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

The main aim

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 Friend-or-Foe (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.

The main requirements to aerial objects civil recognition systems

- 1. Maximum compatibility.
- 2. Support of a large number of aerial objects.
- 3. Support of outdated recognition complexes.
- 4. Support for alternative ways of recognition.
- 5. Alternative data entry methods support.
- 6. Low price

The main requirements to aerial objects military recognition systems

- 1. The maximum speed of the recognition process
- 2. Protection against false positives.
- 3. Protection from imitation of the correct FoF requests and answers
- 4. Support for a large number of aerial objects.
- 5. Protection against cases of legitimate air object loss.
- 6. Secret part rotation.
- 7. Protection against the false-negative result to prevent friendly fire.
- 8. Protection against “man-in-the-middle” attacks.

The main requirements to aerial objects military recognition systems

- 9. Flexible integration with the NATO block recognition system.
- 10. Purely domestic production and support of the FoF identification system.
- 11. Protection against EW means.
- 12. Support of several recognition modes.
- 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.

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 Pretty easy algorithms can work even on outdated hardware.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.

Disadvantages of the FoF identification system, currently used in Ukraine

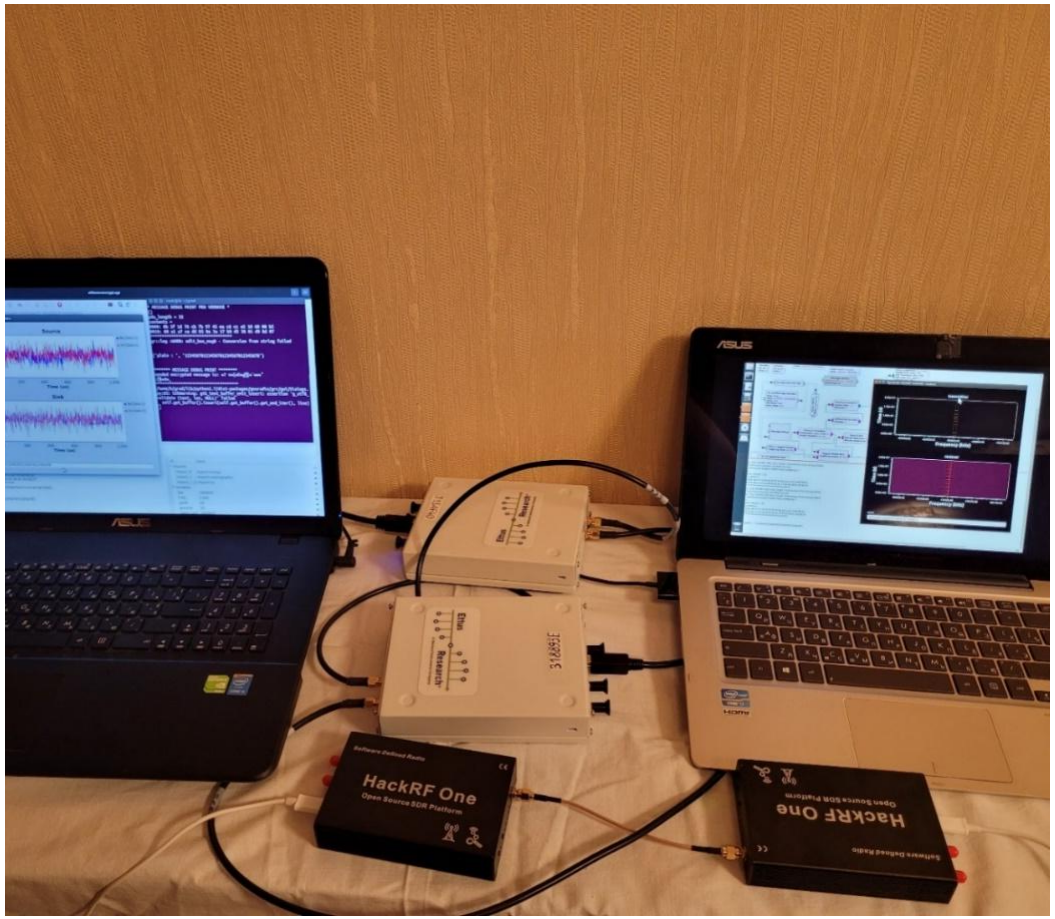
- 1. Support of the insufficient recognition object amount (110).
- 2. Insufficient radio-electronic protection of the recognition process.
- 3. Insufficient imitation resistance – the probability of the enemy imitating the correct response to a recognition request is as much as 0.5%.
- 4. Lack of interaction with any types of ground-based weapons 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.
- 7. The insufficient number of individual identification codes for "Who are you?" requests.
- 8. High probability of recognition signals detection and interception.
- 9. The system work principles are known to the enemy in every detail.

Recommendations for eliminating shortcomings of the FoF identification system

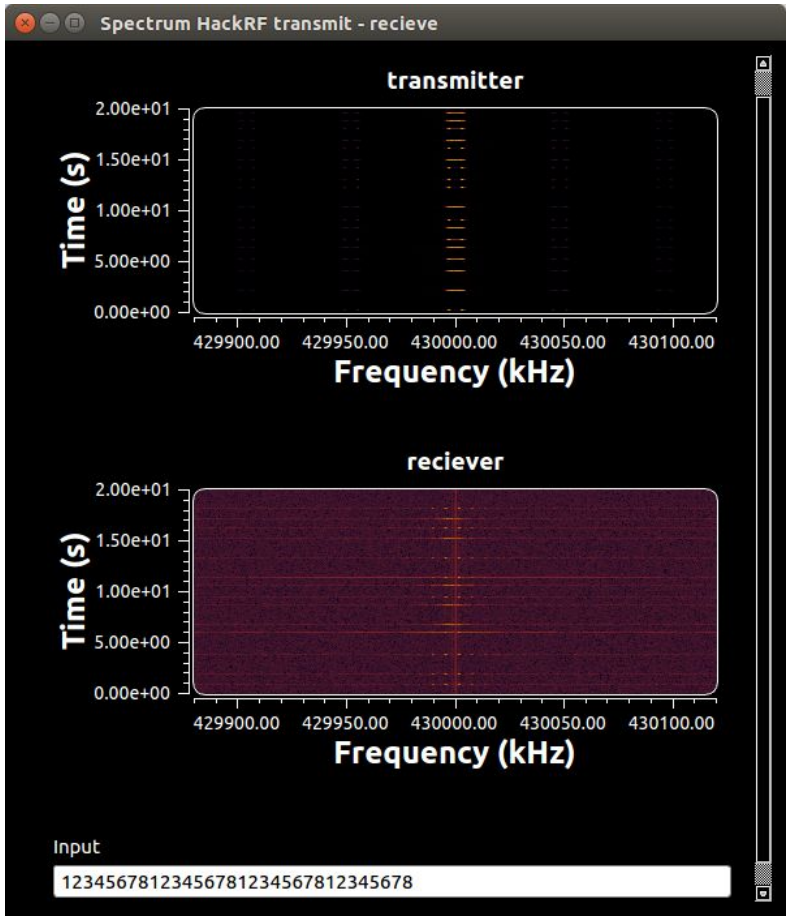
- 1. Replacement of the current state identification system by a more modern one, which will support modern cryptographic algorithms and a larger number of recognition objects.
- 2. Support of various directions recognition lines, including "Ground – UAV", "Aircraft – Tank", "Aircraft – UAV" and others.
- 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 Radio Based Combat Identification.
- 6. The use of wide-spectrum signals to reduce the probability of their detection and interception, as well as signal-code structures and a used frequency grid.

Development of improved FoF identification system mock-up with backup channels

- 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 can use broadband signals in the ultra-high frequency range 2.5 GHz 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 433 MHz. 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.



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



Frequency-time (WaterFall) diagram of the transmission and reception of encrypted request signals by software-controlled HackRF One radio stations

Laboratory experiments results

- Ettus B200 professional software-controlled radio successfully received and decoded approximately 99% of packets. 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.
- The experiments had proven that HackRF One software-controlled radios cannot be used for building the FoF identification system – even in the laboratory conditions they were able to decode less than half of the data packets.

Conclusions

- 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.
- 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.
- 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.

Thank you for your attention!