A model of Cyber Threat Information Sharing with the Novel Network Topology

A model of Cyber Threat Information Sharing

Jari Hautamäki
School of Technology, JAMK University of Applied Sciences, jari.hautamaki@jamk.fi
Timo Hämäläinen
IT Faculty, University of Jyvaskyla, timo.t.hamalainen@jyu.fi

The digitized environments are particularly vulnerable to various attacks. In such a situation of a security attack, detecting and responding to attacks require effective actions. One of the most significant ways to improve resilience to security attacks is to obtain accurate and timely situational aspect of the security awareness. The efficient production and utilization of situation information is achieved by sharing information with other actors in the information sharing network quickly and reliably without compromising the confidential information of one's own organization. At the same time, it should also be possible to avoid a flood of irrelevant information in the sharing network, which wastes resources and slows down the implementation of security measures. In our study, we have investigated how security-related information can be shared online as efficiently as possible by building a security information sharing topology based on the two most widely used network optimization algorithms. In the article, we present a model of an information sharing network, in which three different parameters have been used to optimize the network topology: the activity level of organization, the similarity of information systems between different actors and the requirement for the level of information privacy generally in the organization.

CCS CONCEPTS • Security and privacy • Networks • Computer systems organization

Additional Keywords and Phrases: Cyber security, Situation Awareness, Security Information Sharing

1 Introduction

In today's society, almost all services are based on data networks and networked information systems. Through the development brought about by digitalization, more and more services are connected to networks. As the volume of data transmission increases rapidly, reliability will play an increasingly important role [1].

In general, it can be observed that the number of security attacks is constantly increasing [2]. The impact of attacks on the security of individuals and the business of organizations is constantly growing worldwide. Attack methods are constantly evolving and diversifying. Knowledge of the methods of attack and the identification of threats are of paramount importance to those actors responsible for combating threats. Sharing information on attack methods and defenses against cyber security plays an important role in the fight against cyber security crime [3]. Information about the attack and defense methods provided by an individual actor provides other actors with an effective way to defend themselves against cyber attacks.

A key prerequisite for information sharing is how actors can share information quickly, accurately, and without compromising their own operations by disclosing information about attacks.

In a cybersecurity breach situation, it is important to understand how the situation will affect the organization's assets and business. This feature is commonly referred to as Cyber Situational Awareness (SA) [4]. Depending on the actor, SA is understood in many different ways.

According to Endsley's definition, "Situational awareness is the perception of the elements of the environment in time and space, understanding their significance, and reflecting space in the near future". Endsley describes situation awareness from an individual person's point of view, where situational awareness consists of three different levels: perception, comprehension, and projection. [5]

Situational awareness is always a personal and unique view of a particular situation, and personal situational awareness cannot be fully shared with any other person. Figure 1. below shows how situational awareness leads to an individual resolution making. [6]

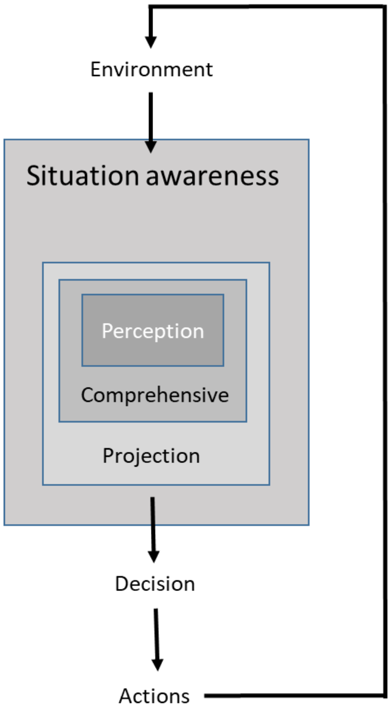

Figure 1: Situational awareness (6)

It is obvious that up to date and timely SA produces efficiency to decision-making. SA depends on the person's character, education and competence in how they react to some specific events and phenomena. [5, 6, 7]. SA emerges from the process of getting relevant information from the organization itself, integrating it into usable knowledge about the present situation and disseminating it again to the people who need it to make the right decisions. [8]

In Finland's cyber security strategy, cyber security is understood as a state in which the cyber operating environment can be trusted, and its operations secured. The cyber operating environment, on the other hand, can be understood in the same way as the digital operating environment, which is rapidly evolving as a part of society and as a service. The SA focused on cybersecurity enables the right measures to be taken to secure an organization's ability to respond to cyber security threats. SA can be used to ensure the continuity of an organization's business more effectively. Finland's Cyber Security Strategy 2019 launches the preparation of a national cyber security development program. The program aims to improve the national SA and link planning to other activities more clearly. [9]

It is extremely important to get correct SA from your own organization's cyber security environment by identifying potential security risk topics. Cyber security situational awareness can be applied by monitoring and analyzing techniques and using situational awareness from short-term operational decision making to long-term strategic decision making. [10]

Maintaining and continuously developing cyber security awareness is crucial in the event of emerging disruptions, especially in critical infrastructures [11]. Cyber security incident manager needs to process heterogeneous information from different assets to effectively mitigate threats. The identification of security events and response to them is more efficient and faster if the organization is sharing information with others [12].

When sharing cybersecurity information, data classification plays an important role. Cyber security information requiring classification includes e.g. information about security breaches, targeted information systems or defensive measures. Classification provides a mechanism to manage the sharing of confidential information. There is always a risk involved in sharing such information. The sharing of information requires a confidential relationship between the actors so that the information can be securely transmitted outside the organization. This can be achieved in many different ways. [13]

The first steps to address this problem were taken by the US government in 1998 with the publication of a directive to facilitate the sharing of cyber data [14]. The Directive described an approach to industrial data analysis and sharing through Information Sharing and Analysis Centers (ISACs) [15]. Several separate ISAC systems have been established over the last fifteen years [16].

The problem with data sharing is that data on intrusions and vulnerabilities cannot generally be passed on to all actors or data is pledged for too long. On the other hand, the information transmitted may be too general to be used in defense measures. In this case, it is often too late to prevent or mitigate the impact of the attacks before serious damage occurs. [17]

The problem field can be summarized in the following observations. There must be a confidential relationship between the actors in the transmission of sensitive information. The transmission of information must be effective. The information must be sufficiently detailed to be used by the received organization. Unnecessary information should be avoided in the transmission of information between actors in order to avoid a flood of information so that relevant information can be detected. There must be willingness between organizations to share sensitive information, which varies greatly [18].

Mitre Corporation has released following standards for information sharing: Structured Threat Information eXpression (STIX™) [19], Trusted Automated eXchange of Indicator Information (TAXII™) [20] and Cyber Observable Expression (CyBOX™ 2020) [21]. STIX and TAXII have been transitioned to the standard of (OASIS™) Cyber Threat Intelligence (CTI) [22], which has been designed to work together for different needs in CTI management system [23]. Most of these systems focus on sharing information about intrusions and vulnerabilities.

Another alternative and popular standard for cyber security information sharing is Malware Information Sharing Platform (MISP) [24].

According to David Sutton [25]: "Successful cyber situational response requires the timely and reliable exchange of problem and resolution information between interested parties."

In a networked organization environment, it is essential to share cyber security information. Efficiency in a networked environment means trusted and fast sharing of security information, and in this way developing an organization's capability to react against cyber security threats.

In our earlier studies [26, 27] we described the first two models for sharing information of situational awareness between organizations. Utilizing the previous models, we created a cyber security information sharing topology for STIX and TAXII based infrastructure. The model offered the possibility to share classified security related information between multiple organizations with high confidence. In that first model, we used a non-weighted link scenario with calculation of shortest path by Dijkstra algorithm [28]. In the second model, we used link weight in calculation where the weight comes from the organization's activity level and data protection from the privacy classification level. In the study, we continued to develop the model further by adding organization's information services to the calculation of link weight. By adding services to link weight calculations, the goal was to strengthen the efficiency of sharing information online between organizations with similar services. In this model, shortest path was calculated with two methods: Kruskal algorithm [29] and the Dijkstra algorithm used by us in the previous studies.

The journal is organized as follows. In section 2 we first introduce our model which is tested in the Results 3. Lastly, in section 4, we conclude our study with found future research topics.

1.1 Related researches

The sharing of cyber security threat information has been studied from several different perspectives.

Simola et al [30] studied, if it is possible to adapt HAVARO's operations and the system itself to the EU-level early warning system. One of the most significant findings of the study was that the European Union does not have a common cyber ecosystem that detects cyber security threats. The study proposes a new common early warning system database (European Warning System, EWS). The EWS model is based on national information sharing models where countries, companies, public security systems and other actors are involved. From the national level, cyber security threat information is distributed to the EU level using the STIX format.

In their study, Serrano et al [31] present a Knowledge Exchange (KE) model. Organizations can visit KE and order information, and they use the service offering by contacting the publishing organization directly. During operations, each organization maintains a list of known KE providers. The organization can see all available data / service offerings with these KEs. An organization may decide if they want to deploy one or more KEs, publish its information and existing KEs in the service offering, or a combination of both. This approach provides a decentralized ecosystem of information and services. In the study, they propose three main types of KE. Private information exchanges are individual components isolated from other information exchanges through a strict authentication and authorization mechanism; public information exchange shares public information by calling well-known organizations for new exchanges, and community information exchange information with other communities based on their credentials.

In their study, Cha et al [32] propose a blockchain-based cyber threat information sharing architecture. The architecture uses blockchain technology for efficient processing of large data and supply in a decentralized manner, taking into account security and privacy. The cloud server is used to third-party node, which receives a variety of shared cyber threat information from input layer. Cloud server nodes and input layer nodes are accessed through the blockchain. Cloud server nodes have two functions, block creation and confirmation of information. The input layer node has only one function that checks the information.

2 Methods

2.1 STIX, TAXII and MISP

The Structured Threat Information eXpression (STIX™) is a community that defines and develops a language to represent structured threat information and supports following cyber threat management use cases: analyzing cyber threats, specifying indicator patterns, managing response activities and sharing the information of cyber threat. The STIX language has been adopted by a wide range of cyber threat-related organizations and communities around the world. [19]

The STIX architecture has eight constructs, all of which have been generated by the XML schema. The constructs are Observable, Indicator, Incident, TTP (Tactics, Techniques, and Procedures), ExploitTarget, CourseOfAction, Campaign and ThreatActor. [19]

Services and message exchanges between organizations are defined in TAXII protocol. TAXII supports three different threat information sharing architectures: hub-and-spoke, peer-to-peer, and source-subscriber as illustrated in Figure 2. TAXII service has two different solutions, TAXII server and TAXII client, where server and client exchange information in a request-response model. TAXII enables the implementation of complex data sharing structures between multiple actors. In the solution, cyber threat data can be efficiently shared using STIX data structures. [20]

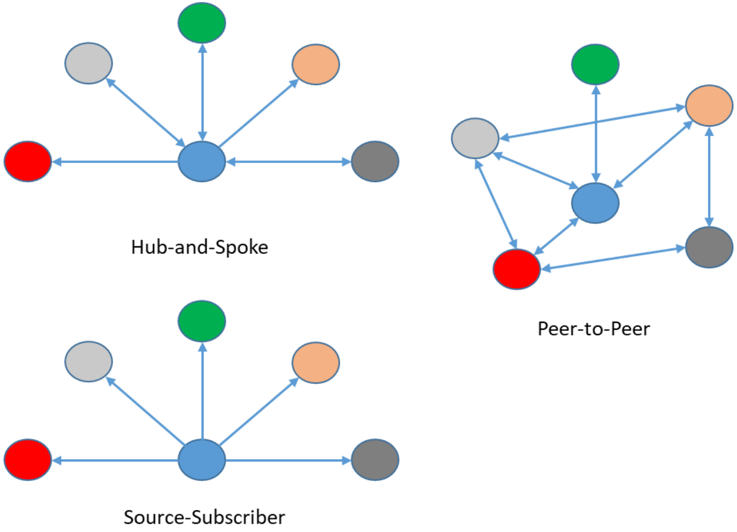

Figure 2. TAXII threat sharing models

MISP is an open source threat intelligence platform for sharing, storing and correlating different kinds of cyber security information. The main target with the MISP is the want of sharing information in easily and automatically to avoid duplication of work. MISP has several features such as indicators of compromise (IOC), sharing groups, automatic correlation, free-text import, event distribution and collaboration. It supports several export formats and has an email alerting capability. [24, 33]

2.2 Cyber Security Information Sharing Model

Organizations in sharing topology can be divided into three categories: Computer Emergency Response Teams (CERTs), Internet Service Providers (ISP) and enterprises.

CERTs are an important actor of the cyber security community. The main objective in their activity is to ensure communications networks and services functions such as response for the protection against, detection of and response to an organization's cybersecurity incidents. CERTs can be divided into three level categories: National or Governmental, Service providers and organizational CERTs.

The CERTs coordinate and monitor activities in data networks collaboration with the network service providers, security vendors, government agencies and the industry sectors [34].

The original model of knowledge sharing is the so-called Hub-and-Spoke model. This model has several challenges, such as trusted relationships between actors, regulation and legal limitations, efficiency of information sharing, and technology itself. [20, 34, 35, 36]

HUB is the key player in this model. HUB acts as a compiler and distributor of information and conveys information to other actors (spoke) in the information sharing network.

At the same time, it can act as an event handler and enricher, as well as a solver for related queries before sharing information. The Hub-and-Spoke model is a good sharing model in situations where the network is small and information sharing is not too time-critical, as the model inevitably delays the data passing through the hub to other spokes. On the other hand, HUBs may have better knowledge to handle events than individual spokes. In this model, also sharing of sensitive information is better controlled. If spokes trust HUB, and HUB has a good understanding which information is sensitive to importing spoke, it can reduce sharing of information based on that rejection.

A more flexible model than Hub-and-Spoke is the so called Peer-to-Peer model, where none of the actors has such a security information distributor role, like HUB has in HUB-and-Spoke model [20, 37].

In this model, where cyber security information is directly shared between different organizations, load balancing and fault tolerance in the whole network is easier to implement. Peer-to-peer model also has challenges. In this model, the challenges come from sharing confidential information. Another challenge is how to ensure that relevant security information is transmitted to all the actors in the network who need it [26].

This study has sought to address the challenges outlined above by developing a new model by combining Hub-and-Spoke and Peer-to-Peer models. The model is an improved version of the previously published models [26, 27].

The purpose of this new model is to speed up the security information sharing in a Peer-to-peer network by calculating between organizations the shortest path that they use to share information. At the same time, the model aims to ensure the secure sharing of information between organizations and to avoid the flood of security information that is not important for the organization in the information network. This is achieved in the new model by including a new parameter in the calculations of the shortest path i.e., the similarity number of enterprises' information systems.

2.3 Information sharing network topology optimization algorithms

In this study, we used two most common algorithms in calculation of the optimized network topology between organizations to information sharing. These two algorithms have several variants.

2.3.1Kruskal algorithm.

Kruskal algorithm [29] is the most commonly used algorithm in Minimum Spanning Tree [38]. Kruskal algorithm finds a minimum spanning tree of an undirected edge-weighted graph, which uses the greedy approach. It handles the graph as a forest and every node it has as an individual tree. If the graph is connected, it finds a minimum spanning tree. A tree will only connect to another if it has the lowest weight of all available options and does not violate minimum spanning tree properties.

2.3.2Dijkstra algorithm.

Dijkstra algorithm is an algorithm, which allows calculating the shortest paths between nodes in a graph. The algorithm creates a tree of shortest paths from the starting vertex to all other nodes in the graph. Dijkstra algorithm is the most used shortest path algorithm is network routing protocols, most notably IS-IS (Intermediate System to Intermediate System) and Open Shortest Path First (OSPF) [39].

2.4 Information sharing model

In this study, we used three different factors to calculate the optimized network topology. Organizations deliver this factor information to the common Path Control System (PCS). Based on these factors, the PCS calculates weights for all links between organizations. The PCS model is illustrated in Figure 3.

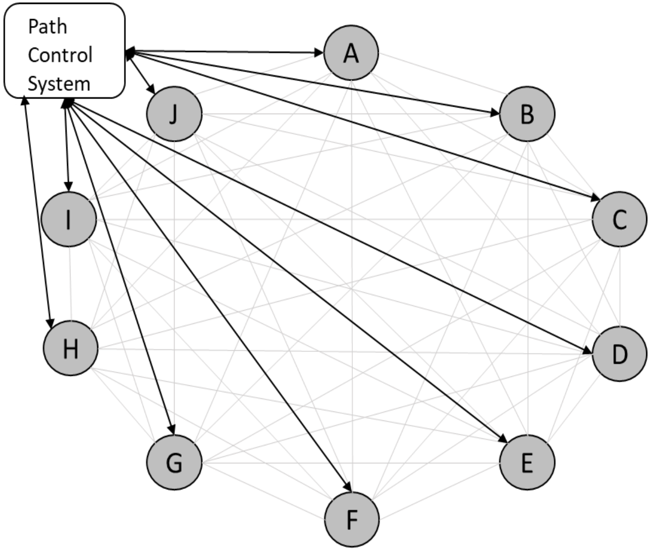

Figure 3. Path Control System and Information sharing Network

The following subsections describe how link weight factors have been calculated.

2.4.1 Similarities between information services of organizations.

In the new model, one of the factors in the decision on information sharing paths is based on the similarities between information services of organizations. Information services cover operating systems, hardware and applications including version numbers. Similarity between organizations' information systems means the common security threats. In this case, e.g., different versions of software create different security threats, and then it is not the same information system. Hardware similarity arises through their operating system versions and hardware configurations.

The organizations store the descriptions of their information services to the Path Control System (PCS), which includes a common configuration management database (CMDB) for all organizations. Organizations can see only their own descriptions in the database.

PCS calculates how many similar organizations have similar information systems based on the following equation:

$$W_l = \frac{1}{I_s+1} \qquad (1)$$

where W_l is the link weight number and I_s is the sum of similar information systems.

In Figure 4 below an example situation has been described where two organizations have the same information systems 1, 8 and 17. The sum of the common information systems is 3. The formula gives weight number $W_{AB} = 0.25$ for the link.

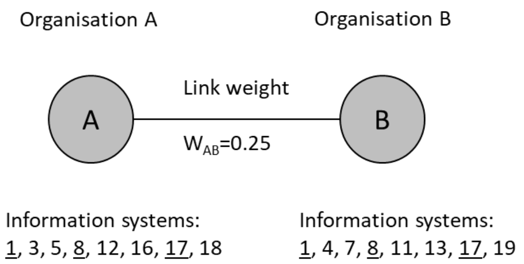

Figure 4. Link weight

Let us make an example of information sharing network where all organizations have a connection to other organizations so that we have a full mesh network. Organizations have similar (character x) information systems as seen in an example in Table 1.

Table 1. Similarity information systems

Information System																				
Organization	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
A	x		x						x				x	x					x	
B	x					x					x		x				x			
C		x		x	x				x		x					x		x		
D			x				x			x				x		x				x
E	x			x		x		x				x		x						
F		x		x				x					x					x	x	
G		x	x			x			x			x			x					
H	x				x		x	x		x							x			
I		x			x		x				x				x					x
J			x			x			x				x	x				x		

Table 2. contains the sum of similar information systems (above) and calculated link weight by calculating with the formula (1).

Table 2. Links' weight between organizations by using only information systems' similarities in calculation

Sum of similar information systems										
Organization	A	B	C	D	E	F	G	H	I	J
A		2	1	2	2	2	2	1	0	4
B	0.33		1	0	2	1	1	2	1	2
C	0.50	0.50		1	1	3	2	1	3	2
D	0.33	1.00	1.00		1	0	1	2	2	2
E	0.33	0.33	0.50	0.50		2	2	2	0	2
F	0.33	0.50	0.25	1.00	0.33		1	1	1	2
G	0.33	0.50	0.33	0.50	0.33	0.50		0	2	3
H	0.50	0.33	0.50	0.33	0.33	0.50	1.00		2	0
I	1.00	0.50	0.25	0.33	1.00	0.50	0.33	0.33		0
J	0.20	0.33	0.33	0.33	0.33	0.33	0.25	1.00	1.00	
Link weight										

Based on this formula, PCS creates an example network map between organizations by using Kruskal algorithm. The network map is illustrated in Figure 5.

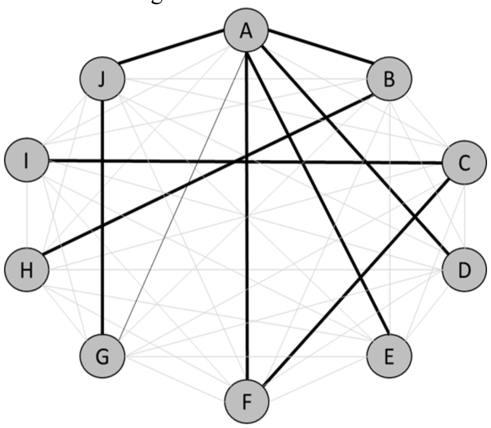

Figure 5. Information sharing network with Kruskal algorithm

As we can see in Figure 5, those organizations with the most common information systems have connected directly together (thick black line), and the other ones have connected to the tree based on shortest link to source vertex organization (A) based on Kruskal algorithm. This topology offers a fast method to share security information about the most common information systems. There are still some problems with effective information sharing. Some paths (e.g. I-C-F-A-E) between organizations are still too long, and that way information sharing is also too slow.

Table 3. illustrate the average link count from each organization to another by Kruskal algorithm. In table, every link space from organization direct to another has value 1.

Table 3. Average link count from each organization to another by Kruskal algorithm

A	B	C	D	E	F	G	H	I	J	Total
1.56	2.22	2.67	2.44	2.44	2.00	3.11	3.11	3.56	2.22	2.53

If we use the same formula which has described in formula (1) and the same example of links' weight between organizations by using only information systems' similarities in calculation, we get different information sharing network topology with Dijkstra algorithm as it has been illustrated in Figure 6.

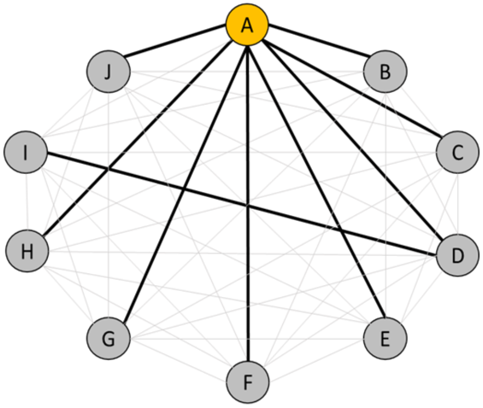

Figure 6. Information sharing network topology with Dijkstra algorithm

Table 4. illustrate the average link count from each organization to another by Dijkstra algorithm. In table every link space from organization direct to another has value 1.

Table 4. Average link count from each organization to another by Dijkstra algorithm

A	B	C	D	E	F	G	H	I	J	Total
1.11	2.00	2.00	1.78	2.00	2.00	2.00	2.00	2.67	2.00	1.96

This information sharing topology much resembles of the original Hub-and-Spoke model where almost every connection goes through the A node. Node A has been implemented as a source vertex. The same situation is repeated with other simulations where the source vertex was something else.

Based on only similarities between organizations, we can see that Dijkstra algorithm works better. The number of average links from every organization to another is less than Kruskal algorithm based topology.

This model does not take into account organization's activity levels or total data protection privacy classification level.

2.4.2 Organization's activity level and privacy classification level.

In the earlier studies we used only organization's activity level and privacy classification level in the equation. This model calculates the link weight with the following equation.

$$W_l = (L_s + L_d) \cdot (|S_s - S_d| + 1) \qquad (2)$$

In the formula, the link weight W_l represents the value of risk for sharing cyber security information. L_s and L_d in the data sharing network represent the organization's activity level of the sender and destination of the network. Activity levels are divided into three categories: corporate, operator and national or industrial operator level (CERT). Each level is assigned its own activity level value. The value increases as you move up from the enterprise level to the ISP level and from there to the CERT level. The formula has been given one for the enterprise level value, two for the operator level, and three for the CERT level. At its fastest, the exchange of information takes place between the lowest level organizations, i.e. companies and the Internet service providers of companies and the second level organizations. The same communication principle is repeated in the original Hub and Spoke model, where the Hub acts as a centralized data distributor.

S_s and S_d are the privacy classification levels defined for the sender and recipient for the available security classification. A lower privacy classification level determines that an operator has information that is more critical in their organization. A value of 1 has also been added to the equation to avoid a situation where the same level of privacy classification of organizations produces a value of zero for the link between them. Various methods can be used to determine the privacy classification level, such as the ISO27005: 2018 series of standards or national security audit criteria. In Finland, for example, the security inspection tool KATAKRI [40] for authorities has been developed for this purpose, which can be used to make a privacy classification [41].

Implemented in this way, every link between organizations are given their own weight. Link weight can be used by determining the shortest path for data transfer. Implemented in this way, a non-directional network is obtained. Figure 7 shows an example of link weight calculation.

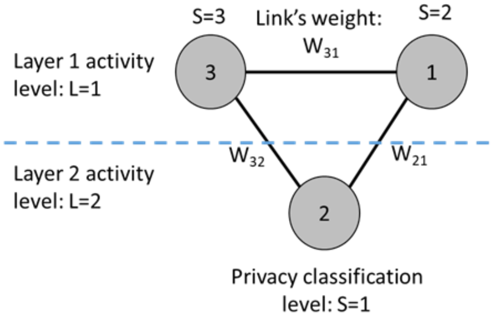

Figure 7. Links weight example

Weights of the links in Fig. 3. are calculated as follows:

$$W_{31} = (1+1)\cdot(|3\text{–}2|+1) = 4 \qquad (3)$$

$$W_{32} = (1+2)\cdot(|3\text{–}1|+1) = 9 \qquad (4)$$

$$W_{21} = (2+1)\cdot(|1\text{–}2|+1) = 6 \qquad (5)$$

3 Results

If we calculate with the same formula similar information systems, the organization's activity level and the privacy classification level, we get the following equation for link weight (Wl):

$$W_l = (L_s + L_d)\cdot(|S_s - S_d| + 1)\cdot\frac{1}{(I_s+1)} \qquad (6)$$

Now the developed model is able to better avoid risky connections, providing a more secure solution for the efficient sharing of cybersecurity-related information. The starting point of the study is that all organizations involved in the information sharing network are responsible for determining their own privacy classification level of security and thereby sharing their own information. At the same time, the developed model also takes into account the activity level in which the organization is located in the information sharing hierarchy and how many similar information systems the organization has. By storing all this information to the PCS, it can calculate the shortest path and inform every organization where they should share security information. The shortest path between organizations ensures that the organization does not have to share information with all other organizations.

As an example we have added organization's activity level and privacy classification level so that A,B and J are CERTs, C and I are ISP operators and D, E, F, G and H are enterprises. Table 5 shows an example of this.

Table 5. Example of organization's activity level and privacy classification levels

Organizatio n	Activity level	Privacy classificatio n level
A	1	4
B	1	3
C	2	3
D	3	2
E	3	2
F	3	1
G	3	2
H	3	1
I	2	2
J	1	4

By adding this information to link weight calculation together with sum of similar information systems as it has been described in formula (3), link weight table is following, as seen in Table 6.

Table 6. Links' weights between organizations by using in calculation information systems' similarities, activity level and privacy classification level

Sum of similar information systems										
Organization	A	B	C	D	E	F	G	H	I	J
A		2	1	2	2	2	2	1	0	4
B	1.33		1	0	2	1	1	2	1	2

C	3.00	1.50		1	1	3	2	1	3	2
D	4.00	8.00	10.00		1	0	1	2	2	2
E	4.00	2.67	5.00	3.00		2	2	2	0	2
F	5.33	6.00	3.75	12.00	4.00		1	1	1	2
G	4.00	4.00	3.33	3.00	2.00	6.00		0	2	3
H	8.00	4.00	7.50	4.00	4.00	3.00	12.00		2	0
I	9.00	3.00	2.00	1.67	5.00	5.00	1.67	3.33		0
J	0.40	1.33	2.00	4.00	4.00	5.33	3.00	16.00	9.00	
						Link weight				

Based on presented formula (3), PCS create a network topology between organizations by using Kruskal algorithm according to the link weights from the Table 6. The network topology is illustrated in Figure 8.

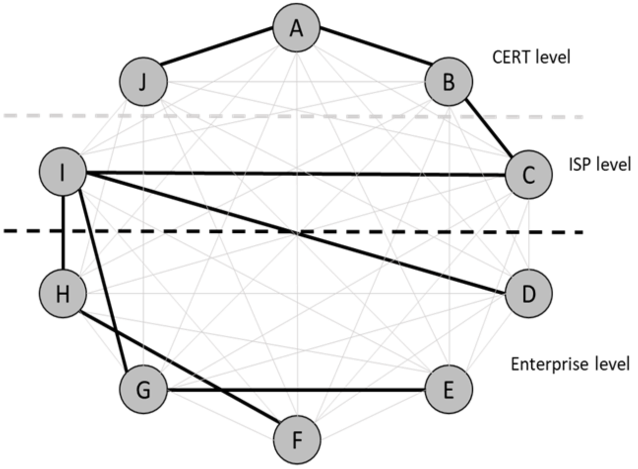

Figure 8. Network topology with Kruskal algorithm, where links' weight between organizations has calculated by using in calculation information systems' similarities, organization's activity level and privacy classification level

As we can see in Figure 8 above, information sharing paths formed are quite long. Information sharing path from enterprise level to ISP and CERTS level is too long even if the security of sharing sensitive information between reliable actors is confirmed.

Table 7. illustrate the average link count from each organization to another by Kruskal algorithm. In table every link space from organization direct to another has value 1.

Table 7. Average link numbers from all organizations to other

A	B	C	D	E	F	G	H	I	J	Total
3.22	2.56	2.11	2.78	3.44	3.44	2.56	2.56	1.89	4.11	2.87

Total links number in the example information sharing network is 9. The sum of used weighted links in optimized network topology is 16.90. Average of used weighted links is 1.88.

If we use Dijkstra algorithm where source vertex is organization A, the network topology looks different. The optimized network topology with Dijkstra algorithm is described in Figure 9.

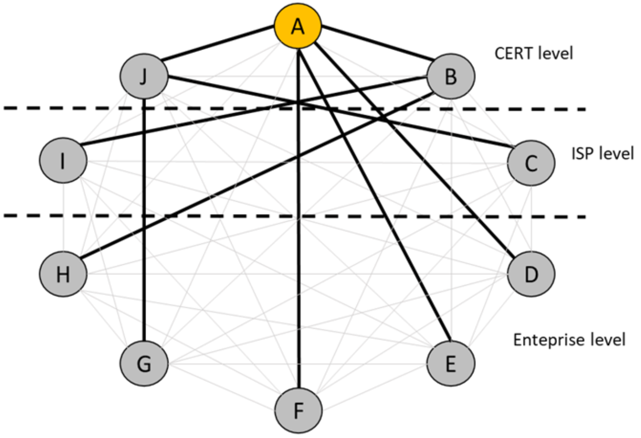

Figure 9. Network topology with Dijkstra algorithm, where links' weight between organizations has been calculated by using in calculation information systems' similarities, organization's activity level and privacy classification level

Table 8. illustrate the average link count from each organization to another by Dijkstra algorithm. In table every link space from organization direct to another has value 1.

Table 8. Average link numbers from each organization to another

A	B	C	D	E	F	G	H	I	J	Total
1.44	1.89	2.78	2.33	2.33	2.33	2.78	2.78	2.78	1.89	2.33

Total links number in the example information sharing network is 9. The sum of used weighted links in optimized network topology is 24.07. Average of used weighted links is 3.01.

It seems that Dijkstra algorithm still creates a more effective topology. Enterprises share security information directly to CERT level, and CERTS share information to ISP level and each other. On the other hand, in Kruskal algorithm-based topology enterprises have direct sharing between EG and FH. This is a faster method at enterprise level; however, the information sharing path from enterprises to ISP is ineffective and longer.

4 Conclusions

The purpose of the model is to improve the security of the sharing of threat information between organizations, to speed up the transmission of security information and to provide a mechanism to avoid the flood of threat information in the receiving organization by primarily transmitting threat information relevant to it.

The security of the sharing threat information is enhanced by the classification of the information to be protected. Each organization defines its own privacy classification level, which serves as one parameter when calculating the weight of links. Other parameters in calculating the weight of the link are the similarity of the information systems and the level of the organization in the information sharing network. The weight is utilized in optimizing the network topology. Thus, the optimization result is not based only on one parameter. It is a combined result of all three parameters according to the formula (3).

We tested the model with two different topology optimization algorithms as well as several simulation times. The article presents only one simulation case. All other simulation cases with different topologies gave similar results. The results show that this model is useful in achieving efficient cybersecurity data sharing by optimizing data sharing paths.

If we compare topologies of both algorithms, we can see differences. Kruskal algorithm gives shortest paths between enterprise organizations. It works well with a small network that we had in our simulation. When the network size increases, paths from enterprise level to CERT and ISP levels lengthen. Average links numbers from each organization to another are bigger with Kruskal algorithm (Table 7: 2.87) than Dijkstra algorithm (Table 8: 2.33). Instead of that, the total sum of used weighted links with Kruskal algorithm is 16.90, which is clearly less than with Dijkstra algorithm (24.07). The same situation we can see also with the average number of weighted links: Kruskal (1.88) and Dijkstra (3.01).

The conclusion from comparison of algorithms is that Kruskal works better in a small network where the emphasis is on efficient security information sharing between individual organizations at enterprise level. Dijkstra works well in larger information sharing networks where sharing from enterprise level to CERT and ISP level in both directions is most relevant.

The test simulation proves that the model can be used in real-life situations with real classified information and different organizations. The same model also works between international organizations, where information is shared through the responsible authorities. Data sharing requires defining the privacy classification level of shared data in each organization and describing existing information systems to calculate the network topology. However, the model is theoretical and requires testing with real data and information systems. Implementing our model would require the creation of an information sharing network using jointly agreed or standard data descriptions and sharing methods. From the existing solutions, we recommend Mitre's STIX format for data description and data transmission using the TAXII protocol and server-client applications. Another equally suitable solution would be to use a MISP-based platform for data sharing. The next step in the study is to test the functionality of the model in practice in the right environment and with the right data. The Health Care Cyber Range project (HCCR) underway at JAMK University of Applied Sciences in Jyväskylä provides an excellent opportunity for this. The project aims to implement a cyber security exercise with partner hospital districts, authorities, and healthcare companies.

ACKNOWLEDGMENTS

Authors would like to thank Ms. Tuula Kotikoski for proofreading the manuscript. This research is partially funded by the European Union under the H2020 Programme Grant Agreement as part of the CyberSec4Europe and the Regional Council of Central Finland/Council of Tampere Region and European Regional Development Fund as part of the Health Care Cyber Range (HCCR) project of JAMK University of Applied Sciences, the Institute of Information Technology.

REFERENCES

<bib id="bib1"><number>[1]</number> Ameneh Deljoo, Tom van Engers, Ralph Koning, Leon Gommans L. 2018. Towards trustworthy information sharing by creating cyber security alliances. 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). 1506-1510. doi: 10.1109/TrustCom/BigDataSE.2018.00213</bib>

<bib id="bib2"><number>[2]</number> Leanne Hirshfield, Philip Bobko, Alex J. Barelka, Mark R. Costa, Gregory J. Funke, Vincent F. Mancuso, Victor Finomore, Benjamin A. Knott. 2019. Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications. Hershey, PA: IGI Global. 1482-1499. doi: 10.4018/978-1-5225-8897-9</bib>

<bib id="bib3"><number>[3]</number> Deepak Tosh, Shamik Sengupta, Charles A Kamhoua, Kevin A Kwiatb. 2018. Establishing evolutionary game models for cyber security information exchange (cybex). Journal of Computer and System Sciences. 98: 27 - 52. https://doi.org/10.1016/j.jcss.2016.08.005</bib>

<bib id="bib4"><number>[4]</number> Martin Husák, Jana Komárková, Elias Bou-Harb, Pavel Čeleda. 2019. Survey of Attack Projection, Prediction, and Forecasting in Cyber Security. IEEE Communications Surveys and Tutorials. 21: 640-660. doi: 10.1109/COMST.2018.2871866</bib>

<bib id="bib5"><number>[5]</number> Mica R. Endsley. 1995. Toward a theory of situation awareness in dynamic systems. Human Factors. 37: 32-64.</bib>

<bib id="bib6"><number>[6]</number> Hannu Rantanen. 2018. Tilannekuvan tuottaminen, hyödyntäminen ja jakaminen - Kriittinen nykytilan tarkastelu. Aluehallintovirastojen julkaisuja. Retrieved November 9, 2020 from https://www.avi.fi/documents/10191/10616116/Julkaisu-42_20180713.pdf/52e3bb5b-f40d-4fcc-8a93-9ab735c3028e.</bib>

<bib id="bib7"><number>[7]</number> George P. Tadda, John S. Salerno. 2009. Overview of Cyber Situation Awareness. Cyber Situational Awareness, Issues and Research, Advances in Information Security. Springer. 46: 15-35. https://doi.org/10.1007/978-1-4419-0140-8_2</bib>

<bib id="bib8"><number>[8]</number> Rauno Kuusisto, Tuija Kuusisto T, Leigh Armistead. 2005. Common Operational Picture, Situation Awareness and Information Operations. Proceedings of the 4th European Conference on Information Warfare and Security. 175-185</bib>

<bib id="bib9"><number>[9]</number> Secretariat of the Security Committee. 2019. Finland's Cyber Security Strategy. Government Resolution. Retrieved November 9, 2020 from https://turvallisuuskomitea.fi/en/finlands-cyber-security-strategy-2019/.</bib>

<bib id="bib10"><number>[10]</number> Angela Horneman. 2019. Situational Awareness for Cybersecurity: An Introduction. Carnegie Mellon University, Software Engineering Institute. Retrieved November 9, 2020 from https://insights.sei.cmu.edu/sei_blog/2019/09/situational-awareness-for-cybersecurity-an-introduction.html.</bib>

<bib id="bib11"><number>[11]</number> Antti Evesti, Teemu Kanstrén, Tapio Frantti. 2017. Cybersecurity situational awareness taxonomy. 2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA). 1-8. doi: 10.1109/CyberSA.2017.8073386</bib>

<bib id="bib12"><number>[12]</number> Jana Komárková, Martin Husák, Martin Laštovička, Daniel Tovarňák D. 2018. CRUSOE: Data Model for Cyber Situational Awareness. Association for Computing Machinery. doi: 10.1145/3230833.3232798, 1-10.</bib>

<bib id="bib13"><number>[13]</number> Adam Zibak, Andrew Simpson. 2019. Cyber Threat Information Sharing: Perceived Benefits and Barriers. ARES '19: Proceedings of the 14th International Conference on Availability, Reliability and Security. 1-9. doi: 10.1145/3339252.3340528. </bib>

<bib id="bib14"><number>[14]</number> Stefan Laube, Rainer Böhme. 2017. Strategic Aspects of Cyber Risk Information Sharing. ACM Computing Surveys (CSUR). 50-5: 1-36. doi:10.1145/3124398,2017. </bib>

<bib id="bib15"><number>[15]</number> Lawrence A Gordon, Martin P Loeb, William Lucyshyn, Lei Zhou. 2015.. The impact of information sharing on cybersecurity underinvestment: A real options perspective. Journal of Accounting and Public Policy. 34-5: 509-519. https://doi.org/10.1016/j.jaccpubpol.2015.05.001</bib>

<bib id="bib16"><number>[16]</number> Meilin He, Laura Devine, Jun Zhuang. 2018. Perspectives on cybersecurity information sharing among multiple stakeholders using a decisiontheoretic approach. Risk Analysis. 201838-2: 215-225. doi: 10.1111/risa.12878</bib>

<bib id="bib17"><number>[17]</number> Cristin Goodwin, J. Paul Nicholas, Jerry Bryant, Kaja Ciglic, Aaron Kleiner, Cornelia Kutterer, Alison Massagli, Angela McKay, Paul McKitrick, Jan Neutze, Tyson Storch, Kevin Sullivan. 2015. A framework for cybersecurity information sharing and risk reduction. Microsoft. Retrieved November 9, 2020, from https://download.microsoft.com/download/8/0/1/801358EC-2A0A-4675-A2E7-96C2E7B93E73/Framework_for_Cybersecurity_Info_Sharing.pdf.</bib>

<bib id="bib18"><number>[18]</number> Claudia Colicchia, Alessandro Creazza, Carlo Noè, Fernanda Strozzi. 2019. Information sharing in supply chains: a review of risks and opportunities using the systematic literature network analysis (slna). Supply Chain Management: An International Journal. 24-1:5-21. https://doi.org/10.1108/SCM-01-2018-0003</bib>

<bib id="bib19"><number>[19]</number> Sean Barnum. 2014. Structured Threat Information eXpression (STIXTM). White paper, version 1.1, revision 1. Retrieved November 9, 2020 from http://stixproject.github.io/getting-started/whitepaper/.</bib>

<bib id="bib20"><number>[20]</number> Julie Connolly, Mark Davidson, Charles Schmidt. 2014. The Trusted Automated eXchange of Indicator Information (TAXIITM), white paper. Retrieved October 9, 2020 from http://taxiiproject.github.io/getting-started/whitepaper/.</bib>

<bib id="bib21"><number>[21]</number> Cyber Observable eXpression (CybOX™) Archive Website. 2020. Retrieved October 9, 2020 from https://cyboxproject.github.io/.</bib>

<bib id="bib22"><number>[22]</number> OASIS STIX™ and TAXII™ documentation. 2020. Retrieved October 9, 2020 from https://oasisopen.github.io/cti-documentation/.</bib>

<bib id="bib23"><number>[23]</number> Md Sahrom Abu, Siti Rahayu Selamat, Aswami Ariffin, Robiah Yusof. 2018. Cyber threat intelligence – Issue and challenges. Sahrom Abu's Lab. 371-379. doi: 10.11591/ijeecs.v10.i1. </bib>

<bib id="bib24"><number>[24]</number> MISP - Malware Information Sharing Platform. 2020.. Retrieved September 28, 2020 from https://www.misp-project.org/index.html.</bib>

<bib id="bib25"><number>[25]</number> David Sutton. 2015. Trusted information sharing for cyber situational awareness. e & i Elektrotechnik und Informationstechnik. 132-2: 113-116. doi:10.1007/s00502-015-0288-3. </bib>

<bib id="bib26"><number>[26]</number> Tero Kokkonen, Jari Hautamäki, Jarmo Siltanen, Timo Hämäläinen. 2016. Model for sharing the information of cyber security situation awareness between organizations. 23rd International Conference on Telecommunications (ICT). 1-5. doi: 10.1109/ICT.2016.7500406</bib>

<bib id="bib27"><number>[27]</number> Jari Hautamaki, Tero Kokkonen. 2020. Model for Cyber Security Information Sharing in Healthcare Sector. 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), Istanbul, Turkey. doi: 10.1109/ICECCE49384.2020.9179175 </bib>

<bib id="bib28"><number>[28]</number> Edsger Wybe Dijkstra. 1959. A note on two problems in connexion with graphs. Numerische Mathematik. 1-1. doi: 10.1007/BF01386390.</bib>

<bib id="bib29"><number>[29]</number> Joseph Bernard Kruskal. 1956. On the shortest spanning tree of a graph and the traveling salesman problem. Proceedings of the American Mathematical Society. 7: 48-50. https://doi.org/10.1090/S0002-9939-1956-0078686-7</bib>

<bib id="bib30"><number>[30]</number> Jussi Simola, Martti Lehto. 2020. National Cyber Threat Prevention Mechanism as a part of the E-EWS. International Conference on Cyber Warfare and Security. Reading. doi:10.34190/ICCWS.20.106.</bib>

<bib id="bib31"><number>[31]</number> Oscar Serrano, Luc Dandurand, Sarah Brown. 2014. On the Design of a Cyber Security Data Sharing System. WISCS '14: Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security, 61–69. doi: 10.1145/2663876.2663882.</bib>

<bib id="bib32"><number>[32]</number> Jeonghun Cha, Sushil Kumar Singh, Yi Pan, Jong Hyuk Park. 2020. Blockchain-Based Cyber Threat Intelligence System Architecture for Sustainable Computing. Sustainability. 12(16):6401. doi:10.3390/su12166401</bib>

<bib id="bib33"><number>[33]</number> Konstantina Fotiadou, Terpsichori-Helen Velivassaki, Artemis Voulkidis, Konstantinos Railis, Panagiotis Trakadas, Theodore Zahariadis. 2020. Incidents Information Sharing Platform for Distributed Attack Detection. IEEE Open Journal of the Communications Society. 1: 593-605. doi: 10.1109/OJCOMS.2020.2989925. </bib>

<bib id="bib34"><number>[34]</number> Eduard Babulak. 2011. Tutorial 3: Cyber Security: The Importance of CERTs (Computer Emergency Response Teams). UkSim 13th International Conference on Computer Modelling and Simulation. doi: 10.1109/UKSIM.2011.117.31. </bib>

<bib id="bib35"><number>[35]</number> Seyedeh Negar Khajeddin, Afsaneh Madani, Hossein Gharaee, Farzaneh Abazari. 2019. Towards a functional and trustful web-based information sharing center. 5th International Conference on Web Research. ICWR). 252-257. doi:10.1109/ICWR.2019.8765297</bib>

<bib id="bib36"><number>[36]</number> Florian Skopik, Giuseppe Settanni, Roman Fiedler. 2016. A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. Computers & Security. 60-C: 154-176. https://doi.org/10.1016/j.cose.2016.04.003</bib>

<bib id="bib37"><number>[37]</number> Manoj Parameswaran, Anjana Susarla, Andrew B.Whinston. 2001. P2p networking: an information sharing alternative. Computer. 34-7: 31-38. doi: 0.1109/2.933501</bib>

<bib id="bib38"><number>[38]</number> Haiming Li, Qiyang Xia, Yong Wang. 2017. Research and Improvement of Kruskal Algorithm. Journal of Computer and Communications. 5:63-69. doi: 10.4236/jcc.2017.512007.</bib>

<bib id="bib39"><number>[39]</number> Phani Raj Tadimety. 2015. OSPF: A Network Routing Protocol. Apress. doi:10.1007/978-1-4842-1410-7_22.</bib>

<bib id="bib40"><number>[40]</number> Ministry of Defence, Finland. 2015. Katakri, information security audit tool for authorities - katakri, tietoturvallisuuden auditointityökalu viranomaisille. Katakri. Retrieved October 9, 2020 from https://www:defmin:fi/files/3165/Katakri 2015 Tietoturvallisuuden auditointityokalu viranomaisille.pdf.</bib>

<bib id="bib41"><number>[41]</number> Jyri Rajamäki. 2014. Challenges to a smooth-running data security audits. case: A finnish national security auditing criteria katakri. 2014 IEEE Joint Intelligence and Security Informatics Conference. 240-243. doi:10.1109/JISIC.2014.45</bib>