UDC 004.78 http://doi.org/10.15407/pp2022.03-04.387

# FRIEND-OR-FOE RECOGNITION ALGORITHM DEVELOPMENT FOR THE CORRESPONDING SOFTWARE BUILDING

*Maksym Ogurtsov*

2022 рік показав нагальну необхідність вдосконалення існуючих систем впізнавання об’єктів типу «свій-чужий», що викликана зростанням кількості технічних засобів (особливо – безпілотних) на полі бою. Таке різке зростання кількості об’єктів, що водночас приймають участь в бойових діях у повітрі, потребує вдосконалення систем впізнавання військових об’єктів як за якісними, так і за кількісними показниками. Це вимагає розробки відповідних алгоритмів ідентифікації об’єктів типу «свій-чужий» нового покоління.

Виділено основні вимоги до систем впізнавання повітряних об’єктів цивільного застосування. Вони включають: максимальну сумісність; підтримку великої кількості об’єктів; підтримку застарілих комплексів впізнавання; підтримка альтернативних шляхів впізнавання; підтримку альтернативних методів введення даних та визначення координат повітряних об’єктів в аварійній ситуації.

Також розглянуто системи впізнавання типу «свій-чужий» для військових застосувань. На відміну від цивільних систем, для них виділено такі основні вимоги:

1) Максимально висока швидкодія процесу впізнавання.
2) Захищеність від помилково-позитивних спрацювань.
3) Захищеність від імітації роботи відповідача легітимного повітряного об’єкту.
4) Підтримка великої кількості об’єктів.
5) Захищеність від випадків втрати легітимного повітряного об’єкту.
6) Ротація секретної частини.
7) Захищеність від помилково-негативного спрацювання для запобігання дружньому вогню.
8) Захищеність від атак типу «man in the middle».
9) Гнучка можливість інтеграції з системою впізнавання блоку НАТО.
10) Наявність можливостей суто вітчизняного виробництва та супровіду системи впізнавання об’єктів.
11) Захищеність від засобів РЕБ.
12) Підтримка декількох режимів впізнавання.
13) Автоматичне блокування пуску засобів ураження типу «земля-повітря» та «повітря-повітря» по об’єктам, що підтверджують свою легітимність правильною відповіддю на запит.
14) Визначення координат повітряних об’єктів в аварійній ситуації.

На основі сформульованих вимог запропоновано новий алгоритм захисту інформації для системи державного впізнавання для військових об’єктів, побудований на основі державних стандартів та з урахуванням особливостей його програмної реалізації з метою підвищення швидкодії, що забезпечуватиме достатню масштабованість, стійкість, надійність та багаторівневість впізнавання.

Ключові слова: державне впізнавання, свій-чужий, криптографія, криптоаналіз, БПЛА.

The year 2022 showed an urgent need to improve the existing systems for recognizing objects in the aerial space, which is caused by the significant increase in the number of technical means (especially unmanned aerial vehicles) on the battlefield. Such a sharp increase in the number of objects that simultaneously take part in combat operations in the air requires the improvement of military object recognition systems, both qualitatively and quantitatively. This requires the development of appropriate new generation Friend-or-Foe algorithms for the objects’ recognition.

The main requirements for recognition systems of aerial objects of civil application were determined. They includes: maximum compatibility; support for a large number of objects; outdated recognition complexes support; support for alternative ways of recognition; support for alternative data entry methods; determining the coordinates of aerial objects in an emergency situation.

Friend-or-foe recognition systems for military applications are also considered. In contrast to civilian systems, the following basic requirements have been identified for them:

1) Maximum speed of the recognition process.
2) Protection against false positives.
3) Protection against legitimate aerial object imitation.
4) Support for a large number of objects.
5) Protection against cases of loss of a legitimate aerial object.
6) Rotation of the secret part.
7) Protection against false-negative results to prevent friendly fire.
8) Protection against man-in-the-middle attacks.
9) Flexible integration with the NATO block recognition system.
10) Availability of opportunities for purely domestic production and support of the object recognition system.
11) Protection against electronic warfare means.
12) Support for several recognition modes.
13) Automatic blocking of the launch of ground-to-air and air-to-air weapons against objects that confirm their legitimacy by a correct response to a request.
14) Determining the coordinates of aerial objects in an emergency.

Based on the formulated requirements, a new friend-or-foe algorithm for the state identification system for military use is proposed, built based on the state standards, and taking into account the features of its software implementation in order to increase speed. Its implementation will ensure sufficient scalability, stability, reliability, and multi-level recognition.

Keywords: vehicles recognition, friend-or-foe, cryptography, cryptanalysis, UAV.

The year 2022 showed an urgent need to improve the existing systems for recognizing objects in the aerial space, which is caused by the significant increase in the number of technical means (especially unmanned aerial vehicles) on the battlefield. Thus, the creation of an army of drones was announced in Ukraine [1]. This concept focused on procurement, repair and replacement of the massive number of UAVs. At the first stage of the program implementation 200 tactical level UAVs will be purchased for air reconnaissance. At the second stage each unit of the Armed Forces will have its own reconnaissance UAV.

It should be considered that this will lead to a huge increase of the UAVs number that could simultaneously be in the airspace control zone. Also, in addition to the tactical reconnaissance UAVs of the Armed Forces units, strategic reconnaissance UAVs, reactive and ballistic missiles can be present in the same airspace – and all this together with the usual airplanes and helicopters. And then this number should be at least doubled – to consider the corresponding number of enemy targets in the air.

Such a sharp increase in the number of objects that simultaneously takes part in combat operations in the air requires the improvement of military object recognition systems, both qualitatively and quantitatively. This requires the development of appropriate new generation Friend-or-Foe algorithms for the objects' recognition.

It is also necessary to consider the fundamental differences in the requirements for the aerial objects recognition systems of civil and military use. When describing them, let us use the definition "legitimate aerial object" – this is an aerial object that has the right to be in the given airspace, has a working respondent of the aerial objects identification system and provides correct answers to requests from the identification center.

## The main requirements for recognition systems of civil application aerial objects

Let's determine the main requirements for recognition systems of civil application aerial objects (responders for the civil air traffic control system):

1) Maximum compatibility. The identification system must determine the identity of every aerial object, including aircrafts and helicopters of large and small airlines from around the world plus ones that belong to the private owners.

2) Support for a large number of objects. In connection with the number of aerial vehicles increase, aerial object recognition systems (especially when used at large airports) must support the processing of many aerial targets at the same time.

3) Outdated recognition complexes support. The civil air traffic control system must support cases when a request is received from an aerial object is based on an outdated recognition algorithm – to be able to correctly process the received response and determine the object's ownership.

4) Support for alternative ways of recognition. In the case when automatic recognition of an aerial object has failed, the controller must be able to find out the ownership of the aerial object using an alternative way. This usually could be done by manual request using radio communication.

5) Support for alternative data entry methods. In the case when the object's ownership was determined by an alternative way, the operator should be able to enter the received information into the system manually, so that other operators wouldn't have to use alternative identification methods again.

6) Determining the coordinates of aerial objects in an emergency situation. This should happen when the aerial object sends a special "Alarm" signal or a distress signal.

## The main requirements for recognition systems of military application aerial objects

Now let's consider the difference with the recognition systems made for military applications. The basic operational principle of any modern government identification system used in military applications is to process the incoming request according to a formula that is a cryptographic secret and changes regularly (for example, every 24 hours). In contrast to civil systems, the following **basic requirements** have been identified for them:

1) Maximum recognition process speed. 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, even human losses. So, for example, for anti-aircraft missile systems, the target's stay in the affected zone usually does not exceed a few tens of seconds. This is especially relevant for UAVs, as UAVs usually have very strict limitations on the amount of free space for installing the recognition system, and its weight and power consumption – and, accordingly, on speed and the amount of available memory for this system. So, the development process of the software component of this system should take this into account.

2) Protection against false positives. For civil applications, cases of trying to pretend that aerial object is not what it is truly is theoretically unlikely (and without involvement in military applications have not yet occurred) - because in such situation the aerial object owner will not be able to avoid responsibility and will lose a large amount of money in fines and lawsuits. On the other hand, in military applications, since the enemy is most interested in pretending that its aerial objects are belong to us (and therefore – avoiding facing anti-aircraft defense system) so it is ready to spend almost unlimited time and resources for this, and the result of a false-positive result of the aerial object recognition can be airstrikes and human casualties, then protection against such situations should be the highest priority of the state recognition system.

3) Protection against response imitation of a legitimate aerial object. Since the entire exchange of information in the state identification system "friend-or-foe" is carried out through the radio air, it is quite possible that all the data circu-

lating between the legitimate aerial object that gives a correct answer to the "friend-or-foe" request, and the recognition center on the ground, can be intercepted by the enemy. After that, the enemy can try to simply repeat the same responses to requests from the recognition center or try to change them in a way that simulates a legitimate aerial object's response. That is why the state identification system must be reliably protected against this type of attacks.

4) Support for a large number of objects. As already mentioned above, "friend-or-foe" military identification system must support the simultaneous recognition of multiple aerial objects of different types to determine the identity of aircraft, helicopters, UAVs and their swarms and cruise missiles in a timely manner.

5) Protection against cases of a legitimate air object loss. This requirement should be considered if a legitimate air object was shot down over the enemy territory or fell into the enemy's hands by some other way. If there is no such protection, then the situation described above will lead to the entire "friend-or-foe" identification system compromise and the state will have to replace it on all legitimate aerial objects and recognition centers. Such situation has already happened in the past, for example, in the Soviet Union [2]. Thus, it is not the answer itself that should be secret, but the information held inside it, and it should be possible to easily replace it without changing any hardware – just with the software update.

6) Rotation of the secret part. To prevent the possibility of theft of the "friend-or-foe" system secret part, for a government identification system of military application, the secret part rotation should take place on a permanent basis. Normally, the recommended value is to change the secret answer every day. This requirement overlaps with and complements the previous requirement.

7) Protection against false-negative results to prevent friendly fire. As already mentioned above, the exchange of questions and answers with the aerial object takes place through the radio air. In the case of military operations, such an exchange is usually complicated (for example, by using electronic warfare (EW) means, both friendly and hostile). But the "friend-or-foe" recognition complex must work as reliably as possible to prevent non-recognition of the correct answer from a legitimate aerial object (for example, due to non-receipt or partial arrival of the correct answer to the recognition center due to the EW means effect). This problem is very relevant to prevent the activation of, for example, anti-aircraft weapons against friendly targets (the so-called "friendly fire"). The problem may seem far-fetched – but, for example, the US troops during the operation "Desert Storm" in 1991 suffered 23% of all losses from "friendly fire" [3].

8) Protection against man-in-the-middle attacks. Consider the following situation: a legitimate aerial object is over territory controlled by an 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 aerial object and the recognition center there is situated an enemy ground complex equipped with a radio communication system. Also, there is an enemy aerial object moving to our aerial space. Our recognition complex sends a recognition request to the enemy's aerial object. It relays the request to the enemy's ground complex, which transmits it to the legitimate aerial object. The legitimate object sends a response, which is again relayed from the enemy's recognition center to enemy's aerial object. And the object relays this response to the legitimate recognition center. As a result, the recognition center will consider the enemy aerial object to be legitimate – so we have a false positive result of the "friend-or-foe" recognition.

9) Flexible integration with the NATO block recognition system. Since Ukraine is on course for Euro-Atlantic integration and is rapidly moving to NATO standards, in the future there will be a moment when it must integrate the military object recognition system with the corresponding system of NATO countries – for international trainings and operations.

10) Purely domestic "friend-or-foe" recognition system production and support. If for civil systems it is possible to purchase the system (as a whole or its components) abroad, but for the military recognition system such an approach is inadmissible due to the increased risks of information leakage to potential enemies.

11) Protection against EW means. This requirement relates to several others and determines that the "friend-or-foe" recognition system must work and determine the belonging of aerial objects even in the case of active use of radio-electronic warfare.

12) Support for several recognition modes. Usually, when identifying military objects, the support of such requests as "Where are you?" and "Who are you?" must be ensured. In addition, standard and control recognition modes should be supported (to detect enemy air objects that use interference against recognition means).

13) Automatic blocking of the ground-to-air and air-to-air means of attack launch against objects that confirm their legitimacy by a correct response to a recognition request.

14) Determining the coordinates of aerial objects in an emergency situation. The special signal "Alarm" must be general and unchanged in all situations – and the signal about any happening accident as well – and can be accompanied by additional useful information.

The only overlap in the requirements for the recognition systems of civilian and military objects are the support of a large number of objects and special signals for emergency situations.

## Current situation analysis – advantages and disadvantages of the current "friend-or-foe" object recognition system

To date, the "Parol-M" hardware/software complex, which is a modification of the Soviet Union system, developed in the 1980s and was itself developed as a replacement for the long-outdated "Kremniy-2" (2M) complex, which supported only 10 requesters and 10 respondents at the same time.

The technical capabilities of the “ Parol-M” complex provide for the simultaneous recognition of up to 110 requesters and 110 responders [4]. At the same time, a similar system in the NATO countries– MarkXII – performs 400 polls per second in the nominal mode [5].

**Advantages of the “friend-or-foe” identification system currently used in Ukraine**:

1) Presence of an anti-imitation recognition mode.

2) Availability of guaranteed recognition mode.

3) The ability to perform the recognition procedure even in conditions of high-intensity interference application by EW means.

4) Availability of individual codes for recognition based on the principle “Who are you?”

5) Protection against receiving responses on the side lobes of the directional diagram.

6) Application of a high frequency range.

7) Variation in the frequencies of requests and responses [2].

**Disadvantages of the “friend-or-foe” identification system currently used in Ukraine:**

1) Support of an insufficient number of recognition objects.

2) Insufficient radio-electronic protection of the recognition process.

3) Insufficient imitation resistance – the probability of imitation of a correct response by the enemy is as much as 0.5% [2] – that means that in the case of sending a swarm of 200 enemy UAVs, one of them will be able to pass through and pretend to be a legitimate aerial object.

4) Lack of interaction with all types of ground weapons (armored ground vehicles, manual anti-aircraft defenses, etc.) to prevent friendly fire.

5) Absence of the possibility of integration with the NATO “friend-or-foe” recognition system.

6) Insufficient number of individual identification codes for such requests as “Who are you?”.

7) High probability of detection and interception of recognition signals.

8) The operation of the system is known to the enemy (specialists from the Russian Federation) in almost all details.

In NATO countries, a large amount of works [6]-[8] is devoted to the issue of object recognition on the battlefield. Among the areas of development of the so-called Battlefield Combat Identification System (BCIS), the following should be highlighted:

1) Identification based on means of automatic radio data transmission about one’s troops (Radio Based Combat Identification – RBCI).

2) Identification using radio tags (Radio Frequency Identification tags – RF tags).

3) Targets recognition on the battlefield (application of Battlefield Target Identification Devices – BTID).

**RBCI**, also called Battlefield Force Tracking System (BFTS) or Blu-Force Tracking (BFT) System, is built on network-centric principles. Each legitimate aerial object equipped with the system transmits data about its location every 5 minutes by means of satellite communication or in the VHF communication network. In active mode, the requester sends a general request with coordinates – and the responder compares the received coordinates with their own, and if they match – sends a response. All data in wireless communication channels is 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, rapid aging of data for fast-moving objects, high impact of EW means and high cost of the system.

Recognition with the help of **radio tags** (RF tags) is also based on the “request-response” principle, as for civilian tags, used, for example, at a warehouse, the response is formed by modulating the incoming request. Active (similar to BTID), semi-active (have their own power source) and passive (powered by the energy of requests from the requester) tags may be used. The detection range of an active or semi-active tag can reach 40 km [6]. In fact, radio tags are currently the only potentially applicable identification method for determining the affiliation of individual enlistee or small units of them on the battlefield. And due to their small size and power requirements, they are potentially applicable for UAVs as well.

**BTID systems** are designed to recognize aerial objects in the “friend-unknown” format. Its essence does not differ from the general recognition of the “friend-or-foe” identification at Mk XII system. The term “unknown-friend” was introduced into military practice in view of the fact that an object of recognition that does not respond to a request is not necessarily an enemy object [6]. BTID systems also work on the “request-response” principle, the signals are encrypted and, to reduce the probability of interception, broadband.

## New “friend-or-foe” recognition algorithm

The state “friend-or-foe” recognition algorithm must be built based on the national state standards. In fact, it should not be a single algorithm, but a family of algorithms – since the same algorithm cannot be used, for example, for the “land-aircraft” recognition line, as for the “aircraft-tank” line. At the same time, during the algorithms and corresponding software development the specified requirements, presented in the previous subsections, must be considered.

The algorithm and procedure for generating random keys should be highlighted separately. It should also be based on the national state standards. This procedure would be applied on an ongoing basis due to the requirement for constant key rotation. Generation of a pseudorandom sequences could be used for this goal. Another option is to use a physical generator to produce random sequences (for example, by saving the parameters of parasitic transistors capacitances etc.) [9]. But as the requirements to the software performance of these algorithms aren’t that severe (generation may take hours to complete and may be done with the parallel algorithms on the cluster, or just powerful hardware), so they wouldn’t be analyzed in more detail.

**The recognition system includes** (figure 1):

1) The main recognition center.
2) Recognition centers (usually installed at radar complexes).
3) Centers for launching aerial objects (airports and military units, armed with UAVs).
4) Aerial objects (manned and unmanned).
5) Ground objects*.
6) Naval and underwater objects*.

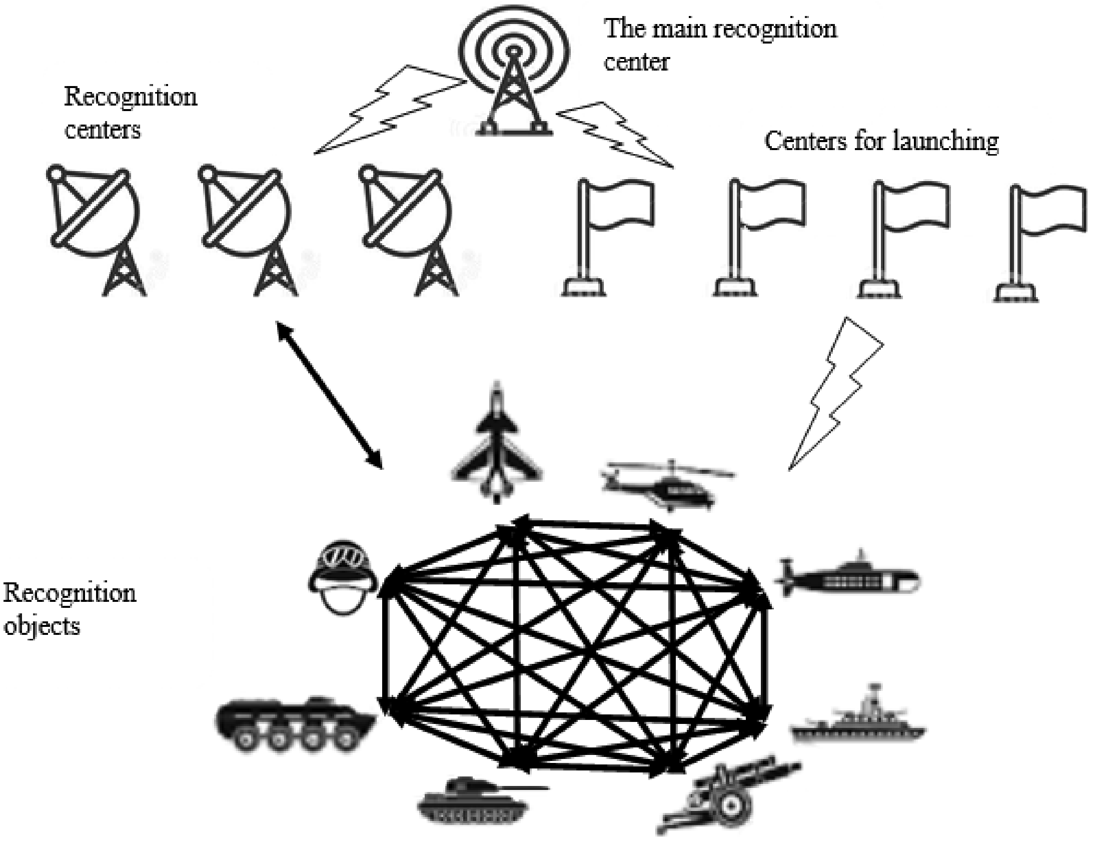

Figure 1. The composition of the “friend-or-foe” recognition system

* This work deals mainly with aerial objects. In case of expanding the work of the friend-or-foe” recognition system to land and naval objects, the recognition system should include headquarters (for distributing keys from the main recognition center to land objects) and ports (for water/underwater objects objects). At the same time, since ships and submarines can perform tasks autonomously for more than one day, this specificity should also be considered separately when implementing “aircraft-ship”, “ship-aircraft” recognition lines etc.

**The general scheme of the “friend-or-foe” recognition system** (figure 2):

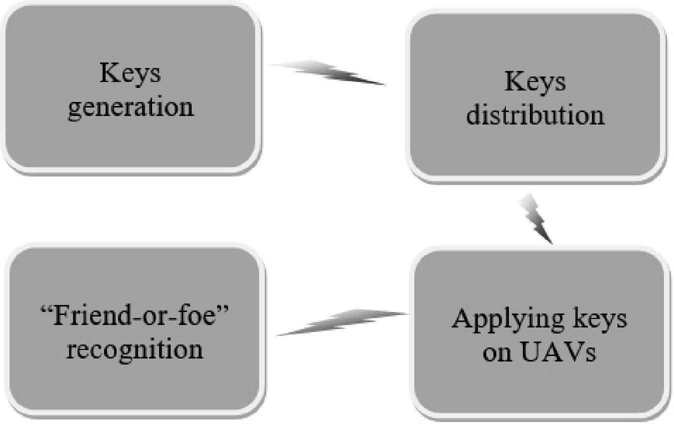

Figure 2. The general scheme of the “friend-or-foe” recognition system

1. The main recognition center generates random keys (general and individual, for recognition based on the "Who are you?" principle). New keys are generated every day. In this case, even if the current keys are compromised, the system will be protected again the very next day.

2. At the end of each day, the keys generated by the main recognition center are sent to all recognition centers and aerial objects launch centers (if necessary, to headquarters, etc.).

3. Next day, before each flight of manned and unmanned aerial vehicles, the keys are stored in their memory.

4. During the execution of the flight task, if necessary, recognition takes place along the required recognition line.

Due to the existence of two conflicting requirements for the "friend-or-foe" recognition system (recognition must occur as soon as possible to prevent friendly fire – but it must be reliable so that the enemy cannot deceive and bypass the air defense system), identification is proposed to be carried out in two stages:

1. Stage 1. Maximum speed, but reliable recognition is not fully guaranteed. Does not answer the questions "Who are you?", "Where are you?".

2. Stage 2. A slower, but better protected stage, which verifies the correctness of Stage 1 object recognition. Can answer the questions "Who are you?", "Where are you?".

These stages determine **the statuses of objects in the "friend-or-foe" recognition system** (figure 3):

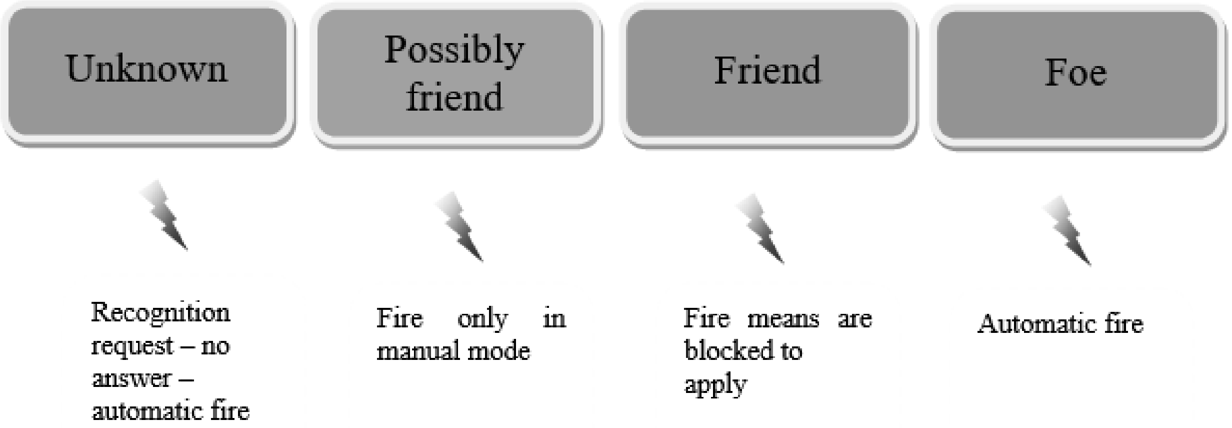
Unknown
Possibly friend
Friend
Foe
Recognition request – no answer – automatic fire
Fire only in manual mode
Fire means are blocked to apply
Automatic fire

Figure 3. The statuses of objects in the "friend-or-foe" recognition system

1. "Unknown". Before the first stage of recognition, the object to which the recognition procedure is applied is considered "unknown".

2. "Possibly friend". This status is assigned to an object that has successfully passed the first stage of recognition.

3. "Friend". This status is assigned to an object that has successfully passed the second stage of recognition.

4. "Foe". This status is assigned to an object that has failed the first or second stage of recognition and given a wrong answer.

**From the software implementation point of view** – as it was mentioned above, most of the UAVs have very limited power and space resources for installing "friend-or-foe" recognition system. So, it should be done as small and low power-consuming as possible. In the result mostly single-plate computers or even integrated circuits are used. Their performance in most cases is poor. Therefore, the first stage algorithm should be able to be implemented programmatically on such hardware and work fast on it. So, it must be as simple as possible. And as the most cryptographic algorithms (even symmetric ones) are pretty resource-consuming, it should be considered as well.

Now let's describe **the developed fast, but not fully guaranteed reliable algorithm of Stage 1 and aspects of its software implementation**:

1. As described above in the general scheme of the recognition system, the main recognition center generates random keys (common to all objects of the recognition system) valid for 24 hours. For stage 1, three keys are generated - a 128-bit request key *KI*1 and a 64-bit response key *KI*2. These two keys will be common to all recognition centers and objects. In addition, an enough number of random request identifiers of one-time use $IZ_i$, $i$= 1...$N$ are generated, the number of which $N$ depends on the expected volumes of state identification request-response procedures during the next 24 hours. Each of these request identifiers is 128 bits long. Each day, the main center will generate new sets of $N$ $IZ_i$, *KI*1 and *KI*2, and it is better to generate more $N$ request identifiers than needed instead of not enough – to have a reserve in case of an unexpected activity increase in the controlled airspace.

2. Keys and request identifiers are distributed between $M$ recognition centers and launch centers (airports, military units armed with UAVs etc.). At the same time, everyone is given the *KI*1 and *KI*2 keys, but everyone receives their own disjoint subset $P_j$ ($j$=1...$M$) from the entire set $N$ $IZ_i$ – so each subset:

$$\mathrm{Pj} \subset \mathrm{N}$$

Herewith:

$$P_1 \cap P_2 = P_1 \cap P_3 = \ldots = P_{M\text{-}1} \cap P_M = \varnothing$$

That means that no subset has elements in common with any other subset.

3. Before letting the recognition object (aircraft, UAV etc.) taking off on a task, the launch center transmits $KI1$ and $KI2$ keys, as well as a disjoint subset $P_{jk}$ ($k$=1...$S$, where $S$ is the expected, planned volume of requests from the object of recognition) of the subset $P_j\ IZ_i$.

4. To carry out Stage 1 of the recognition procedure, the requester (for any of the lines of recognition, the algorithm is unchanged) forms a request: with the operation of exclusive disjunction (which also has the names exclusive OR, or XOR) encrypts the previously unused $IZ_i$ request identifier with $KI1$ key, at the output we receive a 128-bit encrypted recognition request $R_a$ s, which is sent to the respondent:

$$R_a = KI1 \oplus IZ_i$$

XOR was chosen for speeding up software work – as it is very fast operation to perform on any hardware.

5. The respondent (for example, the UAV) receives the $R_a$ request.

6. The respondent uses the key $KI1$ and decrypts the received $R_a$ request using the exclusive disjunction operation (due to the double XOR operation using the key $KI1$, it deletes itself):

$$R_b = KI1 \oplus R_a = KI1 \oplus KI1 \oplus IZ_i = \mathrm{IZ_i}$$

7. The respondent performs an exclusive disjunction operation on the first and second halves of the deciphered $IZ_i$ identifier – $IZ_i1$ and $IZ_i2$:

$$R_b = IZ_i1 \oplus IZ_\mathrm{i}2$$

In this way, the respondent receives a block $R_b$ with a length of 64 bits.

8. The respondent encrypts the received block $R_b$ by an exclusive disjunction operation with the $KI2$ key:

$$R_c = R_b \oplus KI2$$

9. The respondent sends the requester an answer – $R_c$.

10. The requester decrypts the received answer $R_c$ with the $KI2$ key:

$$R_d = R_c \oplus KI2 = R_b \oplus KI2 \oplus KI2 = R_b$$

11. Immediately after step 4, the requester performs the same action as the responder at the step 7 – an exclusive disjunction operation on the first and second halves of the used identifier $IZ_i$ to obtain a control value:

$$R_k = IZi1 \oplus IZ_\mathrm{i}2$$

12. After receiving and decoding the answer from the respondent, the requester compares the decoded answer $R_d$ with the control value $R_k$. If they match, the respondent has successfully passed the check and receives the status "Possibly friend".

It is also possible to further simplify and speed up Stage 1 – to abandon the use of the $KI2$ key, and discard steps 8 and 10, then at the cost of a slight decrease in system reliability, you can get rid of two encryption/decryption operations.

Let's consider what data an attacker can get from a request and response exchange intercepted on the radio during the Stage 1.

An attacker can intercept two messages transmitted over the radio air – the request $R_a = KI1 \oplus IZ_i$ at step 4 and the response $R_c = R_b \oplus KI2$ at step 9.

If the public key $KI1$ and the identifier $IZ_i$ are presented in the form of two parts of 64 bits each (respectively $KI_{11}$ and $KI_{12}$, as well as $IZi1$ and $IZ_\mathrm{i}2$), then an attacker in the request can intercept at the step 4 next data:

$$\mathrm{DATAPACK1} = \begin{cases} KI_{11} \oplus IZ_i 1 \\ KI_{12} \oplus IZ_i 2 \end{cases}$$

In response, he can intercept:

$$\mathrm{DATAPACK2} = IZ1_\mathrm{i} \oplus IZ2_\mathrm{i} \oplus KI2$$

Since all the initial data that should remain hidden from the adversary ($KI_{11}$, $KI_{12}$ and $KI2$, as well as $IZi1$ and $IZ_\mathrm{i}2$) according to statistical characteristics should not differ from random ones, the means of statistical analysis will not be able to give the adversary any clues about these initial data according to intercepted datapacks.

If he tries to use the intercepted data to find out more by performing XOR operation, he can get the following combinations:

$$KI_{11} \oplus IZ2_\mathrm{i} \oplus KI2$$

$$KI_{12} \oplus IZ2_1 \oplus KI2$$

$$KI_{11} \oplus IZ2_\mathrm{i} \oplus KI_{12} \oplus IZ2_1$$

$$KI_{11} \oplus KI_{12} \oplus KI2$$

If an attacker sends (for the purpose of determining secret keys) a false identification request according to Stage 1, for example (for ease of understanding), it will consist of all zeros – then the respondent will perform a decryption operation on this request, receiving a sequence of two halves of the key $KI1$ – $KI_{11}$ and $KI_{12}$, then perform XOR operation on these keys – $KI_{11}$ and $KI_{12}$ – and then perform a XOR operation on the received result with the key $KI2$ – and sending the received result to the attacker.

That is, the attacker will again receive the sequence $KI_{11} \oplus KI_{12} \oplus KI2$ (or, in the case of using the simplified algorithm of Stage 1 – $KI_{11} \oplus KI_{12}$).

Since the statistical characteristics of the keys and identifiers will not differ from random ones, the obtained data will not give the attacker any useful information about the values of $KI_{11}$, $KI_{12}$, and $KI2$ – there is a very large (limited only by the size of the keys) number of variants of $KI_{11}$, $KI_{12}$, and $KI2$ sets (or in the simplified case - $KI_{11}$ and $KI_{12}$), which will correspond to the data known to the attacker. And he will not have the opportunity to determine which option from this set is correct, without going through them sequentially, using it as an answer to a request to the object of recognition, facing all the consequences of the fact that after an incorrect answer, this the object will be marked by the recognition system with the status “foe”.

Now, after this analysis, let’s describe **the advantages of Stage 1**:

1. Stage 1 is the fastest and does not require many hardware resources. To prepare a request, the requester should perform only one operation of exclusive disjunction (XOR) of two data blocks of 128 bits each. The length of the request is also only 128 bits. The respondent must perform three exclusive disjunction operations, the first for data blocks of 128 bits each, the second and third for blocks of 64 bits each. The response to the request is only 64 bits long. In the memory of the respondent (if it is not planned that he will perform the identification procedure as a requester) there should be space for only two keys with a total volume of 192 bits and the same amount of free memory should be available for performing decryption/encryption operations. So, from the software development point of view this algorithm is very fast.

2. Stage 1 recognition is sufficiently reliable. No data is transmitted with it in open form. The operation of exclusive disjunction is used for encryption, which is vulnerable to an attack on known plaintext. But in the case when each request identifier is used only once, and all request identifiers and encryption keys are generated in a truly random manner, then XOR provides sufficient robustness because:

a) Text and password have the same length.

b) No data in the message (request identifiers) is used more than once (reverse requirement of “no password is used more than once).

c) Both the password and the message are random and cannot be guessed either by a dictionary or by other methods (an enhanced requirement compared to the classic “password is random”).

d) If we consider request identifiers as one-time keys, then in the absence of any statistical regularities during their generation, the algorithm is close to 100% security.

3. Due to the physical features and limitations of the recognition procedure (blocking repeated requests for some time to prevent the processing of reflected signals behind the side lobes of the multi-channel receivers’ radar), it is protected from bruteforce attacks. In addition, you can set timeouts and block responses to requests from the same requester after a certain number of attempts.

**Disadvantages of Stage 1**:

1. Does not answer the question “Who are you?” and “Where are you?”.

2. Anyone can impersonate a legitimate requester. When performing Stage 1 recognition, the responder cannot verify the legitimacy of the request – and therefore will respond to any request of this format, including from an attacker sending a random 128-bit request without knowing any of the keys and identifiers.

3. Does not provide protection against “man-in-the-middle” attacks. If an attacker receives a Stage 1 request and sends it to a legitimate respondent, and then forwards its response to the requester, it can impersonate the legitimate respondent. The probability of this can be reduced by limiting the maximum response waiting time, but the theoretical possibility of such an attack remains.

4. Requires the daily generation of a large number of recognition identifiers.

To compensate for these shortcomings, the Stage 2 algorithm should be applied.

As an algorithm of Stage 2, it is possible to use the algorithm, based on Ukrainian symmetric cryptography standard  [10] proposed and detailly described in [11-12]. In case the direct object-object recognition (“plane-plane”, “plane-tank” etc.) should be provided without any of the objects being the recognition center, analogue of Kerberos protocol [13] may be used.

## Conclusions

In this work the main requirements for recognition systems of aerial objects of civil application were determined, which includes maximum compatibility; support for a large number of objects; outdated recognition complexes support; support for alternative ways of recognition; support for alternative data entry methods; determining the coordinates of aerial objects in an emergency situation.

Home-foreign recognition systems for military applications are also considered. In contrast to civilian systems, the following basic requirements have been identified for them: maximum speed of the recognition process; protection against false positive; protection against legitimate aerial object imitation; support for a large number of objects; protection against cases of loss of a legitimate aerial object; rotation of the secret part; protection against false-negative results to prevent friendly fire; protection against man-in-the-middle attacks; flexible integration with the NATO block recognition system; availability of opportunities for purely domestic production and support of the object recognition system; protection against electronic warfare means; support for several recognition modes; automatic blocking of the launch of ground-to-air and air-to-air weapons against objects that confirm their legitimacy by a correct response to a request; determining the coordinates of aerial objects in an emergency.

Based on the formulated requirements, a new friend-or-foe algorithm for the state identification system for military use is proposed, built based on the state standards, and taking into account the features of its software implementation in order to increase speed. Its implementation will ensure sufficient scalability, stability, reliability, and multi-level recognition.

## References

1. *The Government Portal*. (2022) The General Staff of the Armed Forces, the Ministry of Digital Transformation and UNITED24 are gathering the "Army of Drones". The Government Portal. 1st July, 13:25. Available from: https://www.kmu.gov.ua/news/genshtab-zsu-mincifri-ta-united24-zbirayut-armiyu-droniv. [Accessed: 2nd July 2022].
2. ERMAK, S.N., KASANIN, O.A. & KHOZHEVETS, S.N., (2017) *The Construction and Operation Principles of Ground Means of the State Identification System*. Minsk: BGUIR.
3. UNITED STATES OF AMERICA. Defense Technical Information Center, Department of Defense (1996) *Fratricide: Incorporating DESERT STORM Lessons Learned*. VA: Defense Technical Information Center.
4. ZAKREVSKYI O. (2014) *Friend-or-foe*. [Online] June 11, 2014. Available from: https://dou.ua/forums/topic/10097/ [Accessed: 2nd July 2022].
5. NATO (2016) STANAG 4193:2016. *Technical Characteristics of the IFF Mk XIIA System Part I: System Description and General Characteristics*. NATO.
6. KAMALTINOV G.G., et al. (2016) Recognition of objects on the battlefield. Analysis of world experience. *Armament and military equipment.* 4. p. 22-26.
7. Putatunda, R., Gangopadhyay, A., Erbacher, R. F., & Busart, C. (2022, May). Camouflaged object detection system at the edge. In *Automatic Target Recognition XXXII* (Vol. 12096, pp. 177-187). SPIE.
8. Pearce, N. and Hamilton, S., (2021, October). IFF using Beamforming in Telemetry Beacons. In *2021 IEEE Western New York Image and Signal Processing Workshop (WNYISPW)* (pp. 1-5). IEEE.
9. ZHUYKOV V.Y. et al. (2016) *Adjustable power supply filters to protect information in microcontrollers. Monograph*. Kyiv, 184.
10. MINISTRY OF ECONOMIC DEVELOPMENT (2014) DSTU 7624:2014 *Information technologies. Cryptographic protection of information. Algorithm of symmetric block transformation*. SE "UkrNDNC": SSY.
11. Korolyov V.Y., Ogurtsov M.I. & Kochubinskyi A.I. (2021) Identification of Technical Objects in the Special Networks According to the Principle of "Friend or Foe". *Control Systems and Computers.* 4. p. 2-14.
12. OGURTSOV M.I. (2021) Development of a special algorithm for multifactor users' authentication. In *International Scientific Conference "Mathematical modeling, optimization and information technologies"*. Chişinău – Kyiv – Batumi, 15 - 19 November, 2021. p. 27.
13. Kuperberg, M. and Klemens, R., (2022). Integration of Self-Sovereign Identity into Conventional Software using Established IAM Protocols: A Survey. *Open Identity Summit* 2022.

Received 02.08.2022

***About authors:***

*Ogurtsov Maksym Igorovych,*
researcher,
number of domestic scientific publications – 49,
number of foreign scientific publications – 4,
Hirsch index – 4, ORCID number – 0000-0002-6167-5111.
**Mobile phone number**: +380637902010.
**Email**: maksymogurtsov@gmail.com.

***Place of work**:*

V.M. Glushkov Institute of Cybernetics
of the National Academy of Sciences of Ukraine,
03187, Kyiv, Ac. Hlushkova str. 40, building 1, apt. 801,
fax/phone +380445262008, email: incyb@incyb.kiev.ua

**Прізвища та ініціали авторів і назва доповіді українською мовою:**
Огурцов М.І.
Розробка алгоритму державного впізнавання типу «свій-чужий»
для побудови відповідного програмного забезпечення

**Прізвища та ініціали авторів і назва доповіді англійською мовою:**
Ogurtsov M.I.
Friend-or-Foe Recognition Algorithm Development
for the Corresponding Software Building