Development of an Intrusion-Detection System in Distributed Energy Systems

Yakov Lvovich, Igor Lvovich, Aleksandr Ostapenko, Andrey Preobrazhenskiy and Oleg Choporov

ABSTRACT

Actual problems associated with the detection of anomalies in distributed energy networks were considered. These anomalies can be correlated with intrusions. An analysis of promising algorithms that allow one to solve to a certain extent the problem of detecting anomalies is presented. The structure of the intrusion detection system in distributed energy systems is proposed.

INTRODUCTION

Distributed energy can be considered as one of the important components, showing the transition to modern technologies and their practical use [1, 2]. Modern energy systems are characterized by their digitalization, decentralization and intellectualization.

The distributed nature of such systems determines the appropriate security requirements. The objects of attacks can be a means of protecting information in the control computer networks, as well as various systems related to the prevention of intrusions. In this case, violations in the control system of intellectual energy facilities can be identified by analyzing the anomalies in the processed data.

FEATURES OF INTRUSION DETECTION IN DISTRIBUTED SYSTEMS

At the moment, it is impossible to talk about building a full-fledged theory that describes in a comprehensive way the process of detecting an intrusion in distributed systems.
energy networks. There are correspondent means and mechanisms, but not all of them can be correlated with the scientific description.

When detecting intrusions into distributed energy systems, several modules can be marked, which are combined to solve protection problems: a module designed for tracking; intrusion detection subsystem; subsystem related to the response to the recognized intrusion; control subsystem for all modules in the system data warehouse that is required for the functioning of the system; graphical interface module.

When detecting anomalies [3], it is assumed that any kind of abnormal behavior is associated with deviations from the profiles of normal behavior. A database should be created containing profiles for the activities to be monitored. In such cases, statistical methods are effective (associated with the apparatus of mathematical statistics). If the profile is described unambiguously, then any of the deviations can be considered as anomalous. But in practice, this is not always so.

You can talk about two extreme cases:
- the existence of false positives, when there is no possibility of an unambiguous correlation of anomalous and normal behaviors;
- the existence of omissions of intrusions into energy systems, when there is no possibility of unambiguous identification of anomalous behaviors.

In terms of practice, there are some problems:
- profiles showing normal behavior are not always easy to create;
- it is required that possible boundaries are determined according to the possible behavior of electricity consumers in order to avoid approaching the two extreme cases mentioned above.

Detection of abuse can be carried out on the basis of some action patterns that suggest anomalous activity.

Similar patterns can be built on the basis of different approaches:
- watching repetitions on some actions, when the attacker does not have sufficient information on access to some resources, but he will seek to do it again, and not once.
- control actions that do not correspond to current situations;
- demonstration of the use of vulnerabilities, both in software and hardware.

The main advantages associated with the statistical approach include the following: adaptation to how the object of research behaves; using key provisions of mathematical statistics as the basis.

Various sensors can be the objects of research, they read energy characteristics [4], as well as network devices [5, 6].

The approach is based on the fact that:
- for statistical evaluations of characteristics, one can speak of their permanent character [7];
- as an indication of the anomaly, one can consider a sharp character in the deviation of the expectation, as well as the variance.
PROPOSALS FOR THE STRUCTURE OF THE INTRUSION DETECTION
SYSTEM IN THE DISTRIBUTED ENERGY SYSTEMS

In order to create a combined approach to detect anomalies in distributed energy systems, the use of the following algorithms is proposed: the one of Brodsky-Darkhovsky (method 1), the one based on the Kolmogorov-Smirnov fitting criterion (method 2), the one based on statistical criteria (method 3).

Basing on such approaches, it is possible to analyze energy flows from the point of view of the presence of anomalies and jointly through the use of weighted voting, to make decisions about the presence of anomalies. The use of this approach allows one to improve the accuracy and completeness of classification, by minimizing errors of the 1 and 2 kinds. The minimization of errors is achieved due to the fact that joint decisions are made on possible anomalies, taking into account the availability of information about the quality of the classification regarding the methods used.

The F-measure (1) can be considered an indicator of the quality of the classification of anomalies, which is a function of the accuracy \( P_1 \) (2) and completeness of \( W \) (3).

\[
F = 2 \cdot \frac{P_1 \cdot W}{P_1 + W},
\]

\[
P_1 = 2 \cdot \frac{N}{N + E_2},
\]

\[
W = \frac{N}{N + E_1},
\]

where \( E_1 \) – the first kind error, \( E_2 \) – the second kind error, \( N \) – the number of correctly identified anomalies.

The procedure for voting on the presence of an anomaly is based on the following formula:

\[
V = \alpha F(A) + \beta F(B) + \gamma F(G),
\]

where \( F(A), F(B), F(G) \) – the F-measures of the above methods – 1, 2, 3, correspondingly.

If, based on the results of classifications, according to method 1, an anomaly is present, then \( \alpha=+1 \), otherwise \( \alpha=-1 \). If in method 2, an anomaly is present, then \( \beta=+1 \), otherwise \( \beta=-1 \). If in method 3, an anomaly is present, then \( \gamma=+1 \), otherwise \( \gamma=-1 \).
If \( S \geq 0 \), then the result of applying the combined method means that a network anomaly is present, if \( S < 0 \), then an anomaly is absent.

Among the shortcomings of the statistical approach, we can point out the low sensitivity of statistical systems with respect to the order in which events follow.

The above algorithms are combined into one module of the system.

The second module is based on expert systems [8], while it becomes possible to describe the model of invasions into energy systems using natural language when a high level of abstractions is reached.

The expert system itself is formed on the basis of a set of rules and facts related to the knowledge of specialists who are experts in the field of energy security. The facts, in this case, are considered in the form of initial data on the operation of energy systems [9,10], and the rules - in the form of algorithms for logical decisions about the presence of an invasion, based on the existing set of facts [11].

The database of the expert system should contain information on the scenarios of most of the known intrusions into energy systems. The disadvantage of practical use of expert systems in solving this problem is in the fact that there is no possibility to identify an unknown intrusion for which there is no record in the information database. Due to a small change in the scenarios of a well-known intrusion, an attacker can introduce difficulties in the operation of protection systems.

Figure 1 shows a block diagram of the proposed intrusion detection system in distributed energy systems.

![Figure 1. Block diagram of an intrusion detection system in distributed energy systems.](image-url)
CONCLUSIONS

The features of algorithms for analyzing anomalies in distributed systems were considered. The article gives proposals for the formation of an intrusion detection system, due to which it is possible to significantly reduce the risks associated with interfering with the operation of distributed energy systems.

REFERENCES