di giorno in giorno, è quella dell'Intelligenza Artificiale, che trova applicazione anche e soprattutto nel settore della sicurezza informatica. Come riportato da *isaca.org* [22], l'AI risulta particolarmente effettiva nei seguenti frangenti:

- **Rilevamento di minacce**

    - Grazie alla capacità di analisi di grandi quantità di dati, in tempo reale, l'AI è in grado di identificare anomalie che possono essere collegate ad un attacco informatico. Inoltre, gli algoritmi di Machine Learning possono imparare da esempi passati, migliorando l'analisi con rilevazioni più accurate e previsioni più precise. È dunque possibile studiare una strategia attiva e da queste minacce, adottando tecniche di difesa in tempo reale.
- **Risposta automatica**
    - Di conseguenza, adottare una strategia difensiva, come un cambio improvviso di rotta in fase di volo, non necessita di un intervento umano immediato.
- **Crittografia e manutenzione predittiva**
    - Gli algoritmi di AI possono essere impiegati nel corso delle comunicazioni tra i droni, sia per operazioni di crittografia avanzate, che per rilevare eventuali problemi, derivanti da malfunzionamenti tecnici o da falle nella sicurezza, che potrebbero trasformarsi in vere e proprie minacce

Per contro, l'Intelligenza Artificiale può essere utilizzata anche da utenti malintenzionati, poiché gli algoritmi di Machine Learning possono imparare dagli attacchi passati e sviluppare nuove minacce esplicite, non facili da prevedere.

Blockchain

La tecnologia blockchain offre una strategia di controllo e di verifica decentralizzata, sfruttando la DLT (Distributed Ledged Technology). Il processo di verifica si appoggia ad un apposito registro, distribuito e immutabile, aggiornato con transazioni sicure e disponibile, sotto forma di copia locale, ad ogni nodo della blockchain.

Il vantaggio più importante, in termini di sicurezza, è l'eliminazione da un lato delle dipendenze da autorità di certificazione centralizzate, una delle entità più coinvolte nei data breach, dall'altro della necessità di password superflue.

Questo approccio, molto più ricco di quanto possa sembrare, può essere adottato nelle soluzioni a pilotaggio remoto, facendo agire ogni drone come nodo della blockchain. Il tradeback di questa soluzione risiede nella maggiore complessità hardware richiesta per un corretto funzionamento della blockchain.

Quantum Computing

Un punto cruciale legato alla cybersecurity è rappresentato dall'avvento dei computer quantici, che, grazie alla potenza di calcolo sensibilmente più potente di qualsiasi macchina attualmente disponibile, rischiano di cambiare radicalmente i paradigmi e le certezze sui cui si basano tutte e teorie di crittografia esistenti.

CSA (Cloud Security Alliance) stima che nel 2030[23], precisamente il 14 aprile[24], i computer quantistici saranno in grado di superare tutti gli algoritmi non quantum-safe, alla quale classe appartengono soltanto alcuni

algoritmi di crittografia a chiave pubblica come le QKD (Quantum Key Distribution). Per tutti gli altri algoritmi, i computer quantici riescono a risolvere problemi matematici, che ora richiederebbero molto tempo e risorse, in un lasso di tempo molto minore: un esempio riguarda tutte le equazioni che coinvolgono grandi numeri primi, oggi molto complesse, ma facilmente risolvibili da un computer quantico con l'algoritmo di Shor.

Altri trend

L'integrazione dei droni con le reti 5G permetterà ai droni di inviare dati in real-time, che unita alla presenza di AI, potrà trovare applicazioni nei settori riguardanti le emergenze.

L'implementazione del Remote ID, anche con l'introduzione di nuove leggi specifiche, potrebbe rendere obbligatorio, per ciascun drone, la trasmissione di dati relativi alla propria identità e posizione; questa tecnologia riscontra, però, un impatto forte sulla questione della privacy, rendendola così di difficile realizzazione sotto l'aspetto legislativo.

Bibliografia

[1] 2024, A Brief History of Drones | Imperial War Museums (iwm.org.uk)

[2] Brad Silver, "Welcome to the era of drone-powered solutions: a valuable source of new revenue streams for telecoms operators." *pwc.com*, 2017, www.pwc.com/gx/en/communications/pdf/communications-review-july-2017.pdf

[3] Fortune Business Insights, "Unmanned Aerial Vehicle Market to Worth USD 91.23 Billion by 2030", *globenswire.com*, 2023, https://www.globenewswire.com/news-release/2023/12/20/2799010/0/en/Unmanned-Aerial-Vehicle-Market-to-Worth-USD-91-23-Billion-by-2030-UAV-Industry-Report-by-Fortune-Business-Insights.html

[4] Regolamento Mezzi Aerei a Pilotaggio Remoto, 2016, *enac.gov.it*, https://www.enac.gov.it/ContentManagement/information/N122671512/Regolamento_APR_ed2_em2.pdf

[5] Regolamento di Esecuzione (UE) 2019/947 della Commissione del 24 maggio 2019, https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32019R0947

[6] Drones & Air Mobility, 2024, *easa.europa*, https://www.easa.europa.eu/en/domains/civil-drones

[7] Complete guide to GDPR compliance, 2024, https://gdpr.eu

[8] ENISA, Foresight Cybersecurity Threats for 2030, 2023, *enisa.europe.com*, https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030

[9] UAS Integration, 2023, *eda.europa.com*, https://eda.europa.eu/what-we-do/all-activities/activities-search/remotely-piloted-aircraft-systems---rpas

[10] Commission Implementing Regulation (EU) 2023/203, https://www.easa.europa.eu/en/document-library/regulations/commission-implementing-regulation-eu-2023203

[11] https://www.faa.gov/uas

[12] Transport Canada, Flying your drone safely and legally, 2023, *tc.canada.ca*, https://tc.canada.ca/en/aviation/drone-safety/learn-rules-you-fly-your-drone/flying-your-drone-safely-legally

[13] Drone rules, *casa.gov.au*, https://www.casa.gov.au/knowyourdrone/drone-rules

[14] Drone Laws in Japan, 2024, *drone-laws.com*, https://drone-laws.com/drone-laws-in-japan

[15] Drone Laws in China, 2024, *uavcoach.com*, https://uavcoach.com/drone-laws-in-china

[16] Flying drones and model aircraft, 2024, https://register-drones.caa.co.uk

[17] https://www.easa.europa.eu/en/the-agency/faqs/cybersecurity

[18] Regolalemto Delegato (UE) 2019/945 della Commissione del002012 marzo 2019 https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32019R0945

[19] https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo_OSNMA_Info_Note.pdf

[20] Adrian Perrig, The TESLA Broadcast Authentication Protocol, 2002, https://people.eecs.berkeley.edu/~tygar/papers/TESLA_broadcast_authentication_protocol.pdf

[21] Galileo OSNMA ICD v1.1, 2023 https://www.gsceuropa.eu/sites/default/files/sites/all/files/Galileo_OSNMA_SIS_ICD_v1.1.pdf

[22] Justin Rende, "Track These 7 Trends for Proactive Cybersecurity in 2024", *icasa.org*, Track These 7 Trends for Proactive Cybersecurity in 2024

[23] Enterprises must begin preparing now to secure themselves in a post-quantum world, Cloud Security Alliance Sets Countdown Clock to Quantum | Business Wire, *businesswire.com*

[24] Cloud Security Alliance Countdown Clock, https://cloudsecurityalliance.org/research/working-groups/quantum-safe-security