UDC 004.056

Probabilities estimating for attacks on supply chain for critical infrastructure facilities

Mykola Ilin[1], Oleksandr Rybak[2], and Iryna Stopochkina[3]

1,2,3 National Technical University of Ukraine "Ighor Sikorsky KPI", Beresteyskyi ave., 37, Kyiv, 03056 Ukraine

Abstract

The different types of supply chain for critical infrastructure facilities of industrial sector were analyzed. Also, the main types of attacks in supply chain were considered.

The character of resource dependencies was analysed and representation of supply chain in form of hierarchical oriented graph, with division into levels, was considered. The algorithm of taking into account of attack probabilities for objects, which give resources for functioning of some endpoint object of supply chain was developed basing on dynamic programming principles. Calculation complexity of proposed algorithm was estimated, and it confirmed its effectiveness for practical situations. For the target area of use the proposed approach gives better calculation complexity in compare existing solutions.

Keywords: Supply Chain, Cyber Attack Probabilities, Critical Infrastructure

Introduction

The cyberattack problems for supply chain are relevant direction of investigation.

Popular practices, mainly, are oriented to security support of supply chain elements, and reinforcement of means of cyberprotection [1].

For the study of resource relations of industrial objects, frameworks have been developed that allow the visualization of existing relations using the apparatus of graphs [2]. The assessment of cyber security risks, and especially, probabilities of the supply chain attacks remains interesting problem for this situation.

A number of existing solutions contain general methodological recommendations (for example, on asset valuation, staff training and security settings) [3,4]. Not a lot of attention is paid to the assessment of the probability of the occurrence of undesirable events in supply chain, mainly an expert qualitative assessment is recommended. In [5] the different possible approaches of risk assessment are highlighted, that shows different ways of its calculation.

In the presence of powerful event registration systems, a quantitative assessment is also possible by calculating statistical indicators of the occurrence of undesirable events on the links of the chain. This enables the introduction of quantitative methods of calculation that will enable the calculation of the probability of occurrence of undesirable events due to damage to the supply chain for selected key facilities.

On the other hand, there are a number of models for working with phenomena that can be represented in the form of graphs or networks. Among them, we should mention models in the form of Bayesian networks [6], which are used to model causal relationships. Among the difficulties that arise here is the need to train the network, in particular using machine learning approaches. In a simpler version, the network is set by a specialist based on preliminary calculations, which may include subjective factors. Both options involve practical complexity of implementation.

There are number of works, which use models in the form of graphs. For example, attack trees [7], which take into account the availability of defenses and security policy constraints. Taking into account a detailed list of means and protection measures makes the model impractical for use, due to the computational complexity of working with it. Insufficiently detailed consideration of network operation conditions can lead to a loss of model adequacy. In works [8,9]

the graph-based risk assessment approach is considered, that approves usability graph method for prognostic and simulation needs in risk management.

Another option is models based on the logical-probabilistic approach [10]. Among the features inherent in these models is the need for a detailed analysis of the characteristics of the object under study, the formation of a Boolean formula that reproduces the patterns of attack propagation. These data cannot always be realistically predicted at each specific research object. Models of this kind involve the stage of reduction to perfect disjunctive normal form, which complicates the process and is not justified for problems where strict mathematical proof is not required. Therefore, the use of such models is more appropriate in the tasks of optimization, construction of optimal protected networks, taking into account certain restrictions, than for current risk assessments of supply chains, which must be carried out in a working order.

Existing algorithms and methods involve significant computational complexity. For small graphs, with the number of vertices 10-15, the problem does not arise acutely. However, already with 40-50 vertices, there is a need to look for more computationally efficient ways. In particular, the opportunity may be to use knowledge about the structure of the graph.

This work presents an approach focused on the types of graphs typical for supply chains of critical infrastructure objects of an industrial type, which is a compromise between business-oriented models that weakly take into account probabilistic dependencies between objects and processes, and mathematical models that are difficult to apply to a real case. We are basing on results of [11,12] works to identificate supply chain operation processes and links. The approach is based on the practice of taking into account expert opinion and questionnaires to obtain reputational parameters of organizations and objects that are resource providers for the analyzed subsystem [3], combined with the use of a dynamic programming approach to take into account probabilistic dependencies.

1. Supply chain risk assessment: existing standards and frameworks

The NIST SP 800-37 Risk Framework provides general guidance on the security risk assessment process. It defines the main stages of the organizational and methodological plan for risk assessment. The training plan involves the identification of key roles, the identification of organizational risks, and the appointment of continuous monitoring tools to identify risks. Next, there is a stage of categorization, including in terms of the impact of events on organizational processes, loss of integrity, confidentiality, availability. At the next stage, decisions are made regarding security controls to protect the identified risks of various categories. Ultimately, these controls must be implemented and their effectiveness evaluated. Next, the framework recommends processes for keeping risk assessments and response tools up to date. So, we can see that this framework provides guidelines of a purely organizational nature for security professionals.

The ISO 31000:2018 Risk Management standard is devoted to the general principles of risk management. It provides guidance on activities that can contribute to the effective implementation of risk management – therefore, it is more useful for managers involved in incident handling and efforts to secure a facility.

The Control Objectives for Information and Related Technologies (COBIT®) 2019 framework recommends focusing the risk assessment and management process on stakeholder needs and a dynamic study of factors that contribute to risk. Special importance is attached to an effective management system.

The NIST Cybersecurity Framework (CSF) for organizations contains basic categories for supply chain risks. It is interconnected with the recommendations of the more thorough NIST SP 800-161 Cybersecurity Supply Chain Risk Management.

NIST 800-161 “Cybersecurity Supply Chain Risk Management for Systems and Organizations” provides detailed guidance on the organization of supply chain risk assessment and management, recommendations on how to influence supply chain risks. This document can be quite useful for identifying assets at risk, sources of threats, and controls for the reliability of the supply chain. Again, recommendations for quantitative calculations are not provided here.

The product of MITRE (ATT&CK®) includes the System of Trust (SoT) framework, which can be useful for the implementation of methods of identification and assessment of risks related to the supply chain. Categories of suppliers, products and services are considered. A classification and model for collecting

information about the supplier, products, services and relevant risks has been developed. This framework can be quite useful for practical evaluation, however, cause-and-effect interdependencies between events are hardly taken into account here.

The ISO/IEC 27036 Information Security for Supplier Relationships standard can help ensure secure relationships between suppliers and the facility, and it can be used to form risk assessment methodologies, as it contains requirements and guidelines for software, hardware, and service delivery technologies. (computing, cloud, etc.) and other resources.

Since the supply chain includes supplier organizations that are a source of risks, it should be remembered that there are risk assessment techniques for different suppliers, and companies that perform such assessments in advance, based on the maturity level of the supplier organization, assessments of the overall level of cyber security, etc. Therefore, in our work, we believe that such an assessment of supplier organizations has been completed, and the level of trust, or even the risk indicators for the supplier, are known.

Such evaluations of suppliers for determining the level of cyber security are carried out using existing methodologies that rely on questionnaires. Answers must be supported by evidence. Such methods include CISA ICT SCRM Task Force, CISA NRMC, North American Transmission Forum (NATF) Supply Chain Security Assessment Model, Idaho National Laboratory—Cyber Security Evaluation Tool (CSET) and others.

2. Supply chain types

A supply chain is an interconnected infrastructure of relationships and processes between organizations and their personnel in the development, distribution, and sale of products, services, or resources. In our case, the end user of services and products is a critical infrastructure facility, or more specifically, its subsystems. To emphasize the different roles of subsystems, we rely on the concept of the automation pyramid, which can contain 5 different levels: ERP, MES, SCADA, PLC and smart devices of the Internet of Things, and the physical level [11,12]. Accordingly, each of these levels consumes some resources that may be subject to cyberattacks. In particular, the software that is implemented at a critical infrastructure facility may be infected with malware.

Reference [11] describes the possible variants of supply chains. Let's analyze them and identify those that may be vulnerable to cyber attacks, and give them in graph representation.

In general, a supply chain in the traditional sense is a sequence of resource links such as: raw material supplier → manufacturer → distributor (delivery) → seller → consumer. In our case, we will focus on the end user, which is an industrial-type critical infrastructure facility.

Considering the options of supply chains vulnerable to cyber attacks, we assume that the supplier of raw materials is not sensitive to cyber attacks, so we exclude this link from consideration.

The producer (P) can be understood as:

1. Software product companies - suppliers of off-the-shelf software for the needs of critical infrastructure facilities, P1;
2. Software outsourcing companies - developers of custom software, P2;
3. Manufactures that produce parts of software and hardware that have the ability to memorize and perform intelligent functions: chips, smart cards, magnetic tapes, microcircuits, etc., P3;
4. Manufactures that produce complete software and hardware devices or assemble such devices from parts supplied by manufacturers from item 3, P4.

These types of producers are sensitive to cyber impacts, and among other production risks, they have the risk of cyber attacks.

Distributor (D) is defined as:

1. Channels for obtaining software that is in the public domain and can be obtained through the network, D1;
2. Distribution companies that deliver software and hardware and/or software media, D2.

Seller (R) may be:

1. Intermediaries from among the companies that purchase the rights to distribute software or hardware from the manufacturer P, R1;
2. The companies producing P themselves, R2.
3. Companies that provide software and hardware implementation and maintenance services, as well as security providers, R3.

In view of the above, the supply chain may look like shown in fig. 1.

Meaningful supply chains, which can be compiled based on integrated assessments of trust in supplier companies. Such chains may consist of levels R1-R4.

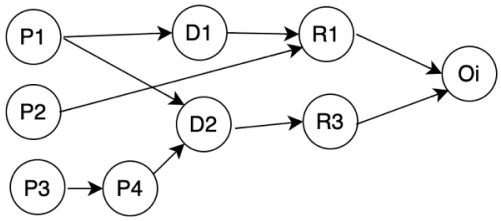

Figure 1: Supply chain graph for Producer-Distributor-Seller-Object

Supply risks, R1:

- Risks of intrusion by an intruder (intruder in the middle) R11
- Unintentional risks (accidental substitution, cyber hygiene risks, workflow organization) R12
- Financial stability and financial investment in cybersecurity, R13;

Risks of suppliers R2:

- Organizational security risks affecting the quality and integrity of supply, R21;
- Supplier vulnerability risks R22 (staff competence, lack of insiders);
- Risks of external influences, R23;
- Product quality risks. Here, we do not consider those risks that affect the delivery time of software or hardware, but only its security, quality, and the presence of vulnerabilities, R24.

Service risks, R3:

- Quality of service risks (correctness of administration, software and hardware security settings), R31;
- Risks of resilience of the implemented architecture to external influences (e.g., denial of service, loss of information, loss of visibility), R32;

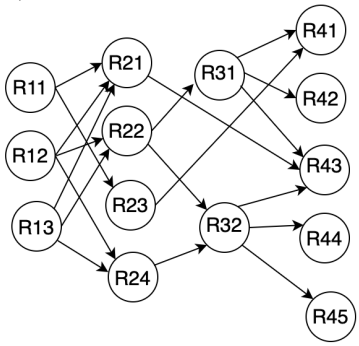

Figure 2: Graph according to MITRE System of Trust risk categories

R4 security risks for the critical infrastructure facility:

- unauthorized access, R41,
- confidentiality, R42,
- integrity, R43,
- availability, R44,
- observability R45.

Information supply risks at the critical infrastructure facility level that affect the integrity, observability, and availability of the network can be divided into:

RWL wireless communication risks:

- risks of failures/malicious interference of long-range radio communication channels (LoRa, etc.), RWL1;
- risks of failure/malicious interference of wireless access points, signal amplifiers, other communication devices, RWL2;
- Risks of short-range wireless communication channels (Wi-Fi, Bluetooth) failures/malicious interference, RWL3;

Risks of failures in the IoT network RN:

- Risks of failure/malicious interference for fog-level devices (PLCs, single-board computers, servers, etc.), RN1;
- RN2: risks of failure/malicious interference for end devices (sensors, detectors, cameras, etc.);

Risks of wired communication, RW:

- Risks of failure/malicious interference for access channels operating on fiber optic technologies, RW1;
- Risks of failure/malicious interference for access channels operating on wired technologies, RW2;
- Risks of flaws and attacks on communication protocols used in communication, RW3.

Risks in the supply of power to end and intermediate devices, RE:

- risks of delivery to devices with built-in batteries, RE1;
- risks of delivery to devices equipped with batteries, RE2;
- risks of supplying devices that are not equipped with batteries or batteries, RE3.

In this case, the graph for calculating risks for a particular object (for example, for fog-level devices) will depend on the topology of the network through which communication is carried out. But it will also have a hierarchical structure. For example, as shown in fig.3

Signals from remote IoT devices are transmitted via a wireless data transfer protocol to the Switch inside the critical infrastructure facility, which is connected by a wired line to an access point that operates both in wireless mode

and in the wireless mode to receive signals via wireless protocols from IoT devices inside the critical infrastructure facility. The information is then transmitted via wired communication channels to the control device (server, controller, single-board computer). The switch and other communication devices are powered by the power grid, while the fog level device has batteries. The "supply" graph for such a control device will look like this (fig.4)

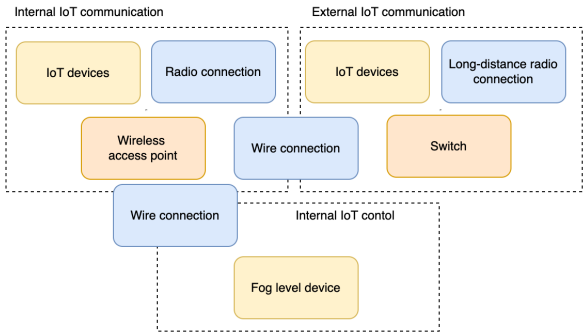

Figure 3: Interaction of external and internal IT devices with the control device

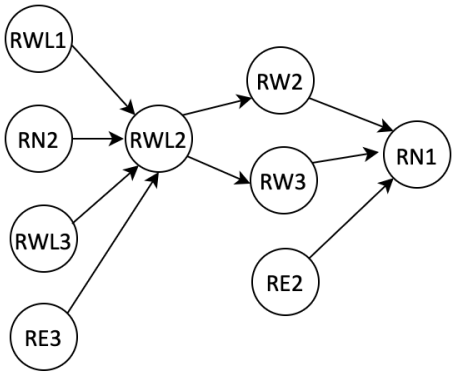

Figure 4: Supply graph for control device

We assume that the risks of a cyberattack have already been calculated for each vendor. However, if this is not the case, the following considerations can be used.

The security risks of the CI/CD chain can be categorized as:

RD development risks:

- Code security, RD1;
- Architecture security, RD2;
- Risks of identifying vulnerabilities and threats to the code, RD3.

Risks of current testing RT:

- Risks of automated code security testing, RT1;
- Risks of code review, RT2;
- Risks of static analysis of SAST code, RT3;
- Risks of the repository, RT4.

Risks of the Preproduction RPP stage:

- Risks of dynamic analysis of DAST, RPP1;
- Risks of interactive analysis IAST, RPP2;
- Risks of fuzzing, RPP3;
- Risks of hybrid analysis, RPP4;
- Risks of penetration testing, RPP5.

Risks of the final stage of Production are denoted by RP.

Then the structure of the supply chain graph for this case will be shown in fig.5.

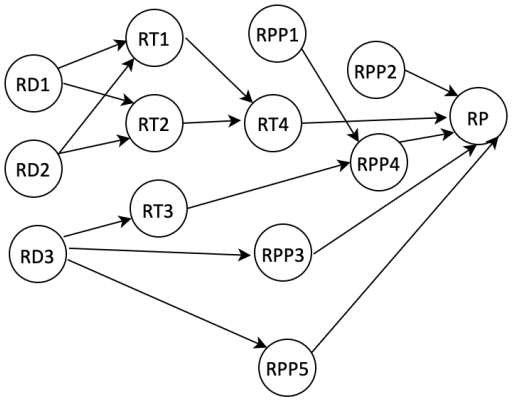

Figure 5: Supply chain for software production

If we have intension to work with supply chain for manufacturing, we should take into account following items, which concern programmable hardware:

1. Manufacturing of OT equipment, OE.
2. Production of firmware and embedded software, FE.
3. Production of smart devices, SD.
4. Packaging of production, P.
5. Logisticts of production, L.
6. Integration into subsystem of critical infrastructure facility, I.

The supply graph is shown in the fig. 6.

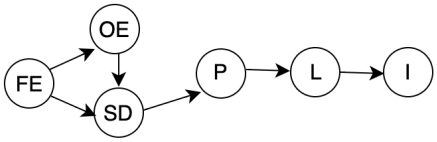

Figure 6: Supply chain for hardware support

3. Method for calculating the probability of a successful cyberattack on the supply chain

3.1. General idea and background

Analyzing the appearance of supply chain graphs (fig. 1-6), we can conclude that resource links in the supply chain can be represented as an oriented graph, the vertices of which represent resource-source objects, and the arcs of which are the directions of resource supply to the following objects. The graph does not contain cycles in its structure.

Every vertex v_i is related with probability p_i of successful attack for the object.

To be specific, let's make the following assumptions:

1) If vertex v_i has no connections, it can be successfully attacked with p_i probability.

2) If vertex v_i has connections, that is, respective object is resource-dependent on others in the supply chain, and can be successfully attacked with probability p_i, provided that at least one of the objects on which v_i depends is successfully attacked. Otherwise, we assume that object v_i is not under attack.

Let's calculate the probability of attacking a certain object v_k, given the data on the resource links to provide it and the corresponding probabilities of attacks at different links (vertices) of the supply chain. For convenience, we will consider vertex v_k to be the final vertex in the graph, i.e., the one from which no arcs come out.

The concept of solution.

Let's divide the graph into "levels". We will assume that arcs can only go from level s to level $s+1$. If this is not the case, then we simply introduce intermediate vertices with a probability of a successful attack p_i=1 (see fig. 7). We assume that the graph does not contain oriented cycles.

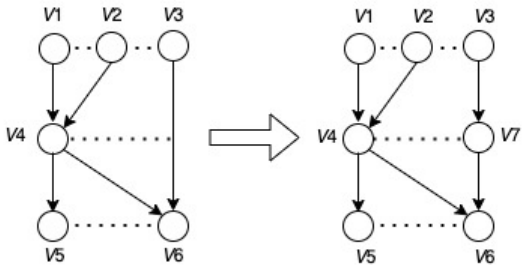

Figure 7: Splitting the graph into levels

According to the topological sorting theorem, such a graph can always be divided into levels in such a way that the direction of the arcs is strictly ascending (fig.8).

Let's perform dynamic programming on the levels from top to bottom (from the first level). For each level, we calculate the probability that this particular subset of vertices will be captured.

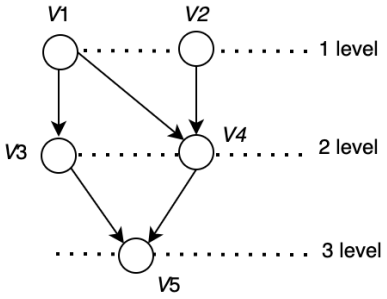

Figure 8: Supply chain graph, splitted into levels

Example. Suppose that the graph is of the form shown in fig. 8.

Then the probabilities of an attack at the first level are as follows:

$\{v_1, v_2\}: p_1p_2$, $\{v_1\}: p_1(1-p_2)$; $\{v_2\}: p_2(1-p_1)$;

$\emptyset: (1-p_1)(1-p_2)$.

Let's calculate for the second level. If a successful attack is carried out on the first level for v_1, v_2, then the probabilities are constructed in the same way:

$\{v_3, v_4\}: p_3p_4$, $\{v_3\}: p_3(1-p_4)$; $\{v_4\}: p_4(1-p_3)$;

$\emptyset: (1-p_3)(1-p_4)$.

All cases are presented in table 1.

Each cell of Table 1 shows the probability that a subset of level 2 will be attacked if a certain subset of level 1 is attacked. The empty set corresponds to the case when none of the node objects were successfully attacked, and we calculate the probability of this event.

As result we have:

$p(\{v_3; v_4\}) = \big(p_1p_2 + p_1(1-p_2)\big)p_3p_4 = p_1p_3p_4$;

$p(\{v_3\}) = \big(p_1p_2 + p_1(1-p_2)\big)p_3(1-p_4) = p_1p_3(1-p_4)$;

$p(\{v_4\}) = \big(p_1p_2 + p_1(1-p_2)\big)(1-p_3)p_4 + (1-p_1)p_2p_4 =$

$= p_1(1-p_3)p_4 + (1-p_1)p_2p_4$;

$p(\{\emptyset\}) = \big(p_1p_2 + p_1(1-p_2)\big)(1-p_3)(1-p_4) + (1-p_1)p_2(1-p_4) +$

$+(1-p_1)(1-p_2)\cdot 1 = p_1(1-p_3)(1-p_4) + (1-p_1)p_2(1-p_4) + (1-p_1)(1-p_2)$.

Similarly, let's calculate the probability of attack v_5 based on the data obtained:

$$p(\{v_5\}) = p_5(p(\{v_3; v_4\}) + p(\{v_3\}) + p(\{v_4\})) =$$
$$= p_5(p_1p_2p_4 + p_1p_3(1-p_4) + p_1(1-p_3)p_4 + (1-p_1)p_2p_4) =$$
$$= p_5(p_1p_3 + p_1(1-p_3)p_4 + (1-p_1)p_2p_4).$$

These ratios are obtained under the assumption that we consider only the probability of "propagation" of attacks committed at nodes v_1, v_2. We assume that the following nodes are insensitive to other attacks. However, the attacks that were previously carried out in them can be stopped.

Example.

Consider the resource connections shown in fig. 9, which describes situation from fig.10.

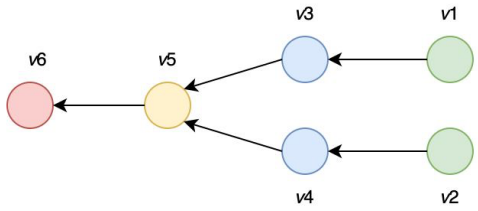

Figure 9: Resource links graph

For such a graph, the result will be represented by

$$p(\{v_6\}) = p_5p_6(p_1p_3 + p_2p_4 - p_1p_2p_3p_4).$$

Let's say that based on the analysis of suppliers, support services, and distributors, as well as the maturity of organizational security processes at the facility itself, the following probabilities were established:

$p_1 = 0{,}1$ (that is, one out of 10 attacks on the introduction of undocumented functions into software is successful),

$p_2 = 0{,}01$ (that is, 1 out of 100 attacks on the introduction of undocumented functions into the device will be successful, due to the higher level of security of the development technological complex than that of a software company).

$p_3 = 0.99$ - the likelihood that the harmful effects from the previous stage will not be stopped (for example, the software is distributed through specialized websites - which are unlikely to detect undocumented functions introduced at the development stage).

$p_4 = 0.999$ - since only 1 device out of 1000 is tested during the distribution and support of hardware.

$p_5 = 0.5$ (half of the attacks can be missed by means of control, testing in a virtual environment and diagnostics applied to all types of hardware and software supplied to the facility),

$p_6 = 0.99$ (only 1 in 100 cases of attacks can be prevented by proper configuration and implementation features).

Then, $p(\{v_6\}) \approx 0.05$ – that is, 5 out of 100 attacks will be successful. This is quite a high rate for a critical infrastructure facility.

Next, let's move up a level.

Let's assume that attacks can be introduced in nodes v_3, v_4. That is, the software distribution service will replace the correct sample with a malicious one.

Or, during the transportation and distribution of a complete hardware sample, it will be replaced with one that has malicious functions.

In this case, the probabilities will depend on the reliability of the software integrity controls (reliable digital signature of the manufacturer) and hardware (physical packaging that cannot be tampered with, batch labeling, etc.)

Suppose the probabilities are:

$p_3 = 0.00001$ – That is, only 1 out of 100,000 attacks on a strong signature will be successful.

$p_4 = 0.0001$ – only one out of 10,000 attacks to spoof physical features can be successful.

The probabilities for the vertices of the first layer in this case are $p_1 = 0$ та $p_2 = 0$.

$p_5 = 0.99$ – controls will detect only 1 out of 100 such attacks.

$p_6 = 0.99$ – facility security systems will detect and stop only 1 out of 100 malicious injections inside the implemented software and hardware.

Then, the formula is transformed into the following

$$p(\{v_6\}) = p_5p_6(p_5p_3 + p_5p_4).$$

The result of the calculations for p_i above is $p(\{v_6\}) = 0.0001$. This result emphasizes that the bulk of malicious interference in the supply chain can occur at the endpoints, i.e., where hardware or software is produced. At the stages of delivery of finished software and hardware, this probability is much lower, although it cannot be neglected.

Thus, we will calculate the probabilities of attacks on different levels of the supply chain. Accordingly, we will calculate the risks if we establish the value of assets potentially damaged by such attacks at the facility. The number and type of such cyber-physical attacks can be quite limited, mainly malicious intrusions and substitution of supplied resources.

As for a successful attack on one of the subsystems of the facility (ERP, MES, SCADA, PLC, physical), we believe that it is possible only if at least one of the nodes that has resource connections to this one is captured.

3.2. Solution algorithm and estimate of its complexity

Suppose a graph has v vertices, and each layer contains $a_1, a_2, \dots, a_k$ vertices, respectively $a_1 + a_2 + \dots + a_k = v$. We show that if there are c and d vertices in the neighboring layers, respectively, we can make a transition from the first layer to the second layer in $O(2^c \cdot 2^d)$ operations. We assume that before the transition is performed, we know the probabilities that all vertices of some subset u of the upper layer will be attacked, while the other vertices of this layer will not be captured by the attacker (see fig.11). This information is given for each subset U in the upper layer. We need to compute the same for each subset V in the lower layer. We may have 2^c options for U and 2^d for V. Therefore, we need to make a calculation scheme such that the average number of operations for pairs (U, V) is finite and depends on c and d.

For each pair (U, V), we essentially perform the following action:

1) If every vertex of V can be reached from some vertex of U , then we add to the probability $p(V)$ the term $p(U)\prod_{v\epsilon V} p_v \prod_{v\epsilon D(u)/V}(1-p_v)$;
2) If the condition in Section 1 does not hold, we do not change $p(V)$,, since in this case a successful attack on the entire set is impossible.

Here, we use the following notation $p(U)$ is the probability that the set U and only it will be captured in layer C, $p(V)$ is the probability that the set V and only it will be captured in layer D $D(U)$ is the set of vertices in layer D to which an edge from at least one vertex of the set U, p_v – given initial probability of successful attack on vertex v, if at least one edge from the previously captured vertex leads to it.

Checking whether you need to select the option 1) or 2), can take $O(c \cdot d)$ operations, because there are from 0 to cd edges between C and D layers.

But we can perform our algorithm for middle number of actions by all (U, V) pairs to be estimated as $O(1)$.

Let us use following approach:

1. Calculate set $D(U)$ previously for separately considered U. This task will be solved inductively. Let $D(U)$ is found for all U, which consists of $u_1, u_2, \dots, u_m$. Suppose, we considered one more vertex $u_{m+1}\epsilon C$.
2. If certain U doesn't contain u_{m+1} , we have already found before.
3. If $u_{m+1}\epsilon\, U$ then $U = WU\{u_{m+1}\}$, where $W \subseteq \{u_1, u_2, \dots, u_m\}$, then we have $D(U) = D(W) \cup D(\{u_{m+1}\})$. $D(W)$ has been already known, so the calculation takes O(d) operations.

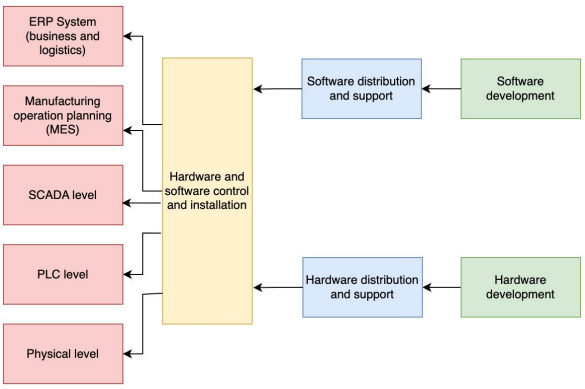

Figure 10: View of resource links for critical infrastructure facility subsystems

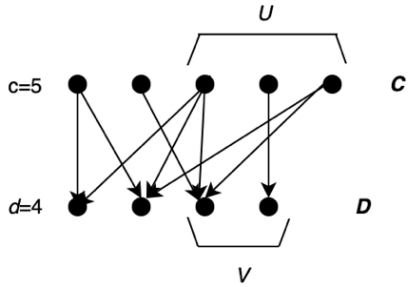

Figure 11: *U* , *V* , *c,* and *d* illustration

Table 1: Probabilities of attacks on subsets of level 2, provided that subsets of level 1 are attacked

1st level / 2nd level	$\{v_1, v_2\}$	$\{v_1\}$	$\{v_2\}$	$\emptyset$
$\{v_3, v_4\}$	$p_3 p_4$	$p_3 p_4$	0	0
$\{v_3\}$	$p_3(1-p_4)$	$p_3(1-p_4)$	0*	0
$\{v_4\}$	$p_4(1-p_3)$	$p_4(1-p_3)$	p_4	0
$\emptyset$	$(1-p_3)(1-p_4)$	$(1-p_3)(1-p_4)$	$(1-p_4)$	1

*For example, if $\{v_3\}$ is attacked (without v_1) – it is impossible to attack v_3, so that cell contains 0. Next, we sum the rows taking into account probabilities for conditions $\{v_1, v_2\}$, $\{v_1\}$, $\{v_2\}$, and $\emptyset$.

In general we have 2^c number of U sets, and $O(d)$ operations for each set. This leads to $O(2^c \cdot d)$ estimate.

Whereas $\leq 2^d$, we can assess complexity of finding of all $D(U)$ (for all $U \epsilon C$) as $O(2^c \cdot 2^d)$.

It is convenient to consider only V: $V \subseteq D(U)$ for every U. The number of such U is $2^{|D(U)|} \leq 2^d$. It means that we sort out $O(2^c \cdot 2^d)$ pares of (U, V).

Using this technique, we can calculate $\prod_{v \epsilon V} p_v$ and $\prod_{v \epsilon S}(1-p_v)$ for all $V, S \subseteq D$. Namely, let us apply formula:

$$\prod_{v \epsilon V} p_v = \left(\prod_{v \epsilon W} p_v \right) p_{v_{m+1}},$$

If $V = W \cup \{v_{m+1}\}$.

Similarly, for

$$\prod_{v \epsilon S}(1-p_v).$$

Therefore, calculation of such products requires $O(2^d)$ operations, that can be estimated as $O(2^c \cdot 2^d)$ also.

So, we have proved that it is possible to modify algorithm in such way to supply the estimate in

$O(2^c \cdot 2^d)$ operations for transition between layers.

In our assumption we have

$$O(2^{a_1} \cdot 2^{a_2} + 2^{a_2} \cdot 2^{a_3} + \cdots + 2^{a_{k-1}} \cdot 2^{a_k})$$

operations, where
$a_1 + a_2 + \ldots + a_k = v$ and $a_1, a_2, \ldots, a_k \geq 1$.

Let us demonstrate that

$$2^{a_1} \cdot 2^{a_2} + 2^{a_2} \cdot 2^{a_3} + \cdots + 2^{a_{k-1}} \cdot 2^{a_k} \leq 2^v.$$

Define $s_1 = 2^{a_1}, s_2 = 2^{a_2}, \ldots, s_k = 2^{a_k}$.

Note that $s_1 s_2 \ldots s_k = 2^v$ and $s_1 s_2 \ldots s_k \geq 2$.

Let us show that $s_1 s_2 + s_2 s_3 \leq s_1 s_2 s_3$.

Having $s_1 s_2 \geq 2$, the sum can be reorganized in following way:

$$s_1 s_2 + s_2 s_3 + \cdots + s_{k-1} s_k \leq$$
$$s_1 s_2 s_3 + s_3 s_4 + \cdots + s_{k-1} s_k \leq$$
$$\leq s_1 s_2 s_3 s_4 + \cdots + s_{k-1} s_k \leq \cdots \leq s_1 s_2 \ldots s_k$$
$$= 2^v.$$

It means algorithm requires $O(2^v)$ operations.

In particular we have better profit, when $a_1 + a_2 + \ldots + a_k = f$, де $f \ll v$. Such situation is often noticed in supply chain graphs. Then $2^{a_i} \cdot 2^{a_{i+1}} \leq 2^f \cdot 2^f = 4^f$. And, the algorithm complexity estimate is $O(4^f \cdot v/f)$ operations.

Conclusions

A study of the type of supply chain graphs for critical infrastructure facilities has shown that the specificity of the links allows us to improve existing approaches to risk estimation and calculation of general attacks probabilities, which lead to NP-complete class of algorithms. The approach proposed in this paper has particular benefits when sum of supply chain graph vertices $a_1 + a_2 + \ldots + a_k = f$, where $f \ll v$. Then algoritm complexity estimate is $O(4^f \cdot v/f)$ operations, that gives good results for supply chain typical graph structure.

The proposed solution can be useful for risk analytics and precise risk management.

References

[1] Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry. URL: https://www.cisa.gov/sites/default/files/2023-01/eo14017-supply-chain-fact-sheet.pdf .

[2] Why supply chain management and graph technology are a perfect match. URL: https://linkurious.com/blog/supply-chain-graph/.

[3] Information and communications technology supply chain risk management task force report. 2020. URL: https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force_year-two-report_508.pdf.

[4] Supply Chain Security Assessment Model. URL: https://www.natf.net/docs/natfnetlibraries/documents/resources/supply-chain/supply-chain-security-assessment-model.pdf

[5] В. І. Полуциганова, С. А. Смирнов. Класифікація моделей ризиків у складних кіберсистемах // Матеріали XXII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених. Київ : КПІ ім. Ігоря Сікорського, Видавництво «Політехніка», 2024. С. 163-165. URL: http://conf.ipt.kpi.ua/2022/06/13/%d0%ba%d0%be%d0%bd%d1%84%d0%b5%d1%80%d0%b5%d0%bd%d1%86%d1%96%d1%8f-2022/

[6] Л.Б. Левенчук, В.Г. Гуськова, П.І. Бідюк. Ймовірнісне моделювання операційних ризиків// KPI Science News, 2021/3. P. 26-37. doi: 10.20535/kpisn.2021.3.251681

[7] C.-W. Ten, C.-C. Liu, M. Govindarasu. Vulnerability Assessment of Cybersecurity for SCADA Systems Using Attack Trees. doi: 10.1109/PES.2007.385876

[8] E. Wasik et al. Supporting Supply Chain Risk Management: An Innovative Approach Using Graph Theory and Forecasting Algorithms// European Research Studies Journal, Vol.XXVII, Spec.Issue 2, 2024. P.25-37.

[9] L.A. Shah, A. Etienne, A. Siadat, F.B. Vernadat. Value-Risk Graph: A decision-making tool for supply chain and industrial system engineering // 6th IFAC Conference on Management and Control of Production and Logistics. IFAC, September 11-13, 2013. Fortaleza, Brazil. P.414-419.

[10] L.Alekseichuk, O.Novikov, A.Rodionov, D.Yakobchuk. The Best Scenario of Cyber Attack Selecting on the Information and Communication System Based on the Logical and Probabilistic Method. // Theoretical and Applied Cyber Security, Vol. 5 No. 2 (2023). P.81-88. DOI: doi: 10.20535/tacs.2664-29132023.2.288973

[11] C. Crossley. Software Supply Chain Security. Securing the End-to-End Supply Chain for Software, Firmware, and Hardware. 2024, O`Reilly Media, Inc.

[12] Chen-Ching Liu, Cyber Security of SCADA, Substations, and Distribution Systems. URL: https://mpr-production-assets.s3.amazonaws.com/media/documents/Presentation1_CCLiu_Cyber_Physical_System_Security_of_a_Power_Grid.pdf