Behavioral Model of a Smart Grid Cyber-physical System Functioning under the Influence of MitM Cyberattacks

Anastasiia Nicheporuk[a], Andrii Nicheporuk[a], Andrzej Kwiecien [b]

[a] *Khmelnytskyi National University, Institutska str., 11, Khmelnytskyi, 29016, Ukraine*
[b] *Silesian University of Technology, Akademicka str., 2A, Gliwice, Poland*

Abstract

A study of the smart grid cyber-physical system functioning was conducted and a behavioral model of its functioning was proposed. The concept of the object, event and state of the cyber-physical system was formalized at the basis of the proposed set-theoretical model, which made it possible to reflect the trajectories of the system's functioning and the behavior of both individual objects and the cyber-physical system as a whole on their basis. The proposed model is the basis for the formalization and analysis of the impact of cyberattacks of various kinds on objects in the cyber-physical system and their trajectories. A formalization of the impact of Man-in-the-Middle cyberattacks on the control level of the cyber-physical system of a smart grid, in which the attacker is considered as a part of the system itself, is proposed. The proposed formalization of the impact of MitM cyberattacks on cyberphysical systems will allow describing known cyberattacks and forming parameterized procedures for their detection, which can be considered as complex features for detection.

Keywords

Set-theoretical model, object, event, state, man in the middle cyberattack, smart grid cyber-physical system

1. Introduction

The smart grid cyber-physical system is the implementation of the general concept of open cyber-physical systems, in which information processes related to the supervisory control of physical devices and the storage, transformation and processing of data from these devices take place, with the aim of automating and optimizing production processes. Smart grid use information and communication networks and technologies to collect information about energy production and energy consumption, which allows to automatically increase the efficiency, reliability, economic benefit, as well as the sustainability of the production and distribution of electricity for end users.

Consider a smart grid cyber-physical system, which is represented by three levels: a supervisory level, a control level, and a level of the physical equipment (or field level), represented by energy production and transmission equipment [1, 2]. The level of supervisory control is represented by a control center, a human-machine interface (HMI), a data server, while the router, gateway, remote terminal units (RTUs) (and/or programmable logic controllers PLCs) to which connected sets of sensors and actuators form the control layer [3]. The generalized scheme of the smart grid cyber-physical system is presented in fig. 1.

From the point of view of security and data protection, the level of supervisory management (communication network and structural objects of the cyber-physical system) is the most protected against cyberattacks [4, 5], which is due to their approximation to traditional IT infrastructures, for which the application of both hardware and software mechanisms for protection and detection of

IntelITSIS’2023: 4th International Workshop on Intelligent Information Technologies and Systems of Information Security, March 22–24, 2023, Khmelnytskyi, Ukraine

EMAIL: eldess06@gmail.com (A. Nicheporuk); nicheporuka@khmnu.edu.ua (A. Nicheporuk); andrzej.kwiecien@polsl.pl (A. Kwiecien);
ORCID: 0000-0001-5366-5792 (A. Nicheporuk); 0000-0002-7230-9475 (A. Nicheporuk); 0000-0003-1447-3303 (A. Kwiecien);

malicious influences, represented in particular by firewalls, intrusion detection systems, encryption of data transmission channels, backup, anti-virus tools, etc.

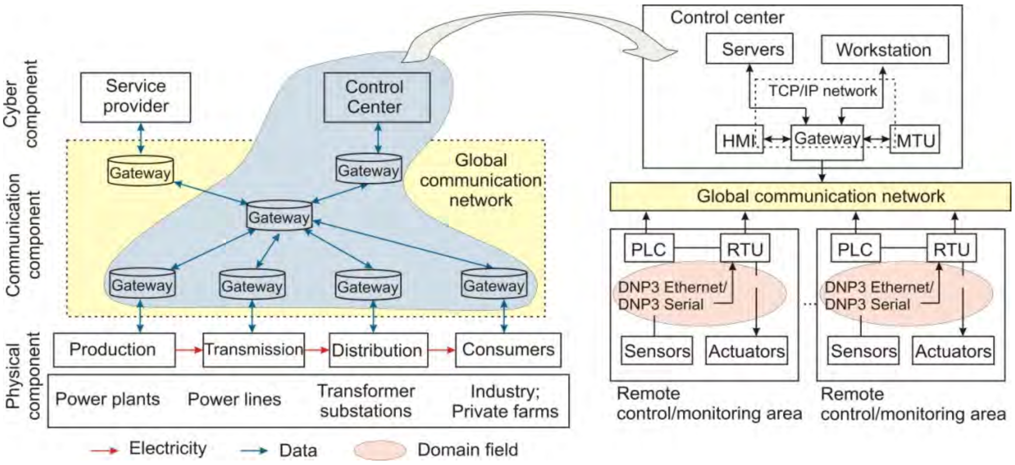

Figure 1: Generalized scheme of the smart grid cyber-physical system

At the same time, the control level is vulnerable to cyberattacks, which is primarily due to the use of special information transfer protocols DNP3, Modbus, IEC 61850, for which indicators of security and confidentiality of information transfer have taken a back seat, giving way to the effectiveness of information transfer between physical and cyber environment [6-8]. And also if it is taking into account the constant development of various technologies of hiding, encryption and obfuscation [9-11], then the situation will look even more complicated. Therefore, MitM cyber-attacks on the smart grid cyber-physical system will be studied in this work specifically for the control level. The purpose of this work is to study and formalize the process of the functioning of the smart grid cyber-physical (CPS) system under the influence of MitM cyberattacks in order to distinguish the procedures of their impact on the CFS, which in the final form will allow to form impact scenarios that can be considered as a complex features, and which in the future can be used as part of detection systems for based on machine learning algorithms [12, 13].

2. Related works

Today, the problem of ensuring the security of cyber-physical systems among scientists is receiving considerable attention.

In [14] authors have to model Smart Grid technology in order to evaluate specific cyber security threats on DNP3 operating in SCADA based implementation. To model the communication behavior between an attacker and legitimate devices, the authors used the principles of game theory and investigated attack scenarios such as a competition between an attacker and a defender, where the strategy of each side is to maximize their gains. In such an implementation, the game will be a non cooperative game between the attacker and the legitimate nodes, which can represent both master and outstations. Also Nash equilibrium was utilized to highlight possible outcomes of MITM attacks and to prove the pass and drop strategy effectively used to detect attacks and to provide understanding to mitigation

Authors of [15] compare the use of machine learning techniques to classify messages of the same protocol exchanged in encrypted tunnels. In theirs work it is considered four simulated cases of encrypted DNP3 traffic scenarios and four different supervised machine learning algorithms: Decision tree, nearest-neighbor, support vector machine, and naive Bayes. The results obtained show that it is possible to extend a Peekaboo attack over multiple substations, using a decision tree learning algorithm, and to gather significant information from a system that communicates using encrypted DNP3 traffic.

In work [16] authors proposed a method to detect attacks targeting SCADA systems. In proposed model the system behavior represent as a network of timed automaton i.e., a finite-state machine extended with clock variables. In order to investigate different cyberattacks the process of modeling and converting logs from SCADA systems into a network of timed automata is carried out. After that through timed temporal logic, they characterize the behavior of a SCADA system under attack.

The approach that utilizes correlated matrix-based object-oriented model for cyberattack modeling is proposed in [17]. In order to implement such approach, the procedure of the cyber-attack had been modeled by an object-oriented method, after that a correlated matrix model had been built for network topology, attack path, and attack procedure. To demonstrate the modeling method and its benefits, authors use the Man-in-the-middle Attack on measurement data of an Automation Voltage Control system as examples, and build a hardware-in-the-loop co-simulation platform to verify the model. However the structure of correlated matrix is relatively large, and its construction is not well-regulated and universal.

In work [18] a cyberattack simulation and evidence chains generation model which computes all possible attack paths associated with specific, confirmed security events is presented. The model considers various attack patterns through simulation experiments to estimate how an attacker has moved inside an organization to perform an intrusion. It analyzes artifacts, e.g., Indicators of Compomise, and any other incident-related information from various sources, e.g., log files, which are evidence of cyber-attacks on a system or network.

In the work [19], the authors investigated the impact of cyberattacks on the Water Distribution Systems. Authors have incorporates pressure readings in the detection algorithm as a constraint and develops a mixed integer nonlinear programming (MINLP) formulation to estimate the nodal demands of a network, as well as its flow rates and nodal pressure readings. These values were estimated using the SCADA readings for link flows, pump’s status, tank’s water level, and total demand of a district metering area. Nodal pressure heads were calculated using Bernoulli’s and Hazen-Williams equations and pump’s head equation.

3. Behavioral model of the CFS functioning

Analysis of the current state of research in the direction of CFS modeling showed that most approaches to CFS modeling are focused on ensuring their stability and reliability of functioning, and not on ensuring stability under the influence of cyberattacks and their timely detection. And although some known approaches are aimed at designing individual elements of systems taking into account potential violations of availability, integrity and privacy caused by cyberattacks, the development of complex models that would allow research and analysis of the impact of cyberattacks on the structural components of the CFS, as well as their identification, is an urgent task, which would become the basis for the design and verification of protected CFS.

Let us define as a *CFS object* an atomic structural node that performs the functions of processing, storing, transmitting information (servers of databases, applications, data processing, software that implements HMI, control systems, etc.), as well as execution, regulation and control components of the physical infrastructure (sensors, actuators, etc.). Each object has a set of parameters characterizing its properties (for example, a water valve has the properties nominal pressure, diameter, conductivity (open/closed)) and a set of states determined by a fixed set of parameters (for example, a water valve with the set value "open" parameter "conductivity").

Let's define the CFS object as a structural unit from which the CFS consists and present it in the form of a tuple as follows:

$$O = \langle type, K, S \rangle \tag{1}$$

where *type* – type of object that determines belonging to one of the levels O_P, O_C, O_N, which define the objects of the physical, cyber and communication components of the CFS, respectively, and which form a complete set of all the objects of the CFS:

$$\Omega = \{ O_P \cup O_C \cup O_N \} \equiv \{ o_i \}_{i=1}^{N_\Omega} \tag{2}$$

where N_Ω – the total number of CFS facilities at all levels;

$K = \{ k_i \mid 1 \le i \le N_K \}$ – a set of structural components that make up an object and with the help of which the functions of the object are implemented, where N_K – the number of components that make up the object o_j, $o_j \in \Omega$;

$S = \{ s_i \mid s_i \in s_0, s_\perp \}_{i=1}^{N_S}$ – the set of states that are defined for o_j, $o_j \in \Omega$, s_0 – initial state, $s_\perp$ – terminal state, N_S – the number of allowable states for the object o_j.

Along with the objects of the CFS, we will define the concept of an *event* that affects the object o_j from the side of other CFS objects $o_i \in \Omega$ or from the side of the object itself o_j, which is initiated by its structural components. In the first case, we will call such an event external, in the other case, internal. A set of external and internal events are catalysts for changing the states of the CFS objects.

We define each *state* in which the object is as follows:

$$S = \langle P, R, O_a, \gamma, t_s \rangle, \quad (3)$$

where $P = \{ p_i \}_{i=1}^{N_P}$ – set of object parameters o_j, where N_P – number of valid parameters for o_j, $o_j \in \Omega$. Changing the parameters of an object is the target function of the process of sending events by other objects or structural components of this o_j object. Thus, through changing the parameters of the object, a change in the state of the object is achieved.

$R = \{ r_i \}_{i=0}^{N_R}$ – the set of events that an object o_j can receive. Events in the CFS can be requests/responses to receive, process and transfer information between CFS objects. For example, read the value from the sensor, write the value to the database, execute the next block of commands (for example, in the case of a PLC or server), etc.

$O_a = \{ o_i \mid o_i \in \Omega, i \le N_\Omega \}_{i=0}^{N_O}$ – the set of objects from which the object o_j in state s_k can receive events;

$\gamma : R \times O_a \to \{ true, false \}$ – binary function for determining the right of an object o_j to receive an event in a state s_k. It should be noted that not all objects can send events to o_j, and even with a change of state o_j this set of objects is limited by the type of objects from which events can be received. In the case of a pair of objects (a_j, a_i), where $a_j, a_i \in \Omega$, o_j can receive messages from o_i, if $o_i(type) \le o_j(type) \le o_i(type)$, where sign $\le$ defines the logical comparison operation of the object level type in the level hierarchy $O_P < O_N < O_C$, that is, in other words, the type of objects o_i must be either the same as in o_j or a level higher/lower. This statement follows from the nature of the CFS and its ability to process information. It is not possible to transfer the sensor data immediately to the database server. For this, information should be transferred first through the network of devices, then to the management network through the programmable controller, then through the controller to the corporate network, and finally to the database server. That is, in this case, the information must go through all three levels in turn: physical, communication and cybernetic. It follows that communication level objects O_N can interact immediately as with physical objects O_P as well as with objects of cyber levels O_C.

$t_s = [t_{s_{begin}}, t_{s_{end}})$ – the time interval of the object being in the state s_k. The time interval of the object o_j being in the state s_k determines the period of activity of this state, during which the object o_j can receive events from other objects $o_i \in \Omega$, moreover $t_{s_{end}}^{s_k} < t_{s_{begin}}^{s_{k+1}}$ is the time of state termination s_k, and $t_{s_{begin}}^{s_{k+1}}$ is the start time of the next state s_{k+1}.

It should be noted that, for the sake of simplification, in this model of the CFS functioning, the state of its object is defined as a discrete entity, that is, one in which there is a clear boundary between two states. However, in practice, it is not always easy to discretize a specific state. If, for example, in the case of a water valve, which has two states open/closed, it is possible to introduce intermediate states open/close, then in the case of a cybernetic object, such as a server, which executes a large number of parallel processes and threads implementing different functions management of the system, it is problematic to draw a clear boundary between the states. Therefore, by the state of a cyber object we mean a higher-level abstraction of the concept of state. In the case of the server, by state we mean the processing of a request from the client and the execution of one process.

Let's define the transition function ξ, which determines the transition of the object from state s_k to state s_{k+1} under the influence of event *r*, at the moment of time t_i as follows:

$$\xi : s_k \xrightarrow{r,t_i} s_{k+1} \tag{4}$$

Then, if the object o_j is represented by a set of states, with the initial state s_0, then lets present functioning of o_j as a sequential change of its state, which are initiated by external or internal events:

$$\xi(o_j) : s_0 \xrightarrow{r_0,t_0} s_1 \xrightarrow{r_1,t_1} s_2 \xrightarrow{r_2,t_2} s_3 \ldots \rightarrow s_{i-1} \xrightarrow{r_{i-1},t_{i-1}} s_i \xrightarrow{r_i,t_i} s_{\perp}, \tag{5}$$

where $s_{\perp}$ – terminal state.

At the same time, we will say that one state is a cause, and another is a consequence, if in the sequence the first state precedes the second.

In a general sense, the terminal state $s_{\perp}$ of an object defines the point in time by which the functioning of the object as a part of the system ends. From the point of view of CFS, objects are functioning continuously (except for breaks for maintenance or exit from an emergency state), alternating cycles of activity with cycles of waiting. Therefore, in this model, we understand the terminal state as the point in time after which the object moves to the next iteration of the activity/waiting cycle.

We will call the expression of the non-empty finite sequence of changes in object states obtained in 5 *the trajectory of the object's functioning* t_{o_j}:

$$t_{o_j} = \bigcup_{i=1}^{N_S} s_i = s_0 \xrightarrow{r_0,t_0} s_1 \xrightarrow{r_1,t_1} s_2 \xrightarrow{r_2,t_2} s_3 \ldots \rightarrow s_{i-1} \xrightarrow{r_{i-1},t_{i-1}} s_i \,, \tag{6}$$

where N_S – the number of allowable states for the object o_j.

The trajectory of the object's functioning can be represented as a sequence of segments of the trajectories of objects interacting with it and the object's own actions over other objects of the CFS and itself, since any operation of obtaining, changing and transmitting information causes a change in the state of interacting objects. For example, in the case of a programmable logic controller, one trajectory of its operation can consist of the following sequence of states: reading a value from a sensor, reading a value from an input buffer, executing the program, writing the result to the output buffer, outputting the result to the executive mechanism. At the same time, another trajectory of operation can consist only of waiting for data from the sensor, by executing a sequence of commands of the waiting program.

The set of all available trajectories of functioning for the CFS object o_j is called the *behavior of the object* and is defined as follows:

$$\mathrm{X}(o_j) = \{ t_{o_j}^i \}_{i=1}^{N_{t_o}} \tag{7}$$

where N_{t_o} – the number of trajectories for the object o_j.

The behavior of the object shown in equation 7 determines its functioning as part of the CFS and allows describing all possible activities of this object.

After determining the atomic entities that make up the CFS, we lets proceed to the description of the functioning of the entire CFS.

Let's present the model of the functioning of the CFS through the functioning of a set of objects from which it consists:

$$M_{CPS} = \left\langle \Omega, S^*, X^*, R^* \right\rangle \tag{8}$$

where $\Omega = \{ o_j \}_{j=1}^{N_\Omega}$ $\quad S^* = \{ s_i^{o_j} \mid o_j \in \Omega, 1 \le i \le N_{S_{o_j}} \}$

$N_{S_{o_j}}$ – the number of allowable states for the object o_j;

$X^* = \{ X(o_j) \}_{j=1}^{N_\Omega}$ – the set of behaviors of all CFS objects; $R^* = \{ r_i^{o_j} \,|\, o_j \in \Omega, 0 \le i \le N_{R_{o_j}} \}$ – the set of events that can be received by CFS objects, $N_{R_{o_j}}$ – the number of events an object can receive o_j;

Fig. 2 shows a schematic representation of the model of the CFS functioning through the trajectories of the functioning of its objects. To simplify the modeling of the functioning of the CFS, it is presented through its three objects, which form three trajectories. Each object in the proposed model is capable of receiving and generating events from/to other objects, thereby performing inter-object interaction. This is the main mechanism of formation of new states of CFS objects.

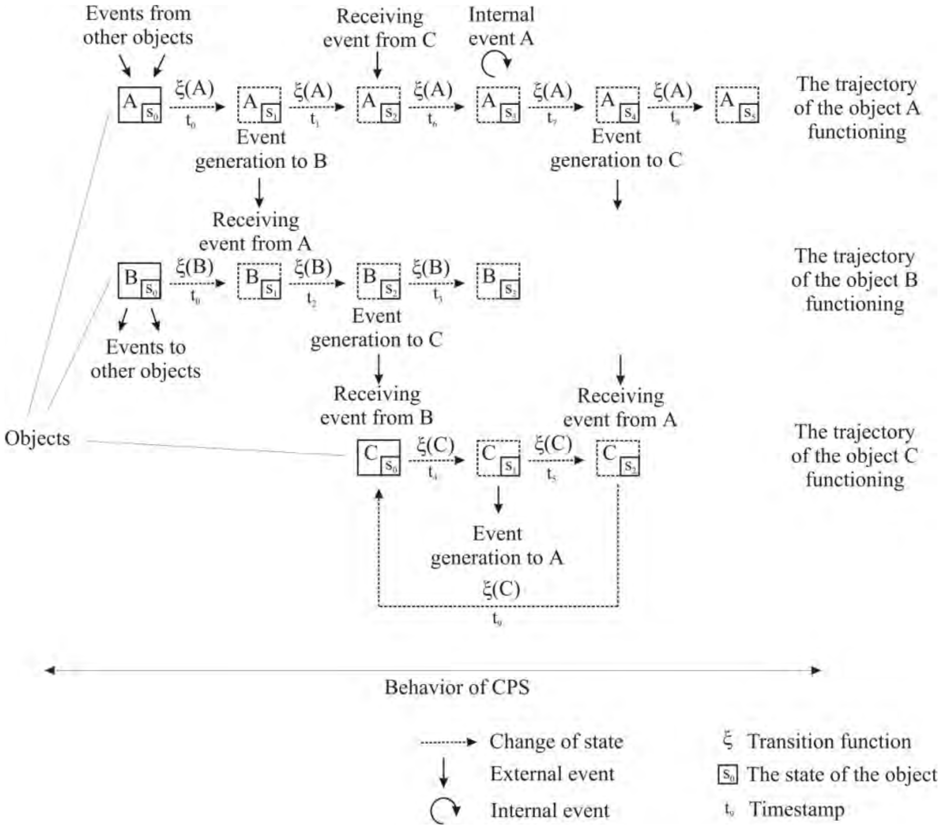

Figure 2: A schematic representation of the model of the CFS functioning through the trajectories of the functioning of its objects

The consecutive change in the states of the CFS objects forms the trajectories of the functioning of these objects. Each moment in time is characterized by the presence of CFS objects in a certain state. Therefore, the totality of all trajectories of objects in a certain time interval form the behavior of the CFS. In this way, the given schematic representation of the model of the functioning of the CFS is actually a reflection of the internal state of the CFS itself, through the state of its objects.

The formalization of a cyber-physical system based on the states of objects and their trajectories is general and can be used to detail the behavior of its individual objects. The proposed model is the basis for the formalization and analysis of the impact of cyberattacks of various kinds on objects in the cyber-physical system and their trajectory.

4. MitM cyberattacks on the control level of the cyber-physical system

A MitM cyberattack on cyber-physical systems is a passive or active form of interference in the communication channel of information exchange between system devices by legitimizing one's presence, thus becoming a full-fledged participant in the communication exchange [20, 21]. Thus, an attacker implementing a MitM attack on a smart grid can perform cyberattacks on false data injection and false command injection, which can endanger the operation of the entire power system, such as state assessments, its dispatching and automatic control of electric power generation.

When considering cyberattacks on the control level of the cyberphysical system of the smart energy supply network, we will assume that the attacker who implements the MitM cyberattack is a component of the cyberphysical system itself, i.e. expands the total number of objects in the set Ω:

$$\Omega = \{ o_j \}_{j=1}^{N_\Omega} \cup o_{MitM} \tag{9}$$

where o_{MitM} – an object of a cyber-physical system that compromises a communication channel and implements MitM cyberattacks.

This statement is based on the fact that in order to initiate a MitM attack vector on a component of a cyber-physical system (the communication channel between the MTU and a remote terminal unit), the attacker must be represented as an object of this system, that is, be a participant in the exchange of information.

The presence in the CFS of an object that implements MitM cyberattacks on multiple objects from set $\Omega \setminus o_{MitM}$ leads to the fact that a *parameterized attack procedure* is implemented, the result of which is the arrival of erroneous data and/or commands to the target object of the cyber-physical system [22]. The result of such a procedure for the target object o_{target} is a change in its parameters, for example, the "state" parameter of the automatic switching switch will change from "closed" to "open" or vice versa. Thus, according to expression 3, the state of the target object itself changes, which leads to the formation of a new trajectory of the object's functioning (change of the observed trajectory to a new one).

In fig. 3 presents a generalized representation of a MitM cyberattack. In the absence of compromise of the communication channel between node A (master station) and a set of outstations *B*

$$X_c = \begin{cases} \xi(B_1): s_{n-2} \xrightarrow{r_{n-2}, t_{n-2}} s_{n-1} \xrightarrow{r_{n-1}, t_{n-1}} s_n \xrightarrow{r_n, t_n} s_{n+1} \dots \rightarrow \\ \xi(B_2): s_{n-2} \xrightarrow{r_{n-2}, t_{n-2}} s_{n-1} \xrightarrow{r_{n-1}, t_{n-1}} s_n \xrightarrow{r_n, t_n} s_{n+1} \dots \rightarrow \\ \dots \\ \xi(B_m): s_{n-2} \xrightarrow{r_{n-2}, t_{n-2}} s_{n-1} \xrightarrow{r_{n-1}, t_{n-1}} s_n \xrightarrow{r_n, t_n} s_{n+1} \dots \rightarrow \end{cases} \tag{10}$$

where X_c –system behavior without compromising the information exchange channel.

Then, after conducting a MitM cyberattack and compromising the communication channels between *A* and $B_1, B_2, .., B_m$, the following trajectories can be obtained:

$$X_{MitM} = \begin{cases} \xi(B_1'): s_{n-2} \xrightarrow{r_{n-2}, t_{n-2}} s_{n-1}' \xrightarrow{r_{n-1}', t_{n-1}} s_n' \xrightarrow{r_n', t_n} s_{n+1}' \dots \rightarrow \\ \xi(B_2'): s_{n-2} \xrightarrow{r_{n-2}, t_{n-2}} s_{n-1}' \xrightarrow{r_{n-1}', t_{n-1}} s_n' \xrightarrow{r_n', t_n} s_{n+1}' \dots \rightarrow \\ \dots \\ \xi(B_m'): s_{n-2} \xrightarrow{r_{n-2}, t_{n-2}} s_{n-1}' \xrightarrow{r_{n-1}', t_{n-1}} s_n' \xrightarrow{r_n', t_n} s_{n+1}' \dots \rightarrow \end{cases} \tag{11}$$

where X_{MitM} the behavior of the system during the compromise of the information exchange channel.

Thus, starting from the moment of time t_{n-1}, the state of objects $B_1, B_2, .., B_m$ will change, which leads to a change in their functioning trajectories. As a result, for objects $B_1, B_2, .., B_m$, their behavior will change, which will include, in addition to trajectories $\xi(B_1)$, $\xi(B_2)$ and $\xi(B_m)$, also trajectories $\xi(B_1')$, $\xi(B_2')$ and $\xi(B_m')$.

If compare equation 10 and 11, and assume that the states *s* of the objects are unknown, then from the point of view of the MitM-type cyberattack detection process, the key point is to determine the set of events $r_i \in R$ that lead to a change in the state of the target object o_{target} and form new trajectories. In this case, if we consider the communication channel between the MTU and the remote telemetry device, the events will be the commands coming from the master node to the slaves (remote stations with a connected set of sensors and actuators), as well as data coming to the master station in response to receiving control commands. These data and commands are transmitted over communication channels via a plurality of TCP/IP packets, in which DNP3 packets are encapsulated, thereby forming network traffic. Considering the process of detecting MitM cyberattacks, an important task is their analysis and formalization of parameterized procedures for their impact on network traffic, which will allow forming impact scenarios and distinguishing a set of features (Fig. 4).

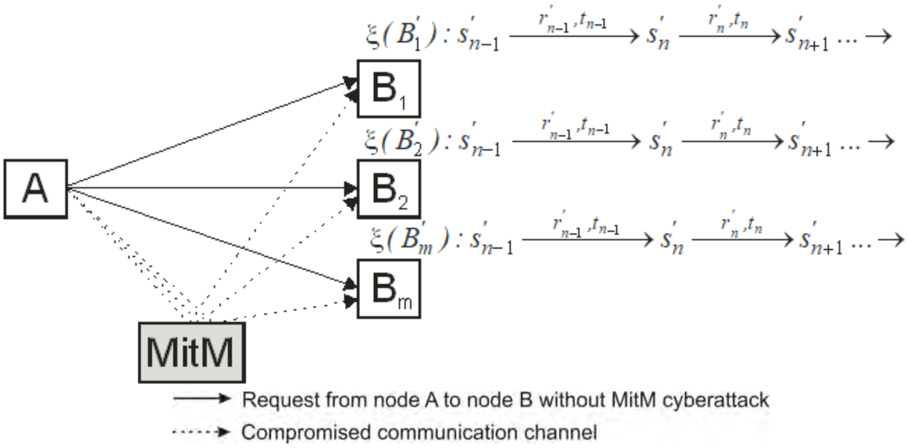
$\xi(B_1'): s_{n-1}' \xrightarrow{r_{n-1}', t_{n-1}} s_n' \xrightarrow{r_n', t_n} s_{n+1}' \cdots \rightarrow$
$\xi(B_2'): s_{n-1}' \xrightarrow{r_{n-1}', t_{n-1}} s_n' \xrightarrow{r_n', t_n} s_{n+1}' \cdots \rightarrow$
$\xi(B_m'): s_{n-1}' \xrightarrow{r_{n-1}', t_{n-1}} s_n' \xrightarrow{r_n', t_n} s_{n+1}' \cdots \rightarrow$
A
B_1
B_2
B_m
MitM
Request from node A to node B without MitM cyberattack
Compromised communication channel

Figure 3: A generalized representation of a MitM cyberattack

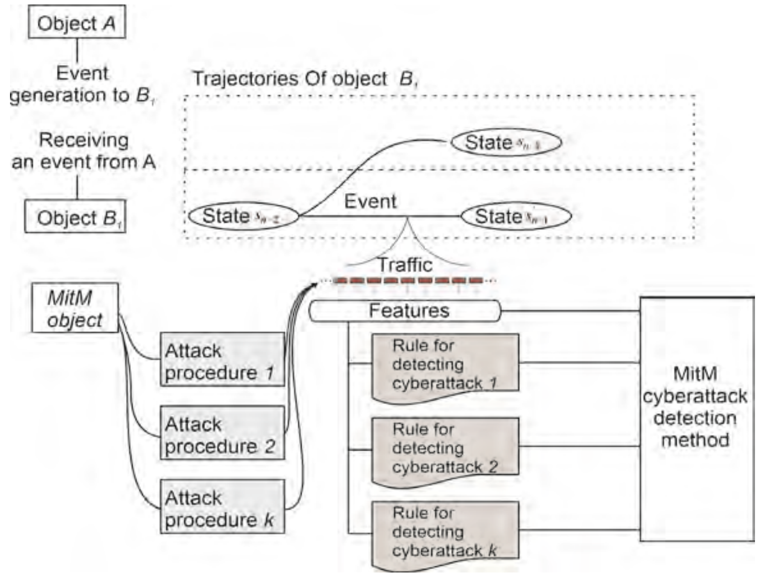
Object *A*
Event generation to *B*
Receiving an event from A
Object *B*
Trajectories Of object *B*
State
State
State
Event
Traffic
MitM object
Attack procedure *1*
Attack procedure *2*
Attack procedure *k*
Features
Rule for detecting cyberattack *1*
Rule for detecting cyberattack *2*
Rule for detecting cyberattack *k*
MitM cyberattack detection method

Figure 4: Formalization of the cause-and-effect relationship between the impact of MitM cyberattacks on the process of forming new trajectories of the CFS object and the rules for detecting this cyberattacks

Such scenarios can be used to form a base of rules, the mapping of which to a feature set will allow the process of detecting MitM cyberattacks.

5. Testbed implementation

To conduct a study of the impact of cyberattacks on the control level of the CFS, data exchange in which is carried out via the DNP3 protocol over TCP/IP, a testbed environment based on xMasterSlave [23] was deployed. This software allows to implement such operations as writing, reading, resetting, cleaning, etc. [24]. The libpcap library [25] was used to obtain network traffic data in the process of data exchange between the center controller and the outstation. The obtained data were stored in the database with purpose of its further research and analysis. A schematic representation of the research environment is shown in fig. 5.

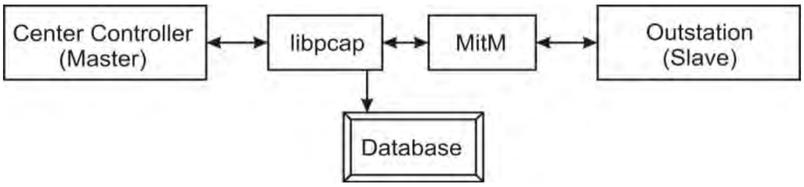

Figure 5: A schematic representation of testbed

6. Conclusion

The paper considers the functioning of the smart grid cyber-physical system was conducted and a behavioral model of its functioning was proposed. The concept of the object, event and state of the cyber-physical system was formalized at the basis of the proposed set-theoretical model, which made it possible to reflect the trajectories of the system's functioning and the behavior of both individual objects and the cyber-physical system as a whole on their basis. The proposed model is the basis for the formalization and analysis of the impact of cyberattacks of various kinds on objects in the cyber-physical system and their trajectories. A formalization of the impact of Man-in-the-Middle cyberattacks on the control level of the cyber-physical system of a smart grid, in which the attacker is considered as a part of the system itself, is proposed. The proposed formalization of the impact of MitM cyberattacks on cyberphysical systems will allow describing known cyberattacks and forming parameterized procedures for their detection, which can be considered as complex features for detection. To carry out the research, a simulation of the control level of the cyber-physical system was carried out, in which data exchange is carried out using the DNP3 protocol over top of TCP/IP in the xMasterSlave environment.

7. Future work

As a direction of further research, known MitM cyberattacks on the control level, in which data exchange is carried out using the DNP3 protocol, will be considered. In particular, among such cyber-attacks, the most common are cyber-attacks on binary and analog control commands, as well as cyber-attacks aimed at disabling unsolicited messages. In view of the proposed formalization of the functioning of the CFS under the influence of MitM cyberattacks, the construction of their parameterized procedures, as well as rules for their detection, will be carried out. The resulting detection rules will form the basis of the MitM cyberattack detection system based on the use of machine learning methods.

8. References

[1] A.V. Jha, B. Appasani, A. N. Ghazali, et al. Smart grid cyber-physical systems: communication technologies, standards and challenges, Wireless Network 27 (2021) 2595–2613. doi:10.1007/s11276-021-02579-1

[2] H. Xu, W. Yu, D. Griffith and N. Golmie, A survey on industrial internet of things: A cyber-physical systems perspective. IEEE Access, *6* (2018) 78238-78259. doi: 10.1109/ACCESS.2018.2884906

[3] D. Bian, M. Kuzlu, M. Pipattanasomporn, S. Rahman, and D. Shi, Performance evaluation of communication technologies and network structure for smart grid applications. IET Communications, 13(8) (2019) 1025–1033.

[4] L. Hadjidemetriou et al., Demonstration of Man in the Middle Attack on a Feeder Power Factor Correction Unit, 2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe), The Hague, Netherlands, 2020, pp. 126-130. doi: 10.1109/ISGT-Europe47291.2020.9248779.

[5] M. K. Hasan, et al, Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations, Journal of Network and Computer Applications 209 (2023) 103540. doi: 10.1016/j.jnca.2022.103540.

[6] B. Sangewar, Dr. A. R. Buchade, Survey On Analysis Of Security Threats In DNP3 Protocol, Internation Journal of Science and Research, 9 6 (2020) 365-369

[7] C. Parian, T. Guldimann, S. Bhatia, Fooling the Master: Exploiting Weaknesses in the Modbus Protocol, Procedia Computer Science. 171 (2020) 2453-2458. doi:10.1016/j.procs.2020.04.265.

[8] G. Liang, et al., The 2015 Ukraine blackout: implications for false data injection attacks. IEEE Transactions on Power Systems. 32 4 (2016) 3317-3318. doi: 10.1109/TPWRS.2016.2631891

[9] O. Pomorova, O. Savenko, S. Lysenko, A. Kryshchuk, A.Nicheporuk, A Technique for detection of bots which are using polymorphic code, Communications in Computer and Information Science 431 (2014) 265-276.

[10] O. Savenko, S. Lysenko, A. Nicheporuk, B. Savenko, Approach for the Unknown Metamorphic Virus Detection, Proceedings of the 8-th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Bucharest Romania, September 21–23, (2017) 71–76.

[11] O. Savenko, S. Lysenko, A. Nicheporuk et al., Metamorphic Viruses’ Detection Technique Based on the Equivalent Functional Block Search, CEUR Workshop Proceedings, 1844 (2017) 555-569.

[12] O. V. Barmak, Yu. V. Krak, E. A. Manziuk, Characteristics for choice of models in the ansables classification, Problems in programming 2-3 (2018) 171-179. doi: 10.15407/pp2018.02.171.

[13] O. Barmak, I. Krak, E. Manziuk, Diversity as the basis for effective clustering-based classification, CEUR Workshop Proceedings 2711 (2020) 53-67.

[14] I. Darwish, O. Igbe, T. Saadawi, Experimental and Theoretical Modeling of DNP3 Attacks in Smart Grids, 2015 36th IEEE Sarnoff Symposium, Newark, NJ, USA, 2015, pp. 155-160, doi: 10.1109/SARNOF.2015.7324661

[15] T.R. de Toledo, N. M. Torrisi, Encrypted DNP3 Traffic Classification Using Supervised Machine Learning Algorithms. Machine Learning and Knowledge Extraction 1(1) (2019) 384-399. doi:10.3390/make1010022

[16] F. Mercaldo, F. Martinelli, A. Santone, Real-Time SCADA Attack Detection by means of Formal Methods, 2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Napoli, Italy, 2019. doi: 10.1109/WETICE.2019.00057

[17] H. Tong, J. Xu, X. Li, L. Zhang Cyber-attack research for integrated energy systems by the correlated matrix based object-oriented modeling method, Frontiers in Energy Research, 10 (2022) doi: 10.3389/fenrg.2022.774645

[18] E.-M. Kalogeraki, S. Papastergiou, T. Panayiotopoulos, An Attack Simulation and Evidence Chains Generation Model for Critical Information Infrastructures, Electronics 11 404 (2022). doi:10.3390/electronics11030404

[19] F. Moazeni,J. Khazaei, MINLP Modeling for Detection of SCADA Cyberattacks in Water Distribution Systems, World Environmental and Water Resources Congress 2020, Henderson, Nevada, 2020. doi: 10.1061/9780784482971.033

[20] H. He, J. Yan Cyber-physical attacks and defences in the smart grid: a survey. IET Cyber-Physical Systems: Theory Applications, *1*(1) (2016) 13–27.

[21] X-G. Zhang, G-H. Yang, S. Wasly, Man-in-the-middle attack against cyber-physical systems under random access protocol, Information Sciences 576 (2021) 708-724. doi: 10.1016/j.ins.2021.07.083

[22] Wlazlo, P., et al., Man-in-the-middle attacks and defence in a power system cyber-physical testbed, IET Cyber-Physical Systems: Theory & Applications, 6(3) (2021) 164–177. doi: 10.1049/cps2.12014

[23] xMasterSlave, URL: http://xmasterslave.tgscada.com/

[24] J. Bai, S. Hariri and Y. Al-Nashif, A Network Protection Framework for DNP3 Over TCP/IP Protocol, 2014 IEEE/ACS 11th International Conference on Computer Systems and Applications (AICCSA), Doha, Qatar, 2014, pp. 9-15, doi: 10.1109/AICCSA.2014.7073172.

[25] Tcpdump/Libpcap public repository, URL: http://www.tcpdump.org/