Original Scientific Paper/Originalni naučni rad UDC/UDK: 004.4:623.746-519
Paper Submitted/Rad primljen: 05.06.2025.
Paper Accepted/Rad prihvaćen: 28.06.2025.
DOI: 10.5937/SJEM2502061M

Unapređenje SecuDroneComm platforme: Uporedna analiza savremenog stanja sa modernim IKT platformama za bezbednu komunikaciju

Rexhep Mustafovski[1]

[1] Ss. Cyril and Methodius University, Faculty of Electrical Engineering and Information Technologies, Skopje, North Macedonia, rexhepmustafovski@gmail.com

Apstrakt: Brzi razvoj IKT rešenja značajno je transformisao bezbednu komunikaciju bespilotnih letelica (UAV). Ovaj rad predstavlja SecuDroneComm - hibridnu platformu osmišljenu za sigurnu i niskolatentnu komunikaciju između drona i komandnog centra. Platforma se upoređuje sa IKT okvirima poput ITU-T X.805, SmartNet arhitekture i sistema sa federativnim identitetom, s fokusom na enkripciju, arhitekturu servera i strategije implementacije. SecuDroneComm koristi hibridne servere, SDN-slične koordinatore i napredne bezbednosne protokole (TLS 1.3, OAuth, AES-256), što je čini pogodnom za primenu u ratnim uslovima, vanrednim situacijama i zdravstvu. Buduća unapređenja uključuju 5G mreže, validaciju zasnovanu na blokčejnu i naprednu kontrolu pristupa. Usklađena sa savremenim IKT trendovima, platform SecuDroneComm pokazuje visok potencijal da postane referentno rešenje za sigurnu i skalabilnu komunikaciju UAV sistema u dinamičnim okruženjima.

Ključne reči: SecuDroneComm, sigurne IKT platforme, hibridna serverska arhitektura, komunikacija bespilotnih letelica (UAV), razmena podataka u realnom vremenu

Advancing SecuDroneComm: A Comparative State-of-the-Art Analysis with Modern ICT Platforms for Secure Communication

Abstract: The rapid growth of ICT has transformed secure UAV communication. This paper presents SecuDroneComm, a hybrid platform designed for secure, low-latency drone-to-command communication. It is compared with ICT frameworks like ITU-T X.805, SmartNet, and federated identity systems, focusing on encryption, architecture, and deployment. SecuDroneComm uses hybrid servers, SDN-like coordinators, and robust security (TLS 1.3, OAuth, AES-256), making it suitable for battlefield, disaster, and health missions. Future enhancements include 5G, blockchain, and advanced access control. Aligned with modern ICT trends, SecuDroneComm shows strong potential as a benchmark for secure, scalable UAV communications in dynamic environments.

Keywords: SecuDroneComm, Secure ICT Platforms, Hybrid Server Architecture, UAV Communication, Real-Time Data Exchange

1. Introduction

In today's fast-paced technological landscape, secure communication systems are essential for modern infrastructure, facilitating everything from personal devices to extensive industrial and military operations. The rise of drones and their incorporation into critical systems has introduced additional complexity and significance to these platforms. These unmanned aerial vehicles (UAVs) have evolved from specialized tools to vital assets in areas such as surveillance, disaster response, logistics, and defense. However, their growing deployment also presents challenges in ensuring secure, real-time communication between drones, their control centers, and the wider network. SecuDroneComm, a hybrid platform aimed at providing secure communication between drones and their command centers, stands out as a timely and innovative solution. It is built on the foundations of advanced ICT systems, utilizing technologies like AES-256 encryption, TLS 1.3, and hybrid server architectures to guarantee data integrity, confidentiality, and availability.

Although current systems have made progress in tackling these issues, there are still gaps in scalability, adaptability, and the capacity to integrate smoothly within dynamic environments (Agarwal & Wang, 2005), (Ahmad et al., 2012).

1.1. The Role of Secure ICT Platforms in Modern Communication

Secure ICT platforms play a vital role in various critical operations. These systems are designed to ensure that sensitive data is transmitted and processed securely, protecting it from interception or unauthorized access. This need becomes even more crucial in areas like drone communication, where operations are distributed and wireless transmission is inherently vulnerable. While platforms such as ITU-T X.805 and SmartNet have made significant contributions to secure ICT infrastructure, they often struggle to meet the modern demands for mobility, real-time responsiveness, and global scalability (Alkussayer & Allen, 2010), (Amir et al., 2004a). SecuDroneComm seeks to tackle these issues by merging the strengths of traditional systems with contemporary innovations (Amir et al., 2004b). It employs hybrid servers that combine the scalability of cloud-based solutions with the low-latency advantages of local servers. Furthermore, the implementation of logical coordinators, similar to SDN controllers, optimizes data flow and resource allocation throughout the system (Amir et al., 2020).

1.2. The Importance of Real-Time Communication for Drones

Drones depend on a constant flow of information to carry out their functions successfully. Whether it's gathering surveillance data or performing autonomous actions, each task relies on secure and reliable communication channels. In critical situations such as battlefield reconnaissance or disaster response, even a slight delay or disruption in communication can have dire consequences (Amin et al., 2003). Conventional ICT systems frequently fall short of the high-speed, low-latency demands of these applications, which is why solutions like SecuDroneComm are essential (Barrows & Powers, 2009), (Benzel et al., 2006).

1.3. Bridging the Gap: Comparing SecuDroneComm with Existing Platforms

Current ICT platforms have significantly advanced secure communication. For instance:

1. ITU-T X.805 offers a comprehensive security framework for ICT systems, but it is primarily designed for stationary environments, making it less effective for mobile and dynamic operations (Braga & Nascimento, 2012).
2. The SmartNet architecture, aimed at energy systems, demonstrates the capabilities of distributed ICT frameworks, yet it lacks the real-time responsiveness essential for UAV operations (Braga, 2013).
3. Federated identity systems in mobile and wireless communications improve user authentication and access control, but they often struggle with scalability and interoperability issues, especially in hybrid server environments (Chatisa et al., 2023), (Chockler et al., 2001).

By drawing insights from these systems, SecuDroneComm integrates advanced features like OAuth-based access control and TLS-encrypted connections, while also catering to the specific needs of drone communication.

Its hybrid design facilitates smooth operation across both local and cloud servers, ensuring uninterrupted data flow even in areas with limited connectivity (Diesburg & Wang, 2010), (Edgar et al., 2011).

1.4. Key Features of SecuDroneComm Platform

1. Hybrid Server Architecture: SecuDroneComm combines local and cloud servers, enabling it to meet various operational needs. Local servers ensure low-latency performance for real-time applications, while cloud servers provide scalability and redundancy for long-term data management (ELECTRA, 2013).
2. Advanced Security Protocols: At the core of SecuDroneComm is a strong focus on security. It utilizes AES-256 encryption to protect data, TLS 1.3 for secure transmission, and OAuth for reliable user authentication. These protocols work together to secure data throughout its entire lifecycle (Enck et al., 2011), (Fragkiadakis et al., 2013).

3. Logical Coordinator (SDN Controller): Drawing from software-defined networking (SDN) principles, the logical coordinator facilitates efficient data routing and server resource management. This feature is especially useful in hybrid environments, where data may need to be dynamically allocated between local and cloud servers (Hiltunen et al., 2001).
4. Real-Time Responsiveness: The platform is built to meet the high-speed demands of drone communication. Its optimized architecture reduces latency, ensuring that data is transmitted and processed promptly (Horsmanheimo et al., 2017).
5. Scalability: SecuDroneComm is capable of scaling from small tactical deployments to extensive, distributed networks. Its modular design allows for the addition of new nodes, servers, or drones without interrupting ongoing operations (Hussain et al., 2014), (Huawei Technologies Co., Ltd., 2023).

1.5. Applications and Use Cases

1. Military Operations: In defense situations, drones frequently operate in challenging environments where secure communication is essential. SecuDroneComm allows for real-time data sharing between UAVs and command centers, ensuring that reconnaissance and tactical decisions rely on accurate, up-to-date information (International Telecommunication Union, 2003), (ITU-R, 2015).
2. Disaster Management: In the event of natural disasters, drones are crucial for assessing damage and finding survivors. SecuDroneComm supports the secure transmission of this information to response teams, enabling timely and coordinated efforts (Keidar et al., 2000).
3. Public Health Monitoring: The platform can also be utilized for health surveillance, such as tracking air quality or identifying pathogens in urban settings. By connecting with cloud servers, it enables health agencies to analyze data on a large scale while ensuring local responsiveness (Pereira et al., 2013).
4. Industrial Applications: Whether inspecting pipelines or monitoring factory emissions, drones equipped with SecuDroneComm guarantee that sensitive industrial data remains secure from breaches or tampering (Reardon et al., 2012).

1.6. Challenges and Opportunities

Implementing SecuDroneComm brings its own challenges, especially when it comes to integrating its components in various environments. The need for advanced technology infrastructure, including hybrid servers and logical coordinators, demands careful planning and investment. Moreover, the platform must be adaptable to keep pace with changing security threats and technological progress. On the flip side, these challenges also open doors for growth. By leveraging emerging technologies like blockchain for data validation and AI for threat detection, SecuDroneComm can significantly boost its capabilities. Collaborating with existing ICT platforms and manufacturers could also speed up its adoption and improvement (Saxena & Chaudhari, 2012), (Schrittwieser et al., 2012).

2. Literature Review

This section examines the latest advancements in ICT platforms designed for secure communication, contrasting them with the proposed SecuDroneComm platform. It incorporates insights from the provided materials to create a thorough understanding of current systems and identifies areas for improvement (Siddiqi et al., 2006).

2.1. Overview of SecuDroneComm Platform

SecuDroneComm is a sophisticated hybrid ICT platform crafted for secure, real-time communication between drones and command centers. Its design combines local and cloud servers, enabling low- latency operations in restricted environments while also allowing for scalability in large-scale deployments. Notable features include AES-256 encryption for data protection, TLS 1.3 for secure data transport, and OAuth-based user authentication. The system includes a logical coordinator, akin to an SDN controller, which dynamically routes data and optimizes server resources (Wang et al., 2012), (Wischounig-Strucl & Rinner, 2015).

This platform is especially well-suited for high-stakes applications such as military operations, disaster response, and public health surveillance, where data security and real-time responsiveness are essential.

By utilizing a modular architecture and state-of-the-art technologies, SecuDroneComm provides flexibility and adaptability across a variety of operational scenarios (Yanmaz et al., 2017).

2.2. Overview of Other ICT Platforms

The following ICT platforms showcase different strategies for ensuring secure communication, each tailored to specific use cases and challenges:

1. ITU-T X.805 Framework: This comprehensive security framework, ITU-T X.805, emphasizes end-to-end protection for networked systems. It features a three-layer architecture (Infrastructure, Services, Applications) and eight security dimensions, offering a solid approach to securing data in distributed environments. However, its emphasis on traditional IP-based networks restricts its use in modern dynamic scenarios like UAV communication (Agarwal & Wang, 2005).
2. SmartNet Architecture: SmartNet is crafted for secure communication within energy systems, utilizing distributed ICT frameworks such as IoT and 5G. Its SGAM (Smart Grid Architecture Model) facilitates efficient data alignment and flow in smart grids. While it shines in flexibility and system integration, its focus on energy systems limits its relevance to UAV operations and real-time needs (Ahmad et al., 2012).
3. Trust-ME Federated Framework: This platform focuses on federated identity management, making user authentication easier across various systems. By utilizing Single Sign-On (SSO) and Intrusion Detection Systems (IDS), Trust-ME improves both security and user experience. However, its main focus is on identity and access management, rather than on real-time data transmission or hybrid architectures (Alkussayer & Allen, 2010).
4. Spread Secure Communication: Spread is a system created for secure group communication, using dynamic group key management protocols. It guarantees data confidentiality and integrity while ensuring scalability for collaborative settings. However, its effectiveness in UAV-based applications is limited due to the complexity of group configurations and the dependence on pre-established networks (Amir et al., 2004a).

Table 1: Overview of the SecuDroneComm and other proposed platforms

Platform	Core Focus	Key Features	Applications
SecuDroneComm	Real-time UAV communication	Hybrid server architecture, AES-256 encryption, TLS 1.3, SDN-like logical coordinator	Military, disaster response, public health monitoring
ITU-T X.805	End-to-end security	Layered architecture (Infrastructure, Services, Applications), Eight security dimensions	Traditional IP-based systems, networked environments
SmartNet	Energy system communication	Distributed ICT frameworks, SGAM model, integration with IoT and 5G	Smart grids, energy management
Trust-ME	Federated identity management	Single Sign-On (SSO), Intrusion Detection Systems (IDS), centralized policy control	Identity management, secure authentication
Spread	Group communication security	Dynamic group key management, scalable data integrity solutions	Collaborative environments, enterprise communication

Source: Authors‘ research

3. Comparison of SecuDroneComm with Proposed Platforms

The SecuDroneComm platform offers a distinctive method for ensuring secure communication among drones by utilizing advanced encryption protocols, a hybrid server architecture, and dynamic routing.

Although existing platforms like ITU-T X.805, SmartNet, Trust-ME, and Spread have made important strides in secure ICT communication, they each fall short in meeting the unique needs of real-time UAV operations. This section presents a comparative analysis, highlighting how SecuDroneComm differentiates itself and draws lessons from these other platforms (Agarwal & Wang, 2005), (Ahmad et al., 2012), (Alkussayer & Allen, 2010), (Amir et al., 2004a).

Table 2: Comparison of SecuDroneComm with Proposed Platforms

Platform	Primary Focus	Strengths	Limitations
SecuDroneComm	Secure real-time UAV communication	Hybrid server architecture, AES-256 encryption, TLS 1.3, SDN-like logical coordinator	Requires advanced infrastructure; initial setup complexity
ITU-T X.805	End-to-end network security	Comprehensive layered framework; adaptable to multiple network scales	Focused on traditional IP-based systems; limited support for mobile and hybrid environments
SmartNet	Distributed energy communication	IoT and 5G integration; highly flexible distributed architecture	Tailored for energy systems; lacks emphasis on UAV and real-time responsiveness
Trust-ME	Federated identity management	Single Sign-On (SSO); intrusion detection; seamless user access	Geared toward authentication and access management; less focus on data routing or scalability
Spread	Secure group communication	Dynamic group key management; scalability for collaborative networks	Complexity in managing group configurations; not optimized for hybrid server architectures

Source: Authors‘ research

4. Effectiveness Comparison of SecuDroneComm with Proposed Platforms

To assess the effectiveness of the SecuDroneComm platform, it's crucial to examine key performance indicators like latency, security, scalability, adaptability, and user accessibility (Agarwal & Wang, 2005), (Ahmad et al., 2012). This section will compare SecuDroneComm with other leading ICT platforms, such as ITU-T X.805, SmartNet, Trust-ME, and Spread, based on these metrics.

The goal of this comparison is to showcase SecuDroneComm's strengths, pinpoint areas where it outperforms existing systems, and explore potential opportunities for improvement (Alkussayer & Allen, 2010), (Amir et al., 2004a).

Table 3: Effectiveness Comparison of SecuDroneComm with Proposed Platforms

Metric	SecuDroneComm	ITU-T X.805	SmartNet	Trust-ME	Spread
Latency	Real-time with hybrid servers	Moderate	High in static environments	Moderate	Depends on group size
Security	AES-256, TLS 1.3, OAuth	Multi-layered framework	Blockchain-based encryption	Federated authentication	Group key management
Scalability	Highly scalable (hybrid model)	Limited to network scope	Flexible in distributed grids	Limited to authentication	Scalable in group settings
Adaptability	Dynamic routing with SDN-like logic	Rigid for IP-based systems	Focused on energy systems	Limited to access control	Limited to preconfigured groups
User Accessibility	Modular design for easy integration	Structured but static	Advanced IoT integration	SSO for seamless access	Complex group configurations

Source: Authors‘ research

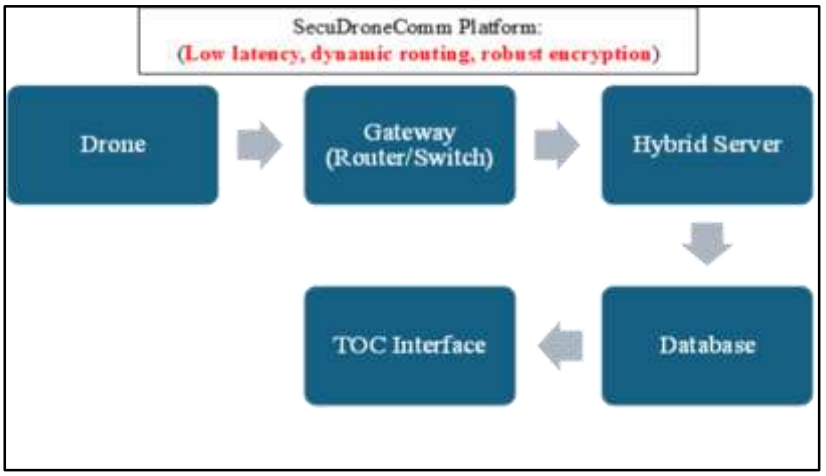
SecuDroneComm stands out from other platforms in several important areas related to UAV communication:

- Its hybrid architecture allows for real-time data processing with minimal latency (Agarwal & Wang, 2005).
- Cutting-edge security protocols offer strong data protection while maintaining scalability (Ahmad et al., 2012).
- The dynamic routing system enhances its adaptability to various and changing environments (Alkussayer & Allen, 2010), (Amir et al., 2004a).

By evaluating the strengths and weaknesses of competing platforms, SecuDroneComm integrates their best practices and addresses significant gaps, positioning itself as a leader in secure UAV communication.

The figures below present a comparative schematic that illustrates the workflows of these platforms (Agarwal & Wang, 2005), (Ahmad et al., 2012), (Alkussayer & Allen, 2010), (Amir et al., 2004a), (Amir et al., 2004b), (Amir et al., 2020), (Amin et al., 2003).

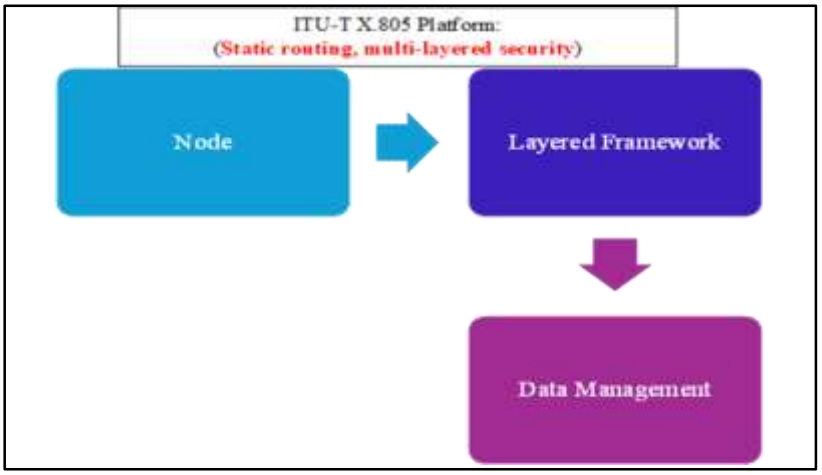
Figure 1: SecuDroneComm Platform Workflow



Source: Authors‘ research

Figure 1 provides an overview of the SecuDroneComm workflow, emphasizing its real-time data handling, robust security layers, and flexible integration capabilities. This schematic highlights how the platform coordinates between UAVs, edge servers, and end-users to ensure seamless and secure communication.

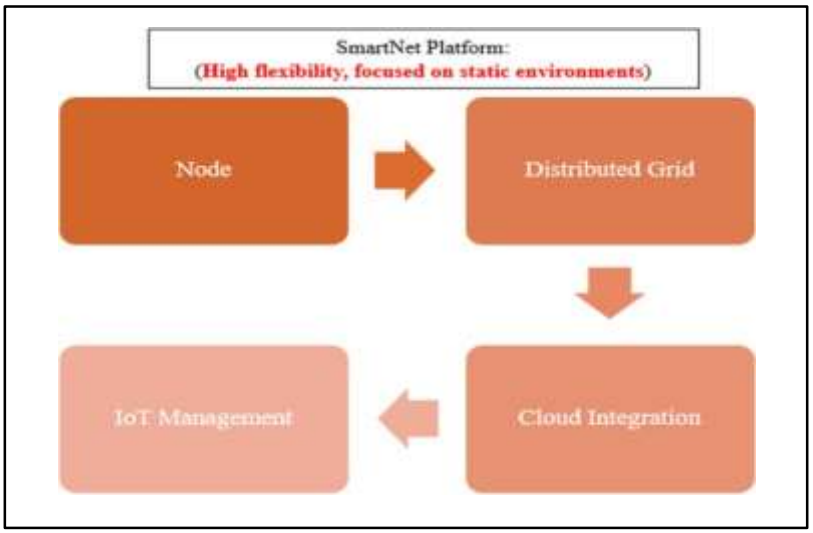
Figure 2: ITU-TX.805 Platform Workflow



Source: Authors‘ research

Figure 2 depicts the workflow of the ITU-T X.805 platform, which is characterized by its structured but relatively rigid architecture. The figure illustrates how the platform‘s multi-layered security framework is integrated within traditional IP-based systems, providing a reference point for legacy ICT solutions.

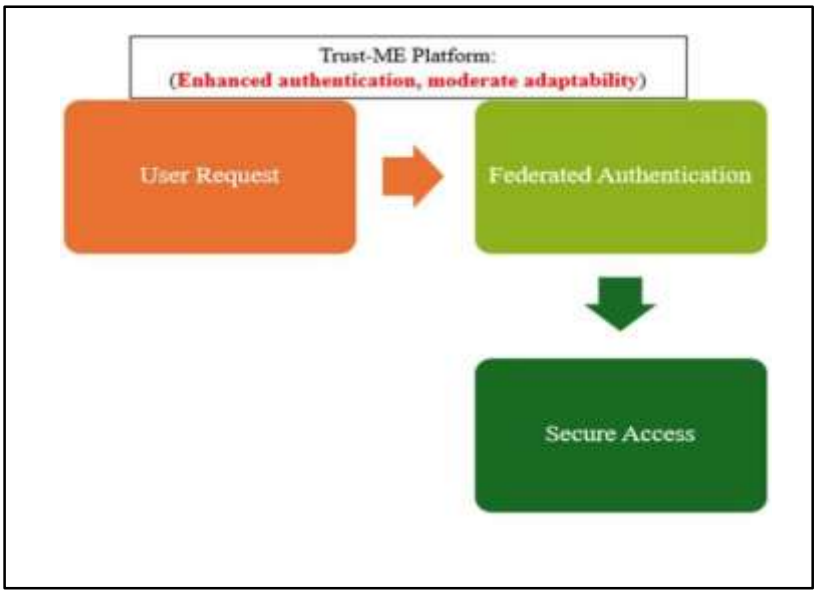
Figure 3: SmartNet Platform Workflow



Source: Authors‘ research

Figure 3 demonstrates the operational flow of the SmartNet platform. This solution focuses primarily on energy efficiency and secure communications within distributed grids. The figure underscores SmartNet's reliance on blockchain-based encryption and its advanced integration with IoT environments.

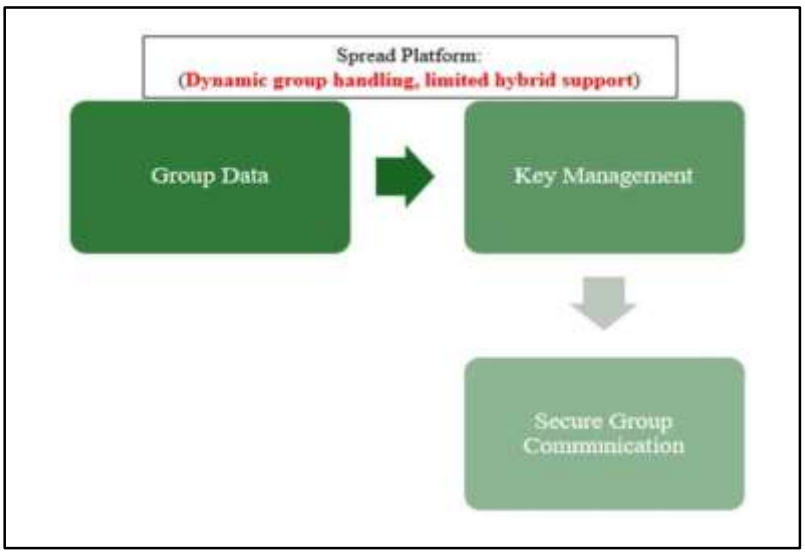
Figure 4: Trust-ME Platform Workflow



Source: Authors‘ research

Figure 4 illustrates the Trust-ME platform‘s workflow, which leverages federated authentication and single sign-on mechanisms for streamlined access control. The schematic details how Trust-ME manages user identities and access privileges, though its adaptability remains limited compared to newer solutions.

Figure 5: Spread Platform Workflow



Source: Authors‘ research

Figure 5 shows the Spread platform‘s workflow, with an emphasis on group communication and key management. The platform is particularly suitable for preconfigured group settings, though its adaptability is constrained by static group definitions.

4. Conclusion

The SecuDroneComm platform marks a major step forward in secure communication systems designed specifically for real-time UAV operations. It integrates a hybrid server architecture with strong encryption protocols such as AES-256 and TLS 1.3, along with a dynamic routing mechanism influenced by SDN principles. This combination effectively tackles key issues like latency, scalability, and adaptability.

Its modular design and ability to integrate with other systems make it a flexible solution for a range of applications, including military operations, disaster management, and public health surveillance. When compared to existing platforms like ITU-T X.805, SmartNet, Trust-ME, and Spread, SecuDroneComm offers better real-time responsiveness, improved security, and increased flexibility in changing environments. However, to implement it successfully, challenges such as infrastructure requirements, cybersecurity threats, and the necessity for user training must be addressed. By using phased deployment strategies, incorporating emerging technologies like AI and blockchain, and ensuring compatibility with legacy systems, SecuDroneComm can further boost its effectiveness.

As UAV operations and secure communication advance, SecuDroneComm is poised to establish a new benchmark in ICT platforms. Its cutting-edge approach addresses the shortcomings of traditional systems while also laying the groundwork for future innovations, guaranteeing safe and efficient communication in a world that is becoming more interconnected and complex.

Literature

1. Agarwal, A. K., & Wang, W. (2005). Measuring performance impact of security protocols in wireless local area networks. *Proceedings of the 2nd International Conference on Broadband Networks*, 1, 581-590.
2. Ahmad, M., Taj, S., Mustafa, T., & Asri, M. (2012). Performance analysis of wireless network with the impact of security mechanisms. *Proceedings of the International Conference on Emerging Technologies (ICET)*, 1-6.
3. Alkussayer, A., & Allen, W. H. (2010). A scenario-based framework for the security evaluation of software architecture. *3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT)*.
4. Amir, Y., Kim, Y., Nita-Rotaru, C., &Tsudik, G. (2004). On the performance of group key agreement protocols. *ACM Transactions on Information Systems Security*, 7(3).
5. Amir, Y., Kim, Y., Nita-Rotaru, C., Stanton, J., &Tsudik, G. (2004). Secure group communication using robust contributory key agreement. *IEEE Transactions on Parallel and Distributed Systems*, 15(5), 468-480.
6. Amir, Y., Nita-Rotaru, C., Stanton, J., &Tsudik, G. (2020). Secure spread: An integrated architecture for secure group communication. *Conference Paper*.
7. Amin, Y., Nita-Rotaru, C., Stanton, J., &Tsudik, G. (2003). Scaling secure group communication systems: Beyond peer-to-peer. *Proceedings of DISCEX3*, Washington, DC.
8. Barrows, C., & Powers, T. W. (2009). *Introduction to the hospitality industry* (7th ed.). Hoboken, NJ: John Wiley & Sons, Inc.
9. Benzel, T., et al. (2006). Experience with DETER: A testbed for security research. *2nd International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities*, Barcelona, 10 pp.-388.
10. Braga, A. M., & Nascimento, E. N. (2012). Portability evaluation of cryptographic libraries on Android smartphones. *4th International Conference on Cyberspace Safety and Security (CSS)*, 459-469.
11. Braga, A. M. (2013). Integrated technologies for communication security on mobile devices. *MOBILITY 2013: The Third International Conference on Mobile Services, Resources, and Users.*
12. Chatisa, I., Syahbana, Y. A., & Wibowo, A. U. A. (2023). A building security monitoring system based on the Internet of Things (IoT) with illumination-invariant face recognition for object detection. *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control Journal*, February.
13. Chockler, G. V., Keidar, I., &Vitenberg, R. (2001). Group communication specifications: A comprehensive study. *ACM Computing Surveys*, 33(4), 427-469.
14. Diesburg, S., & Wang, A. (2010). A survey of confidential data storage and deletion methods. *ACM Computing Surveys*, 43(1).
15. Edgar, T., Manz, D., & Carroll, T. (2011). Towards an experimental testbed facility for cyber-physical security research. *Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research*. ACM, Article 53.
16. ELECTRA. (2013). *Deliverable R4.1: Description of the methodology for the detailed functional specification of the ELECTRA solutions*.
17. Enck, W., Octeau, D., McDaniel, P., & Chaudhuri, S. (2011). A study of Android application security. *Proceedings of the 20th USENIX Conference on Security (SEC)*, 21-21.

18. Fragkiadakis, A., Alexandros, G., Tragos, E., & Ioannis, G. (2013). A survey on security threats and detection techniques in cognitive radio networks. *IEEE Communications Surveys & Tutorials*, 15(1), 428-445.
19. Hiltunen, M. A., Schlichting, R. D., & Ugarte, C. (2001). Enhancing survivability of security services using redundancy. *Proceedings of the International Conference on Dependable Systems and Networks*, June.
20. Horsmanheimo, S., Kokkoniemi-Tarkkanen, H., Kuusela, P., Tuomimäki, L., Andersen, C. A., Dall, J., ... Pardo, M. (2017). *ICT Architecture Design Specification*. European Union‘s Horizon 2020, April.
21. Hussain, A., Faber, T., Braden, R., Benzel, T., Yardley, T., Jones, J., ... Tinnel, L. (2014). Enabling collaborative research for security and resiliency of energy cyber-physical systems. *IEEE International Conference on Distributed Computing in Sensor Systems*, Washington, DC, USA.
22. Huawei Technologies Co., Ltd. (2023). *Data communication and network technologies*. Beijing, China: h Posts & Telecom Press.
23. International Telecommunication Union. (2003). *Security in telecommunications and information technology: An overview of issues and the deployment of existing ITU-T recommendations for secure telecommunications*. Geneva: ITU.
24. ITU-R. (2015). *Recommendation ITU-R M.2083-0: IMT vision - Framework and overall objectives of the future development of IMT for 2020 and beyond*. Geneva: ITU.
25. Keidar, I., Sussman, J., Marzullo, K., & Dolev, D. (2000). A client-server oriented algorithm for virtually synchronous group membership in WANs. *Proceedings of the 20th International Conference on Distributed Computing Systems (ICDCS 2000)*, 356.
26. Pereira, C., et al. (2013). SMSCrypto: A lightweight cryptographic framework for secure SMS transmission. *Journal of Systems and Software*, 86(3), 698-706.
27. Reardon, J., Marforio, C., Capkun, S., & Basin, D. (2012). User-level secure deletion on log-structured file systems. *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, 63-64.
28. Saxena, N., & Chaudhari, N. S. (2012). Secure encryption with digital signature approach for short message service. *Proceedings of the World Congress on Information and Communication Technologies (WICT)*, 803-806.
29. Schrittwieser, S., et al. (2012). Guess who's texting you? Evaluating the security of smartphone messaging applications. *Proceedings of the 19th Network & Distributed System Security Symposium*, February.
30. Siddiqi, J., Akhgar, B., Naderi, M., Orth, W., Meyer, N., Tuisku, M., ... Colin, J. (2006). Secure ICT services for mobile and wireless communications: A federated global identity management framework. *Conference Paper*, April.
31. Wang, Z., Murmuria, R., & Stavrou, A. (2012). Implementing and optimizing an encryption filesystem on Android. *Proceedings of the 13th International Conference on Mobile Data Management*, 52-62.
32. Wischounig-Strucl, D., & Rinner, B. (2015). Resource-aware and incremental mosaics of wide areas from small-scale UAVs. *Machine Vision and Applications*.
33. Yanmaz, E., Yahyanejad, S., Rinner, B., Hellwagner, H., &Bettstetter, C. (2017). Drone networks: Communications, coordination, and sensing. *Elsevier*.