Development of the “friend-or-foe” identification system on the basis of programmable radiomodems

Leonid Hulianytskyi, Maksym Ogurtsov and Vyacheslav Korolyov

V.M. Glushkov Institute of Cybernetics of the NAS of Ukraine, Akademika Hlushkova Ave, 40, Kyiv, 03187, Ukraine

Abstract

The issue of “friend-or-foe” (FoF) vehicles identification and recognition systems improvement in terms of speed and reliability of information processing is considered. Issues of new FoF algorithms and backup channels development for aircraft and unmanned aerial vehicles (UAV) identification based on modern cryptographic algorithms and programmable radiomodems are discussed.

The requirements for governmental civilian and military recognition systems based on cryptography and computer security methods are given. Recommendations for eliminating the shortcomings of the existing FoF recognition system are formulated. Increasing the reliability of the FoF identification system in the proposed work is based on the created series of backup data transmission channels, which should use different operating frequencies and different types of frequency processing of digital radio signals to increase the stability of the special communication system in the case of radio electronic warfare interference stations usage.

The developed friend-or-foe” identification system on the basis of radio modems, made with programmable gate matrices for creating interference-protected and encrypted communication channels have been tested on real software radio stations: Ettus B200 and HackRF One. The functionality of the presented visual models of radio modems and the rationality of their use for the on-board special-purpose devices creation have been confirmed by the results of full-scale experiments in laboratory conditions.

Keywords

Friend-or-foe, cryptography, software-controlled radio stations, radio modems, identification.

1. Introduction

The year 2022 showed the urgent need to improve the existing FoF systems for aerial object recognition and state identification, which is caused by the increase in the number of aerial objects (especially unmanned ones) on the battlefield. Thus, the creation of the drone army was announced in Ukraine [1]. This concept includes complex procurements of unmanned aerial vehicles (UAVs), repairs, and replacements. At the first stage of the program’s implementation, 200 tactical-level UAVs will be purchased for air reconnaissance. In the second stage, each unit of the Ukrainian Armed Forces will have its own reconnaissance UAV.

It should be considered that this will lead to multiple growths in the number of UAVs, that simultaneously can be present in controlled airspace. In addition to tactical reconnaissance UAVs of the Armed Forces sub-units, strategic reconnaissance piloted and unmanned aerial vehicles, unmanned kamikaze drones or barging ammunition also cruise and ballistic missiles can be detected in the air – and all this together with the classical planes and rotorcrafts [2]. And then this number should be at least doubled – to consider the corresponding number of enemy targets in the air [3, 4]. Russian and Belarusian sources and scientific publications should also be taken into account to get in mind their current successes and failures. And to make sure that our results may provide us with advantages over

International Scientific Symposium «Intelligent Solutions» IntSol-2023, September 27–28, 2023, Kyiv-Uzhhorod, Ukraine
EMAIL: LeonHul.icyb@gmail.com (A. 1); ogurtsov.maksym@incyb.kiev.ua (A. 2); korolev.academ@gmail.com (A. 3)
ORCID: 0000-0002-1379-4132 (A. 1); 0000-0002-6167-5111 (A. 2); 0000-0003-1143-5846 (A. 3)

them. Such a rapid increase in the number of aerial objects that simultaneously take part in combat operations in the air requires the substantial improvement of military FoF recognition systems, both qualitatively and quantitatively. This requires the development of appropriate algorithms for the FoF identification of a new generation. Such algorithms can be based on various methods of information security, in particular on symmetric and asymmetric cryptographic algorithms and other methods of cryptography [5, 6]. But it should be considered that asymmetric algorithms are working much slower than symmetric ones [7] (even in the case of using shorter keys, sufficient only for battlefield cryptography [8]). And since the situation in the airspace near the battlefield changes especially dynamically, the FoF identification must be done as quickly as possible – therefore the use of symmetric cryptographic algorithms has a significant advantage due to their higher speed [9].

It should also be considered that there are fundamental differences in the requirements for aerial objects' civil and military recognition systems. When defining them, we will use the definition "legitimate aerial object" – this is an aerial object that has the right to be in the surveyed air space, has a working responder (transponder) of the identification system and provides correct answers to requests from the identification center.

2. The main issues considered in this work

- The main requirements for friend-or-foe (FoF) recognition system as a system of processing, transmission, protection of information and identification of objects based on cryptography and information security methods [10, 11, 12].
- Identifying common and distinctive features for civilian and military recognition systems.
- Determination of the advantages and disadvantages of the existing FoF recognition system.
- Formulation of recommendations to reduce the limitations of the existing FoF recognition system [12].
- Development of testing complex, including hardware and software parts for the practical study of FoF algorithms with reserved channels.

The main aim of this paper is to formulate requirements for the aerial objects recognition systems (both for civil and military use), to determine advantages and disadvantages of FoF identification system, currently used in Ukraine and to formulate recommendations to eliminate found shortcomings, based on the modern FoF identification means with the practical tests of the proposed recommendations.

3. The main requirements to aerial objects civil recognition systems

Let's define the main requirements for the aerial objects recognition systems of civil applications (responders for the air traffic control system – airplane transponders) [13, 14]:

1. **Maximum compatibility**. The aerial objects recognition system must determine the ownership of each aerial object in the controlled airspace, including aircraft and rotorcraft of large and small airlines from around the world (including ones that belong to private owners).
2. **Support of a large number of aerial objects**. In connection with the constant number increase in aerial transport, aerial object recognition systems (especially when applied at large airports) must support the processing of a lot of aerial targets at the same time.
3. **Support of outdated recognition complexes**. The recognition system must support cases when a request is received by, for example, an airplane, containing an outdated state identification responder – to be able to correctly process the received response and determine the object's ownership.
4. **Support for alternative ways of recognition**. If automatic identification of an aerial object has failed, the system operator must be able to find out the ownership of the aerial object in an alternative way. This usually could be done by radio communication request.
5. **Alternative data entry methods support**. If the object's ownership was determined by an alternative way, the system operator should be able to input the received information into the system manually, so other operators do not need to use the same alternative ways of identification again.
6. **Low price**. Such a system’s price should be as low as possible so even a small airport would be able to purchase one.

4. The main requirements to aerial objects military recognition systems

Now let us consider FoF recognition systems for military applications. The basic principle of operation of any modern country-wide FoF identification system used in military applications is that an aerial object should process an incoming request according to some formula (which is a cryptographic secret and changes regularly, for example, every 24 hours). In contrast to civilian systems, the following basic requirements have been identified for them [13, 14, 15, 16]:

1. **The maximum speed of the recognition process**. Since the situation on the battlefield changes very quickly, and for air combat, this statement is even more relevant, any delay in the recognition process can lead to losses, including human losses. So, for example, for anti-aircraft missile systems, the time of the target's stay in the affected zone usually does not exceed a few tens of seconds or even just a few seconds.
2. **Protection against false positives**. For civilian applications, the cases of trying to make an aerial object identified as another are theoretically unlikely (and without terroristic or military involvement have not yet occurred) – because, in the case of such fraud detection, the aerial object owner will not be able to avoid responsibility and will lose a lot of money in fines and lawsuits. On the other hand, in military applications, the enemy is maximally interested in making its own aerial objects to be identified as friendly ones. The enemy usually is ready to spend a lot of time and resources for achieving this goal. And in the case of a false-positive result of aerial object identification can be aerial strikes and human victims. Therefore, protection against a such threat should be the highest priority of the FoF recognition system.
3. **Protection from imitation of the correct FoF requests and answers**. Since the entire information exchange process during the FoF identification is carried out through the radio air, it is quite possible that all data circulating between a legitimate aerial object, which provides a correct answer to the FoF request, and the land-based recognition center can be intercepted by the enemy. After that, the enemy can try to simply repeat the same responses to the requests from the recognition center or try to change them to mimic a legitimate aerial object. That is why the FoF identification system must be reliably protected against this type of attack.
4. **Support for a large number of aerial objects**. As already mentioned above, the military FoF identification system must support the simultaneous recognition of many aerial objects of different types to determine in time the belonging of planes, helicopters, rockets, UAVs, and their swarms.
5. **Protection against cases of legitimate air object loss**. This requirement says that we should be ready for a situation when a legitimate aerial object was broken or shot down over the enemy territory or fell into the enemy's hands some other way. If there is no protection against a such situation, this will lead to the compromising of the entire FoF identification system. As the result, it will cause full replacement of the FoF identification system on all legitimate air objects. This had already happened, for example, in the Soviet Union [14]. Thus, it is not the system itself that should be kept secret, but the information in it, and it should be possible to replace it easily.
6. **Secret part rotation**. To prevent the possibility of compromising the FoF identification system secret part, in military application, the rotation of the secret part must be permanent. Usually, the recommended value is to change the secret part every day [8]. This requirement overlaps with the previous requirement and complements it.
7. **Protection against the false-negative result to prevent friendly fire**. As was already mentioned above, the exchange of requests and answers with the aerial object takes place through the radio air. In the case of military operations, such exchange may often be additionally complicated (for example, because of electronic warfare (EW) means effect, both friendly and enemy ones). But the FoF identification system must work as reliably as possible to prevent non-recognition of the correct answer from a legitimate air object (for example, due to a correct answer non-received or partial arrival to the recognition center thanks to the effect of EW means). This problem is very relevant to prevent the application of, for example, anti-aircraft weapons against friendly targets (the so-called "friendly fire"). This problem may seem far-fetched – but, for example, during the "Desert Storm Operation" in 1991, US troops suffered 23% of losses from "friendly fire" [17].
8. **Protection against "man-in-the-middle" attacks**. Consider the following situation: a legitimate air object is flying above the territory controlled by the enemy. The recognition center is far from it, and there is no direct connection between them at the moment (for example, due to the effect

of EW means). Somewhere in the territory between the legitimate air object and the recognition center, there is the enemy's mobile ground complex, equipped with a radio communication system, and the enemy's aerial object. The recognition complex sends a recognition request to the enemy's aerial object. It relays the request to the mobile ground complex, which transmits it to the legitimate air object. As the result, the legitimate object gets a valid FoF request. So, it processes this request and sends a response, which is delivered to the requester – the enemy's mobile ground complex. Then enemy from this complex also is relaying the response he got to the enemy's aerial object. And enemy's aerial object also relays this response to the recognition center. As a result, the recognition center will consider the enemy's air object to be legitimate. Such attack is complicated to protect from, but this protection is essential.

9. **Flexible integration with the NATO block recognition system**. Since Ukraine is on course to Euro-Atlantic integration and is moving to NATO standards rapidly, in the future there will be a need to integrate the military objects recognition system with the corresponding system of NATO countries – to carry out international training and operations.

10. **Purely domestic production and support of the FoF identification system**. If for civil systems it is possible to purchase the system as a whole or its components abroad, then for the military FoF identification system such an approach is inadmissible due to the increased risks of information leakage to potential enemies.

11. **Protection against EW means**. This requirement is related to several others and determines that the FoF identification system must work and determine the ownership of objects even in the case of active use of radio-electronic warfare means.

12. **Support of several recognition modes.** Usually, when identifying military objects, support of such requests as "Where are you?" and "Who are you?" must be ensured. In addition, conventional and control recognition modes are often required (to detect enemy's aerial objects that use cloaking against recognition means) [2, 18, 19].

13. **Automatic blocking of the ground-to-air and air-to-air rockets launch** on objects, which confirms their legitimacy by the correct response to the FoF request.

14. **Support of modern alternative recognition technologies.** Such technologies as Battlefield Target Identification Device (BTID), Radio Based Combat Identification (RBCI) and Radio Frequency (RF) tags preferably should be supported by any modern FoF identification system [2, 18, 19]. They will be described in more detail later.

As you can see, the only common thing in the requirements for recognition systems of civil and military use is a large number of objects support.

5. Determination of advantages and disadvantages of the current Ukrainian FoF identification system

To date, the "Parol-M" hardware and software complex is used for the cryptographic protection of information in the Ukrainian FoF identification system. "Parol-M" is a modification of the Soviet Union system developed in the 80s of the last century. It was developed as a replacement for the long-outdated Kremniy-2 (2M) complex [13, 14], which supported only 10 requesters and 10 respondents at the same time. The technical capabilities of the "Parol-M" complex support the simultaneous recognition of up to 110 requesters and 110 responders at once [13, 14]. At the same time, a similar system in the NATO countries – MarkXII – performs 400 requests per second in the nominal mode [16].

5.1. Advantages of the FoF identification system, currently used in Ukraine:

1. Presence of an anti-imitation recognition mode.
2. Pretty easy algorithms can work even on outdated hardware.
3. Availability of guaranteed recognition mode.
4. The ability to perform the recognition procedure even under the application of high-intensity interference.

5. Availability of individual codes for recognition based on the "Who are you?" principle.
6. Protection against receiving responses on the side lobes of the directional diagram.
7. High-frequency range usage.
8. Different request and response frequencies [13, 14].

After responding to every request from the requester, the respondent's transmitter is turned off for a certain time defined in the system parameters using a closing device [13]. This prevents responding to radio signals that are reflected from nearby local objects or signals, received on the side lobes of the directional diagram. However, with a very high frequency of requests, the situation can reach a level at which the normal operation of the system is disrupted. To prevent this, an automatic limitation of the maximum number of responses is used. For this purpose, decoded request signals are integrated, and the voltage of the received signal is used to regulate the speed of the response generation. Limiting the frequency of responses also prevents thermal overload of the responder's hardware due to a large number of requests [13]. High-precision radars and means of destroying aerial objects, in addition to radio-technical methods of increasing object recognition accuracy [13, 18, 19], should also provide:

1. Reducing the number of objects in the radar beam.
2. Narrowing of the radar beam pattern.
3. Preventing reflected signals acquisition at the side lobes of multi-channel receivers.
4. Coherent reception and transmission of recognition signals.

It is also possible to additionally apply military object recognition technology [2], using it to recognize the enemy's equipment and personnel to classify them as FoF (based on image recognition).

5.2. Disadvantages of the FoF identification system, currently used in Ukraine

The use of UAV swarms in armed conflicts in the Middle East or mixed attacking waves of ballistic, cruise rockets combined with loitering munition drones and conventional military aviation assaults in Ukraine, Armenia-Azerbaizhan high-intensity conflict [4] with the simultaneous use of manned, UAVs and different missiles shows that the recognition of 110 objects in the responsibility of a military FoF identification system is insufficient today. This problem can be solved by developing new FoF identification systems, which will meet modern requirements. Thus, the limitations of the FoF identification system ("Parol-M" hardware and software complex) currently used in Ukraine are:

1. Support of the insufficient recognition object amount.
2. Insufficient radio-electronic protection of the recognition process.
3. Insufficient imitation resistance – the probability of the enemy imitating the correct response to a recognition request is as much as 0.5% [13]. That meant, that in the case of sending a swarm of 200 enemy UAVs, one of them will be able to imitate the response of the legitimate aerial object without knowing any secret parameters.
4. Lack of interaction with any types of ground-based weapons (armored ground vehicles, manual anti-aircraft defense, etc.) to prevent friendly fire.
5. Absence of the integration possibility with the NATO FoF identification system.
6. Inability to update the algorithm used in the “Parol-M” complex due to its technical limitations and characteristics.
7. The insufficient number of individual identification codes for "Who are you?" requests, that could be send to the aerial targets.
8. High probability of recognition signals detection and interception.
9. The system work principles are known to the enemy (specialists from the Russian Federation) in every detail.

6. Modern FoF identification means

In NATO countries, a large amount of work has been focused on aerial and ground object recognition on the battlefield [2, 18, 19]. Among the areas of development of the so-called Battlefield Combat Identification System (BCIS), the following should be highlighted:

Identification based on means of automatic radio data transmission of all troops (Radio Based Combat Identification - RBCI).
Identification using radio tags (Radio Frequency Identification tags – RF tags).
Recognition of targets on the battlefield (application of Battlefield Target Identification Device – BTID).

RBCI, also called Battlefield Force Tracking System (BFTS) or Blu-Force Tracking (BFT) System, is built based on network-centric principles. Every friendly object equipped with this system transmits data (including the object's location) every 5 minutes, using satellite communication or a very high-frequency radio communication network. In active mode, the requester sends a general request with coordinates - and the responder compares the received coordinates with its own, and if they match - sends a response. All data in wireless communication channels are encrypted.

The advantage of this approach is the ability to recognize objects outside the direct line of sight. Disadvantages are the need to use a complex system of repeaters on the battlefield, the rapid aging of data (especially for fast-moving objects), the high impact of EW means, and the high cost of the system.

Recognition with the help of **radio tags** (RF tags) is also based on the "request-response" principle, just as for civilian tags, used, for example, in warehouses. The response in this system is formed by modulating the incoming request. There are active (similar to BTID), semi-active (have their power source) and passive (powered by the energy of requests from the requester's radio device) tags are used. The detection range of active or semi-active tags can reach 40 km [2, 18]. Radio tags are currently the only potentially applicable identification method for determining the affiliation of individual servicemen or their small units on the battlefield. And due to their small size and power requirements, they are potentially applicable to UAVs as well.

BTID systems are designed to recognize aerial objects in the "friend-unknown" format. Its essence is no different from the general FFI (Friend or Foe Identification) principle, used in the NATO Mk XII system. The term "friend-unknown" was introduced into military practice with the idea that a recognition object that has not responded to a request is not necessarily an enemy object [2, 19]. BTID systems also work on the "request-response" principle, the signals are encrypted and, to reduce the probability of interception, are broadband.

Let us present the results in the form of a recommendations list.

7. Recommendations for eliminating shortcomings of the FoF identification system

Recommendations for eliminating shortcomings of the FoF identification system and increasing its level of reliability:

1. Replacement of the current state identification system, which is currently used in Ukraine, by a more modern one, which will support modern cryptographic algorithms and a larger number of recognition objects.
2. Support of various directions recognition lines, including "Ground – UAV", "Aircraft – Tank", "Aircraft – UAV" and others.
3. Adding support for the NATO standard - STANAG 4579, which was applied in 2001, and others.
4. Adding recognition support using radio tags (RF tags).
5. Adding support of RBCI.
6. The use of wide-spectrum signals to reduce the probability of their detection and interception (which is especially important during the war), as well as signal-code structures and a used frequency grid.

8. Creation of the FoF identification system mock-up

The practice of massive combats including enemy aircrafts, UAVs, and missiles that Ukraine gained in the year 2022 showed that many enemy aircrafts were shot down by manual launchers that do not involve the use of the FoF identification system. Since the enemy, just as Ukraine, mostly uses Soviet-

era aircrafts or their modernized variants with very similar silhouettes, and characteristics, own aircrafts are often attacked. Therefore, it is proposed to use some backup channels for the FoF identification system and to create a small-sized device that can be installed on portable missile systems for target identification.

Two pairs of Ettus B200 and HackRF One software-controlled radio stations were used as a laboratory model for building the FoF identification system mock-up. They performed the functions of the main and backup data transmission channels. As a result of completed works, the main channel [11, 13] can use broadband signals in the ultra-high frequency range in which radars of anti-aircraft missile systems are working.

The reserved channel of the FoF identification system is working in the ultra-short frequency range. It can be used by developers of portable anti-aircraft missile systems. In addition to different operating frequencies, the main and reserve channels used different types of coding: orthogonal frequency division multiplexing and quadrature amplitude manipulation. Both channels use the same type of data packet encryption. Figure 1 shows fragments of laboratory stands for demonstrating the operation of the FoF identification system mock-up with backup channels. The stand consists of two HackRF One software-controlled radio stations, two Ettus B200 software-controlled radio stations, and two laptops with the GNURadio simulation environment version 3.7.10.

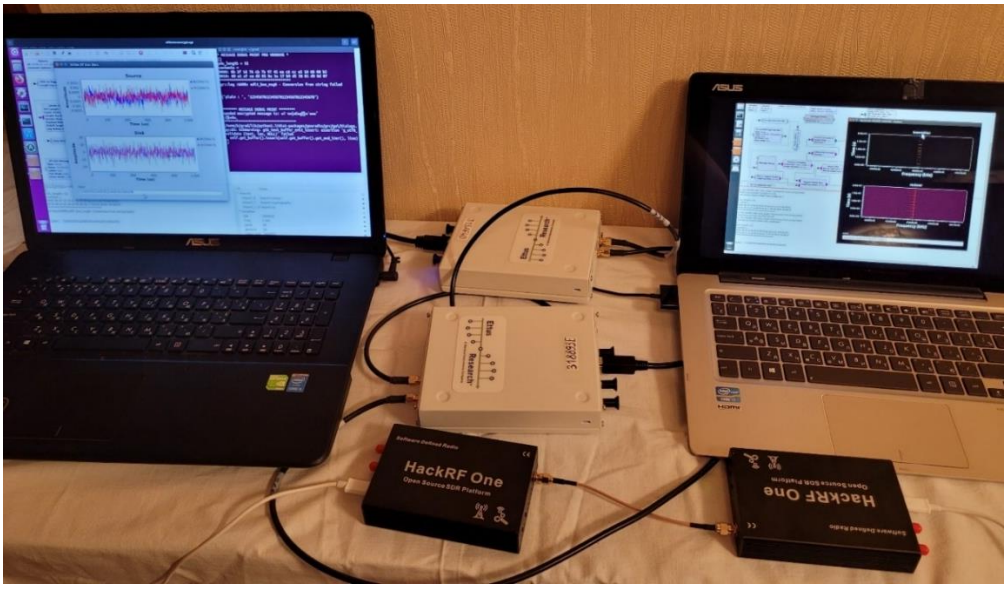

Figure 1: Laboratory set for researching the operation of the state identification system with backup channels

To develop software for radio modems one can use:

- program complex GNURadio;
- Simulink MatLab complex;
- LabView complex;
- libraries from the software-created radio stations manufacturer;
- libraries from independent developers;
- software for creating systems on programmable controllers from Altera (Intel) or Xilinx (AMD).

All the listed development tools were used at various stages of the FoF identification system mock-up development, but since the GNURadio complex had shown the best results in stability, functionality, and productivity areas, the results of research and development are laid out based on this development tool.

Figure 2 shows the frequency-time (WaterFall) diagram of the transmission and reception of encrypted request signals by software-controlled HackRF One radio stations. The request that was used in this example was "12345678123456781234567812345678".

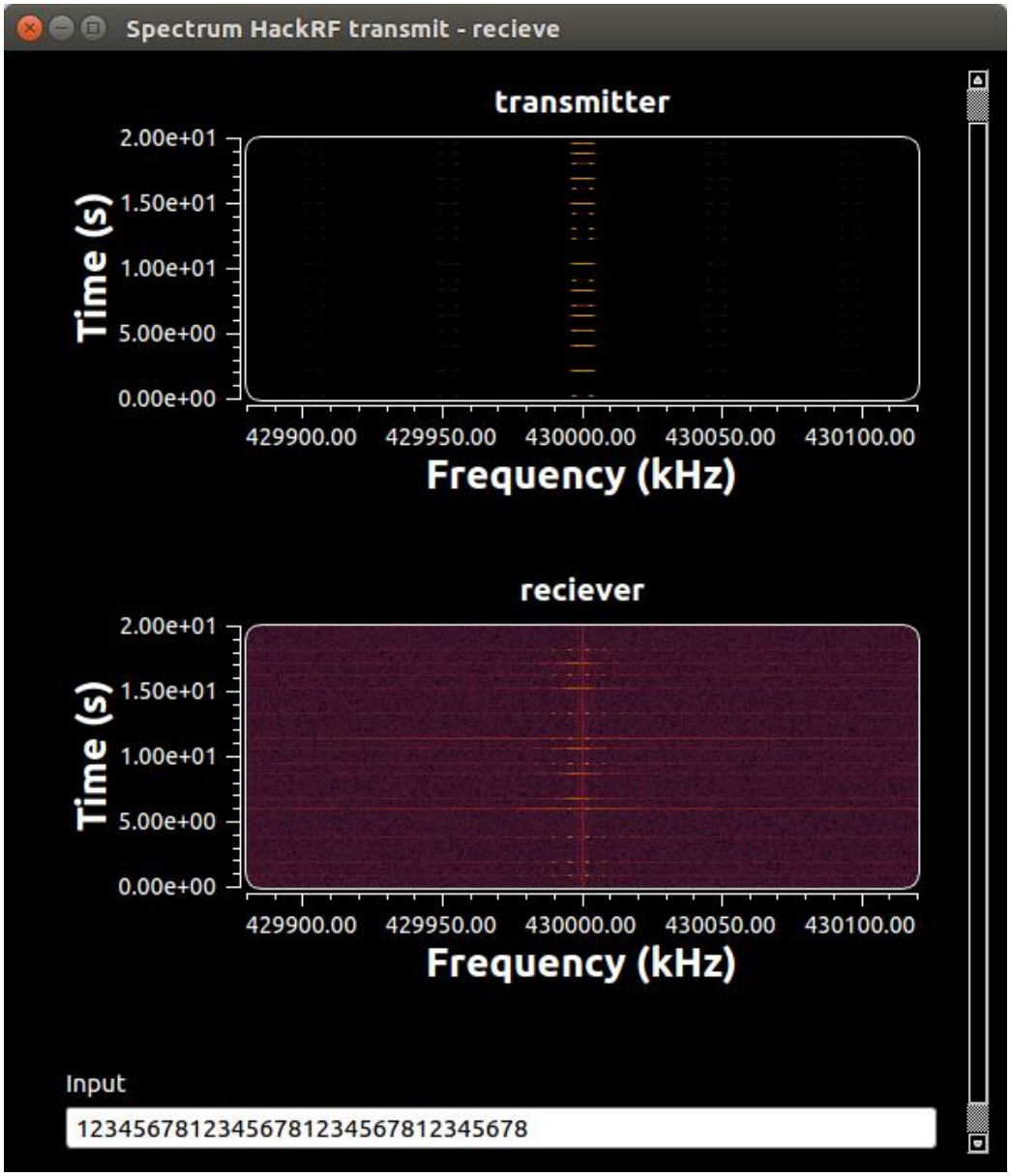

Figure 2. Time-frequency diagram of transmission and reception signals of the encrypted request term

Research and experiments with the HackRF One software-controlled radios have shown that without the use of precessional frequency reference generators and filters, only half of the data packets were decoded by the system. The operating frequency was 433 MHz. Unlike the Ettus B200 professional software-controlled radio, which successfully received and decoded approximately 99% of packets. The operating frequency was 2.5 GHz. Therefore, it may be said that HackRF One software-controlled radios cannot be used for building the FoF identification system – in real conditions outside of the laboratory the results would be even worse.

The advantage of the Ettus B200 radio stations is the complete openness of their electronic circuits and the availability of freely available diagrams of the placement of the components and their connections on the board, which allows using them as a primary prototype for the design of higher-quality digital radio stations.

The experiments performed with the use of Ettus B200 radio stations showed the stable operation of the system in laboratory conditions for 32-byte data packets, encrypted by Advanced Encrypted Standard – AES-256, which is the basis for further research and development works [12].

In free access publications similar solutions with backup channels, based on programmable radio-modems, used for state identification or FoF identification, aren't present.

9. Conclusions

The enemy's use of similar airplanes and helicopters makes it difficult to visually determine their state affiliation according to the FoF principle and may potentially lead to "friendly fire". The use of multiple various types of air defense equipment transferred by allies poses the problem of further integration of such equipment into the Ukrainian air defense system, which requires the development of appropriate FoF identification system devices. Such devices can use different types of frequency ranges and signal-code structures, and their development will be based on different requirements for weight, size characteristics, and power of the FoF identification system signal transmitter. The use of many different types of systems and requirements for the integration of “friend-or-foe” identification systems with the corresponding NATO systems will raise questions about the reliability of the system as a whole.

Increasing the reliability of FoF identification systems and communication systems proposed in this work is based on the creation of various backup data transmission channels. Such backup channels should use different operating frequencies and different types of frequency manipulation of digital radio signals to increase the resistance of the special communication system to jamming by electronic warfare stations. The productivity of target identification can be increased by using distributed processing in command points connected with a special network [10, 11, 12, 21]. To complete these taks authors used programmable radio stations and built FoF identification system laboratory set with backup channels on their basis. Practical tests had proven its applicability for the mentioned purpose.

Considering the limited financial resources of Ukraine, it is possible to suggest using more expensive radio stations for the FoF identification system on the main frequencies only – and cheaper radio stations for the FoF identification system on reserve frequencies.

The proposed results can also be used for the construction of secure communication systems, remote control of unmanned aerial vehicles, and unmanned ground robots. The results can be transferred to programmable logic integrated circuits and used in military tasks if this microcircuit and the product’s technology meet the armed forces' relevant branch's standards of operation.

10.References

[1] K. Chávez, O. Swed, Emulating underdogs: Tactical drones in the Russia-Ukraine war, Contemporary Security Policy, 2023, P. 1-14. doi: 10.1080/13523260.2023.2257964

[2] L. Bowden, The story of IFF (identification friend or foe), IEE Proceedings A (Physical Science, Measurement and Instrumentation, Management and Education, Reviews), 1 Oct. 1985, 132(6):435-7, 1985. doi: 10.1049/ip-a-1.1985.0079

[3] C. E. Lee, J. Baek, J. Son, Y. G. Ha, Deep AI military staff: Cooperative battlefield situation awareness for commander’s decision making, The Journal of Supercomputing, 79(6), 2023, P. 6040-6069. doi: 10.1007/s11227-022-04882-w

[4] Q. Hao, W. Z. Li, Z. K. Qiu, J. L. Zhang, Research on anti UAV swarm system in prevention of the important place, in: Journal of Physics: Conference Series 2020 Apr 1, Vol. 1507, No. 5, IOP Publishing, 2020, P. 052020. doi: 10.1088/1742-6596/1507/5/052020

[5] D. Rudinskas, Z. Goraj, J. Stankūnas, Security Analysis of UAV Radio Communication System, Aviation 13. 4. 2009. P. 116-121. doi:10.3846/1648-7788

[6] C.L. Chen, Y.Y. Deng, W. Weng, C.H. Chen, Y.J. Chiu, C.M. Wu, A traceable and privacy-preserving authentication for UAV communication control system. Electronics, 9(1). 2020. p.62. doi: 10.3390/electronics9010062

[7] M. A. Alia, A. A. Tamimi, O. N. Al-Allaf, Cryptography-based authentication methods, Proceedings of the World Congress on Engineering and Computer Science, 3 Jan. 2014. URL: http://www.iaeng.org/publication/WCECS2014/WCECS2014_pp199-204.pdf

[8] B.J. Matt Lightweight and Survivable Key Management for Army Battlefield Networks, Internal Publication, Network Associates Laboratories, 2003. URL: http://projects.mindtel.com/2005/SDSU.Geol600.Sensor_Networks/sensornets.refs/2003.%20ASC.%20Army%20Studies%20Conference/OA05%20LIGHTWEIGHT%20AND%20SURVIVAB

LE%20KEY%20MANAGEMENT%20FOR%20ARMY%20BATTLEFIELD%20NETWORKS.pdf.
[9] R. Gupta, A. Kumari, S. Tanwar, N. Kumar, Blockchain-Envisioned Soft-warized Multi-Swarming UAVs to Tackle COVID-I9 Situations", IEEE Network, 35 (2), 2021P. 160-167. doi: 10.1109/MNET.011.2000439
[10] V.Yu. Korolyov, M.I. Ogurtsov, O.M. Khodzinskyi, Multilevel Friend Or Foe Identification of Objects and Analysis of the Applicability of Post-Quantum Cryptographic Algorithms for Information Security, Cybernetics and Computer Technologies. 3. 2020. P. 74–84. (in Ukrainian) doi:10.34229/2707-451X.20.3.7
[11] M. Ogurtsov, V. Korolyov, O. Khodzinskyi, To the Problems of the National State Recognition System Improving. Cybernetics and Computer Technologies. 2022. 2. P. 74–82. (in Ukrainian) doi: 10.34229/2707-451X.22.2.8
[12] V.Yu. Korolyov, M.I. Ogurtsov, A.I. Kochubinsky, Identification of technical objects in the special networks according to the principle of "Friend or Foe". Control Systems and Computers. 2021. 4. P. 3-12. (in Ukrainian) doi:10.15407/csc.2021.04.003
[13] C. Yang, J. Mott, D. M. Bullock, Leveraging aircraft transponder signals for measuring aircraft fleet mix at non-towered airports. International Journal of Aviation, Aeronautics, and Aerospace. 2021. 8(2), 1. doi: 10.15394/ijaaa.2021.1563
[14] Iryna V. Svyd, Andrii I. Obod, Ganna E. Zavolodko, Iryna M. Melnychuk, Waldemar Wójcik, Sandugash Orazalieva, Gulzat Ziyatbekova. Assessment of information support quality by "friend or foe" identification systems. // PRZEGLĄD ELEKTROTECHNICZNY, ISSN 0033-2097, R. 95 NR 4/2019. – Warszawa, SIGMA-NOT Sp. z o.o.: 2019. – P. 127-131. DOI: 10.15199/48.2019.04.2.
[15] DSTU 4550: 2006. System of state recognition of objects. Radar recognition. Terms and definitions. [Effective from 2007-08-01]. Kind. of its. Derzhspozhyvstandart Ukraine, Kyiv, 2007, P. 21. (in Ukrainian).
[16] STANAG 4193. Technical Characteristics of The IFF Mk XIIA System, NATO, 2016. p. 45.
[17] D.L. Waterman, Fratricide: Incorporating DESERT STORM Lessons Learned, 2022. URL: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.828.2521&rep=rep1&type=pdf.
[18] P. Rohan, A. Gangopadhyay, A.R. Erbacher, C. Busartet, Camouflaged object detection system at the edge, Automatic Target Recognition XXXII - Vol. 12096, SPIE, 2022. doi: 10.1117/12.2618869.
[19] P. Nolan, S. Hamilton, IFF using Beamforming in Telemetry Beacons, in: 2021 IEEE Western New York Image and Signal Processing Workshop (WNYISPW), 2021, P. 1–5. doi: 10.1109/WNYISPW53194.2021.9661287.
[20] Y. Ahmadi, K. Mohamedpour, M. Ahmadi, Deinterleaving of interfering radars signals in identification friend or foe systems, in: Proc. of 18th Telecommunications forum TELFOR 2010 Nov 23, Telecommunications Society-Belgrade, ETF School of EE, University in Belgrade, IEEE Serbia & Montenegro COM CHAPTER, 2010, P. 729-733.
[21] N. Munir, L. E. Ismaila and S. A. Adeshina, "Decentralized Wireless Communication Using WI-FI in Battlefield Combat Identification System Optimization," 2018 14th International Conference on Electronics Computer and Computation (ICECCO), 2018, P. 1-6, doi: 10.1109/ICECCO.2018.8634802.