1. Mathematical models of attacks

In order to recognize attacks based on the attacker model described in [12], mathematical models of four types of attacks on TMI were developed.

1.Attack. Overlay multiplicative noise

1A. Attack in the entire time window. The monitored parameter after manipulations by the attacker takes the following value:

, (1)

- iteration number in a time window of length n,, - the parameter value in the i-th iteration,

- the value of the parameter, after manipulation by the attacker,

- coefficient, a random number, and

1B. Attack in part of the time window. The parameter after manipulation by the attacker takes the following value:

(2)

- natural noise ratio arising from data transmission, which is a random number in a small range

1C. Attack in a small part of the time window. The parameter after manipulation by the attacker takes the following value:

(3)

2. Substitution of data similar to real ones.

2A. Attack in the entire time window. The parameter after manipulation by the attacker takes the following value:

, (4)

- coefficient, a random number, and

- coefficient, a random number, and .

We also prohibit the mutually compensating values and. For example, the following event cannot be perceived as an attacked signal:

2B. Attack in part of the time window. The parameter after the manipulation of the attacker takes the following value:

(5)

2C. Attack in a small part of the time window. The parameter after manipulation by the attacker takes the following value:

3. Increase or decrease the signal while maintaining the behavior of the signal (Additive Noise Overlay)

3А Attack in the entire time window. The parameter after manipulation by the attacker takes the following value:

, (7)

- - coefficient, a random number, and .

3B. Attack in the entire time window. The parameter after manipulation by the attacker takes the following value:

(8)

3C. Attack in a small part of the time window. The parameter after manipulation by the attacker takes the following value:

4. Forgery of controllers and external influences. When falsifying control and external influences, the model will generate signals from the automatic control system of the gas turbine engine that do not correspond to the actual values of the parameters. Thus, the data generated by the model can be considered attacked.

4A. Impact across the entire time window. To simulate this kind of impact, you can substitute a real signal into any function

., (10)

- parameter value generated by the model for forged control actions, - any function.

4BAttack in part of the time window. The parameter after manipulation by the attacker takes the following value:

(11)

4C. Attack in a small part of the time window. The parameter after manipulation by the attacker takes the following value:

(12)

1. Construction of classifiers for the presence and type of attack on TMI

To build a classifier of the type of attack on TMI, it is necessary to form a training and test sample. To create such samples, 14000 time windows were formed, 15 samples each. For the experiments, the specific fuel consumption G was taken as the parameter modified by the attacker.

An example of some time windows for building an attack type classifier is presented in Table 2.

Table 2 Time windows

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Model data | | | Attacked/not attacked data | | | State class | Attack type | | | | |
| G0 |  | G14 | Ga0 |  | Ga14 | S/D | 0 | 1 | 2 | 3 | 4 |
| 2,8 |  | 4,0 | 2,8 |  | 3,8 | D | 0 | 1 | 0 | 0 | 0 |
| 1,3 |  | 1,3 | 2,2 |  | 44. | S | 0 | 0 | 0 | 0,4 | 0,6 |
| 1,3 |  | 1, | 1,4 |  | 1,4 | S | 1 | 0 | 0 | 0 | 0 |

If data with different types of modifications fell into the same time window, the shares of the attacks were entered in the "Attack type" columns, as shown in line 2.

Attack type classifier is a multi-input and multi-output classifier, so conventional classification algorithms (for example, the usual kNN and Random Forest) are not suitable for this task. An algorithm is needed to build multiple regression. To solve this problem, Multioutput random forest regressor is used.

The quality of classification of attack types by this method was 0.65.

The low quality of classification by multiple regression methods forces us to switch to more complex classification algorithms. It is necessary to apply algorithms built on neural networks to this problem.

Neural networks are a universal tool for approximating functions, which allows them to be used in solving classification problems [13]. A typical task when using neural networks is choosing the neural network architecture (number of layers, activation functions, etc.) for each task. Table 3 shows the iterations done to find the attack type classifier.