Adjusting cyber insurance premiums based on frequency in a communication network

Sapto Wahyu Indratno [a,b,1,*], Yeftanus Antonio [a,2], Suhadi Wido Saputro [c,3]

[a] Statistics Research Division, Faculty of Mathematics and Natural Sciences, Institut Teknologi Bandung, Bandung 40132, West Java, Indonesia
[b] University Center of Excellence on Artificial Intelligence for Vision, Institut Teknologi Bandung, Bandung 40132, West Java, Indonesia
[c] Combinatorial Mathematics Research Division, Institut Teknologi Bandung, Bandung 40132, West Java, Indonesia
[1] sapto@math.itb.ac.id; [2] yeftanus@students.itb.ac.id; [3] suhadi@math.itb.ac.id
* corresponding author

ARTICLE INFO

Article history
Selected paper from The 2020 3rd International Symposium on Advanced Intelligent Informatics (SAIN'20), Virtual, 25-26 November 2020, http://sain.ijain.org/2020/. Peer-reviewed by SAIN'20 Scientific Committee and Editorial Team of IJAIN journal.

Received November 23, 2020
Revised August 9, 2021
Accepted August 9, 2021
Available online November 30, 2021

Keywords
Communication network
Cyber insurance
Frequency
Node-based model
Premium adjustment

ABSTRACT

This study compares cyber insurance premiums with and without a communication network effect frequency. As a cybersecurity factor, the frequency in a communication network influences the speed of cyberattack transmission. It means that a network or a high activity node is more vulnerable than a network with low activity. Traditionally, cyber insurance pricing considers historical data to set premiums or rates. Conversely, the network security level can evaluate using the Monte Carlo simulation based on the epidemic model. This simulation requires spreading parameters, such as infection rate, recovery rate, and self-infection rate. Our idea is to modify the infection rate as a function of the frequency in a communication network. The node-based model uses probability distributions for the communication mechanism to generate the data. It adopts the co-purchase network formation in market basket analysis for building weighted edges and nodes. Simulations are used to compare the initial and modified infection rates. This paper considered prism and Petersen graph topology as case studies. The relative difference is a metric to compare the significance of premium adjustment. The results show that the premium for a node with a low level in a communication network can reach 28.28% lower than the initial premium. The premium can reach 20.99% lower than the initial network premium for a network. Based on these results, insurance companies can adjust cyber insurance premiums based on computer usage to offer a more appropriate price.

1. Introduction

Cyber insurance is a risk management tool to transfer financial losses due to communication and information technology operations [1]–[3]. Economic damage caused by cyberattacks shows an increasing trend in the range of 1.1% to more than 30% of the global gross domestic product [4]. The annual cost of cybercrime is estimated to reach USD 6 trillion by 2021, which is more than twice that of 2015 [5]. This condition can improve cyber insurance sales and the market in the coming years. Cyber insurance still has some technical challenges [6]. One of the main issues associated with cyber insurance is how to estimate premiums or rates [7], [8]. Today, there is no established pricing method for cyber insurance products. Some of the available products are offered at high prices because of the long and complicated identification and selection of risks (underwriting) [9]. Several existing risk models consider the demand and supply of the product. Other factors to consider are assumptions regarding network structure, computer information, and attack's timing. Information and communication technology

(ICT) sources are connected to a network. This condition necessitates an analysis of cyber risk and potential losses that include the structure of the system.

References [10] and [11] are two studies involving network structure in premiums calculation in the last 2 years. The authors used a susceptible–infectious–susceptible (SIS) epidemic model with a different approach. The simulation of the SIS compartment model to predict cyber risk with the Gillespie Algorithm has been carried out for several finite networks [12]. In reference [10], the authors used the SIS model without the possibility of self-infection to capture cyber infection. The claims process was modeled by a marked point process, which was a collective risk model. These claims depend on the spread of cyber threats modeled by SIS. Xu and Hua [10] used the more general SIS model, the ϵ-SIS model, which allowed the self-infection process. The dynamics of virus spread were captured using the Monte Carlo simulation. The loss for each node is calculated using the loss function. Therefore, this model is an individual risk model approach. References [10] and [11] can better understand network structure dependence on cyber insurance pricing. However, both still assumed that each computer (or node) is identical. We have demonstrated similar outcomes on regular networks [13]. Under the same parameter settings, each node with the same degree provided equal premiums. In fact, every computer has different activities. Different levels of activity make the infection rate of each node not homogeneous. Computers with high activity can infect other computers faster than computers with low activity. Thus, the premium can be adjusted according to the activity using in-homogeneous SIS. We have also modified the Markov-based model with local clustering coefficients to generate different rates according to the epidemic inhibition function [14].

This study develops the model to accommodate the frequency in a communication network (the number of connections) as a network security factor [15]. Assume that an attack on ICT sources occurs at an initial infection rate. The infection rate depends on the frequency in a communication network. Transmissibility increases when the frequency is high and decreases when the frequency is low. Thus, the infection rates are a function of the number of connections. Our contributions can be seen in two ways: (1) the robustness of the network structure for cyberattacks and (2) the suitability of insurance premiums. In the process of designing a computer network, network security factors are rarely discussed. Usually, network structure design decisions are based on two main factors: the number of connections and communication routes [16]. We try to add the network security factor in designing the network to choose a more robust structure. It is part of the cyber insurance pricing process when evaluating the network security level.

The premium calculation considers the initial and modified infection rates for comparisons. It aims to adjust the premium using the frequency in a communication network as a cyber risk factor. In other words, the infection rate of a node is a function of its communication intensity. Communication data are generated using a node-based model. This model uses the co-purchase product network formation analogy in market basket analysis [17] and probability distribution. We change the transaction to communication and product to computer/server in the network. This method can adjust cyber insurance premiums based on the frequency in a communication network. Prism and Petersen graph topology were considered as case studies. Both topologies have three degrees in each node, short diameter, stable data distribution process, and easy to manage failure. The main objective of this paper is to provide more appropriate premiums with modified infection rates. This paper is organized as follows: Section 1 provides the study's background, objectives, and contributions. Section 2 summarizes previous studies related to the model, topology, and premium results. Section 3 details the methodology in this study. Section 4 presents the simulation results and discussion. Finally, Section 5 is the conclusion.

2. Method

Cyber insurance pricing in this study involves three aspects: first, the topology type used for pricing; second, a model to describe the communication mechanism on the network; and third, the epidemic model and its characteristics. Methods related to these topics are presented in this section.

2.1. Network Topology

A network topology is the arrangement of computer systems or ICT resources to communicate [18]. There are eight basic topologies in studying networks: point to point, mesh, ring, star, bus, tree, hybrid, or daisy chain. These topologies have advantages and disadvantages that are often discussed. The factors for evaluating the network topology are flexibility, speed, installation, troubleshooting, data transmission, performance, usability, and cost [19], [20]. Generally, network optimization aims to reduce costs and gain efficiency, robustness, and uniform distribution of traffic [21]. Discussions of network topology resilience against cyberattacks [22] in topology design and evaluation are still rare.

As shown in Fig. 1, prism and Petersen graphs can be used in the new topological design process. The prism and Petersen graphs have 10 nodes, 15 edges, and three degrees. The degree is the number of edges on a node. The difference is only in the maximum distance between two nodes or the diameter [23]. The prism diameter is three, whereas the Petersen diameter is two. The previous comparison study shows that the Petersen graph is more reliable and more efficient in sending packet data requests and successful packet data requests than the prism graph [23]. Apparently, this is because Petersen has a shorter diameter than the prism. We choose these two topologies for other comparison objectives. We add two objectives to analyze and compare these networks from a different side: (1) simulating virus transmission to see the robustness of the topology against virus attacks and (2) adjusting insurance prices in both topologies using the number of communications in a network.

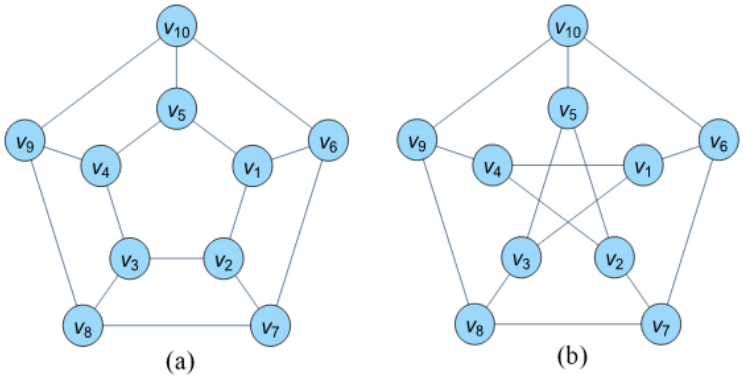

Fig. 1. (a) Prism Graph; (b) Petersen Graph.

2.2. Communication Model

One of the network security options depends on the frequency in a communication network, how strong each communication signal is, and how many channels are used for transmission [24]. We use a node-based model approach to determine the number of communications in a network. This model adopts the process of building a co-purchase product network in market basket analysis [17], [25]. The result of this model is a network with weighted edges. To obtain the communication weight of vertex (or node) i, we used the vertex weight approach in graph theory. The weight of vertex (or node) i is the sum of all edge weights incident to node i. Fig. 2 shows the process of forming a weighted network using a node-based model. For example, there are three communications in a day. These communications are C_1, C_2, and C_3. Each communication involves several nodes that send or receive data. The node-based approach involves two random variables: the number of communications in a network and the number of nodes in each communication. To build a network with weighted edges, the data are generated through the distribution of both random variables. This edge weight is used to calculate the weight of each node.

2.3. Epidemic Model

The study of epidemics and their modeling has been widely used to understand the cyber risk process and how computer viruses spread [26], [27]. Xu and Hua [28] have successfully introduced the modeling and pricing of cybersecurity insurance with a network structure approach. They combined the graph theory and the epidemic model to evaluate the network security level using the generalized susceptible-

infection-susceptible (ϵ-SIS) model [29]. This model has three parameters. These are the infection rate β, the recovery rate ∂, and the self-infection rate ϵ. We adopt this model to an in-homogeneous infection rate [30], where an infected node attacks a secure (but vulnerable) node at different rates. Let an undirected graph $G=(V,E)$ be an abstraction of the network topology, where V is a set of vertices and E is a set of edges [31]. In this case, the vertices (or nodes) represent computers or other ICT sources, such as servers, routers, switches, and hubs. Edges (or links) are communication channels that transmit data over connections between two or more nodes. Undirected graph $G=(V,E)$ has representation in matrix form, that is, the adjacency matrix $A=(a_{ij})$, where $a_{ij}=1$ if $(i,j)\in E$, and 0, otherwise.

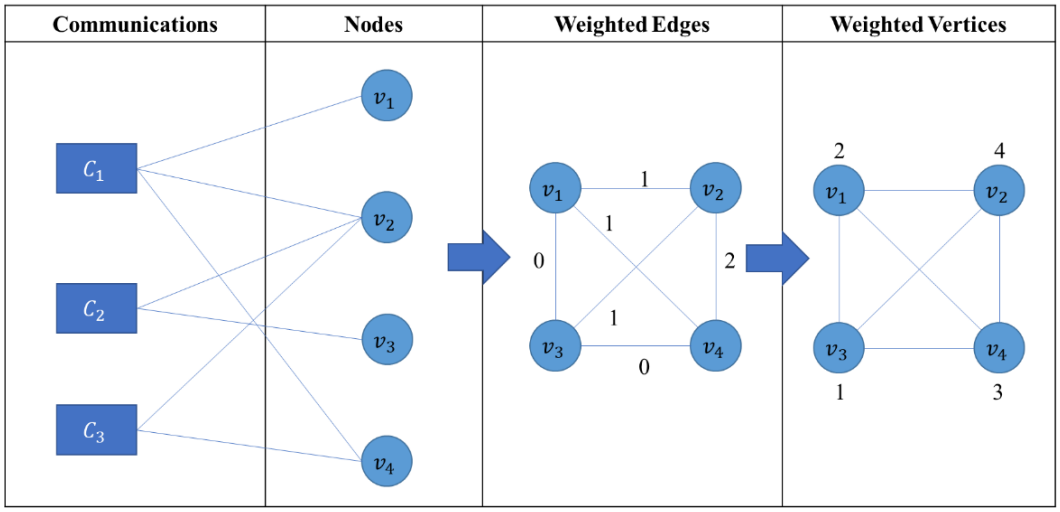

Fig. 2. Communication mechanism in a node-based model using the analogy of building a co-purchase network of products.

Consider $X_i(t)$ as the state of node i at time t where $X_i(t)=1$ if node i is infected at time t and $X_i(t)=0$ if node i is secure (but vulnerable) at time t. Vector $\boldsymbol{X}(t)=\left(X_1(t),\cdots,X_N(t)\right)^{\cdot}$ is the vector of the network status at time t for $|V|=N$. The vector of the infection probability can be written as $\boldsymbol{p}(t)=\left(p_1(t),\cdots,p_N(t)\right)^{\cdot}$, where $p_i(t)=P\left(X_i(t)=1\right)$ for $i=1,\cdots,N$. The transition probability for node i is given by $p_{i,yz}(h)=P\left(X_i(t+h)=z|X_i(t)=y\right)$.

Suppose an infected node i attacks secure (but vulnerable) neighbors at varying rates β_i. This model refers to the in-homogeneous SIS model [19]. We relax the model using the same recovery rate $\delta_i=\delta$. However, this case still considers infection from outside the network with the same self-infection rate ò for every node. Thus, the transition probability from node i can be written as

$$p_{i,yz}(h)=\begin{cases}\left(\sum_{j=1}^{N}\beta_j a_{ij}X_j(t)+\text{ò}\right)h+o(h); & y=0,z=1\\ \delta h+o(h) & ; \quad y=1,z=0\end{cases}, \tag{1}$$

where the function f is equal to $o(h)$ for $\lim_{h\to 0}\frac{f(h)}{h}=0$. The infection rate β_j depends on the frequency in a communication network. Let β be the initial infection rate at which an attack can cause infection. The attack ability can be reduced when communication is low. Conversely, a complete attack

can occur when communication is high enough. Thus, the initial infection rate β_0 becomes the upper bound of the infection rate for all nodes i.

2.4. Simulation

2.4.1. Communication Frequency

Communication weights are generated by the node-based model. Let C be the random variable that represents the number of communications in a day and D be the random variable for the number of active nodes for every communication. The active nodes are randomly chosen with different probability of activation (or sampling probability) sp, where $sp \sim U(0,1)$ uniformly distributed. The steps for building a node-based model are as follows:

Step 1. Specify V and E based on $G(V,E)$.

Step 2. Generate sp from $U(0,1)$.

Step 3. For discrete time $\{1,\cdots T\}$, generate C from $F_C(c)$.

Step 4. For every C, generate D from $F_D(d)$. Randomly select d nodes in V using sp and combine every two-couple node as an active link.

Step 5. Accumulate every active link up to time T.

Step 6. Set total active link as the weight of edges w_{ij} for $(i,j) \in E$.

Step 7. Calculate the weight of node $w_j = \sum_i w_{ij}$.

After obtaining the communication weight for each node, then this weight is used to influence the infection rate. This communication frequency is a necessary condition for calculating the premium with additional factors.

2.4.2. Security Evaluation and Premium Setting

The premium calculation uses Xu and Hua's network security level evaluation approach [28] using the epidemic model. They showed that the dynamic change of node status for the $\grave{o}$ -SIS model can be generated through time to infection due to infected neighbor attacks, time to infection due to attacks from outside the network, and time to recovery. These times depend on β_0, δ, and $\grave{o}$. Let β_0 be called the initial infection rate, which is the strength or speed of the attack. We initiate that this infection rate can be different according to the communication characteristics of each node j, that is

$$\beta_j = \frac{\beta_0}{1+e^{-w_j}} \tag{2}$$

This function shows the relationship between the infection rate of node i and its weight, which acts as a rate adjustment function of node i. For initial β_0, the simulation uses the algorithm and two types of losses provided by Xu and Hua [28]. These results are compared with different β for each node (β_j) using the function in equation (3). Let $Y_{j_1}, Y_{j_2}, \cdots, Y_{j_{D_i}}$ be the random variables of time to infection due to attacks from neighbors of node i where $j_1, j_2, \cdots, j_{D_i}$ are the neighbors of node i and D_i is the number of infected neighbors of node i. Every infected neighbor of node i has its infection rate β_j and $Y_{j_1} \sim F_j(y)$. Let Z_i be the random variable of time to infection of node i due to attack from outside the network where $Z_i \sim G(y)$. Furthermore, let R_i be the random variable of time to recovery

of node i where $R_i \sim H(y)$. Total loss of node i during the contract period $(0,t]$ can be written as follows:

$$S_i(t) = \sum_{k=1}^{M_i(t)} \left[\mu_i\left(L_i^k\right) + \gamma_i\left(R_i^k\right) \right], \tag{3}$$

where $M_i(t)$ is the number of infections faced by node i up to time t, $\mu_i(.)$ is the cost function corresponding to the loss due to infection, and $\gamma_i(.)$ is the cost function corresponding to the loss due to recovery time. Random variables L_i and R_i represent the random losses caused by infection and recovery time.

In this study, in-homogeneous SIS is the Markov model, and then $Y_{j_1} \sim \overline{F}_j(y) = e^{-\beta_j y}$, $Z_i \sim \overline{G}(y) = e^{-\delta y}$, $R_i \sim H(y) = e^{-\delta y}$. All of them are exponentially distributed. This can be proven by the basic theorem of the alternating renewal process (see reference [28]). The simulations are conducted using the following steps:

Step 1. Define the adjacency matrix A, the initial network status, the number of simulations n_s, and the contract period T.

Step 2. Calculate the number of infected nodes M at time t and generate $r_1, r_2, \cdots, r_M$ from $\exp(\delta)$.

Step 3. For every node i, find the infected neighbors $j_1, j_2, \cdots, j_{D_i}$ and then generate $Y_{j_1}, Y_{j_2}, \cdots, Y_{j_{D_i}}$ from $\exp(\beta_j)$ and Z_i from $\exp(\delta)$.

Step 4. Define the time of the first event $t_1 = \min\{r_1, r_2, \cdots, r_M, Y_{j_1}, Y_{j_2}, \cdots, Y_{j_{D_i}}, Z_i\}$.

Step 5. If infection occurs, change the node status from 0 to 1 and calculate the loss. If repair occurs, change the node status from 1 to 0 and calculate the loss.

Step 6. Given that $t + t_1 < T$, do steps 2 to 5 and determine $t = t + t_1$. Otherwise, the process stops.

Step 7. Repeat steps 2 to 6 until the number of simulations n_s is fulfilled.

This process is used to determine topological robustness and premium comparisons.

2.5 Difference Metric

This analysis requires a metric to measure how much the adjusted premiums and initial premiums change. One of the measures for comparison is the relative difference [32]. Let P be the initial premium and PA be the adjusted premium. The percentage of the premium adjustment can be measured by the percentage of relative differences (Δ_r) as follows:

$$\Delta_r = \frac{PA - P}{P} \times 100\%. \tag{4}$$

This metric can indicate how big the adjustment of rates if we include the frequency in a communication network for pricing.

3. Results and Discussion

In this section, we show the simulation results that have been conducted on the two topologies in Fig. 1. These simulations use an observation period of T = 365. The selected input parameters are

β = 0.2, δ = 1, and $\grave{o}$ = 0.05. The process of generating communication weights assumes $C \square Poisson(\lambda_c)$ and $D \square Poisson(\lambda_d)$. Several pairs of parameters are considered to see the effect of communication on the premium calculation results. We considered four pairs of parameters $(\lambda_c, \lambda_d) = \{(10,2),(20,4),(30,6),(40,8)\}$. For the loss function, suppose L_i follows a beta distribution with parameters $a = 3, b = 8,$ and $w_i = 1500$, where the probability density function is given by

$$f_{L_i}(\phi|a,b,w_i) = \frac{1}{\phi B(a,b)}\left(\frac{\phi}{w_i}\right)^{a}\left(1-\left(\frac{\phi}{w_i}\right)\right)^{b-1}, 0 < \phi < w_i. \quad (5)$$

The parameter w_i denotes the initial wealth of the computer/ICT source i. The simulations use the following loss functions: (1) $\mu_i(L_i = \phi) = \psi\phi$ and (2) $\psi_i(R_i = r_i) = \psi_1 w_i + \psi_2 r_i$, where (ψ, ψ_1, ψ_2) are equal to $(1\times10^{-3}, 5\times10^{-6}, 2\times10^{-5})$. This simulation compares the infection rate β with β_j given by equation (3). Finally, the premium calculation for node i using the following standard deviation principles [33]

$$P_i = E\left[S_i(t)\right] + \theta\sqrt{Var\left(S_i(t)\right)}, \quad (6)$$

and for a network is given by

$$P = E\left[S(t)\right] + \theta\sqrt{Var\left(S(t)\right)} \quad (7)$$

where θ is the loading factor and $S(t) = \sum_{i=1}^{N} S_i(t)$. In this case, we choose θ = 0.1.

3.1 Topological Robustness

To analyze topological resistance, Table 1 provides the descriptive statistics of the number of infections for each node in each topology. Regardless of the communication effect, the mean, standard deviation, and minimum and maximum infection of each topology have almost the same values. This is because the two topologies have almost the same characteristics. The only difference is the diameter. The transmission model depends on the degree. Conversely, communication effectiveness depends on the diameter. However, if the simulation shows that the Petersen topology is more effective in communication, then this topology is more vulnerable to cyberattacks. Thus, the optimal topology design considers not only the route and communication effectiveness but also the vulnerability of the topology.

Table 1. Descriptive statistics of the number of infections during a period for prism and Petersen topology.

Node	Prism topology				Petersen topology			
	Mean	*SD*	*Min.*	*Max.*	*Mean*	*SD*	*Min.*	*Max.*
1	31.333	5.642	14	51	30.983	5.412	15	52
2	31.440	5.534	15	55	31.410	5.533	17	51
3	31.242	5.449	14	48	31.022	5.776	16	49
4	31.359	5.723	14	51	31.401	5.495	16	48
5	30.990	5.484	17	49	31.494	5.578	17	53
6	31.050	5.516	16	52	31.250	5.379	15	49
7	31.181	5.569	11	54	30.921	5.340	15	48
8	31.143	5.756	15	51	31.255	5.539	11	49
9	30.890	5.413	14	48	31.309	5.513	15	49
10	31.106	5.584	14	50	31.599	5.587	18	53

3.2 Premium Adjustment

This section discusses the effect of communication on the premium calculation results. This study also considers the size of the premium adjustment for certain communication characteristics. The four selected communication parameters indicate four types of communications, namely, low, medium, high, and very high. The results for adjusting premiums based on the number of communications are compared with the simulation results without including these effects. Fig. 3 shows the premium of each node in the prism and Petersen topology (Fig. 1) that changes with the changes in communication parameters. Node labels are node 1 for v_1, node 2 for v_2, and so on until node 10 for v_{10}.

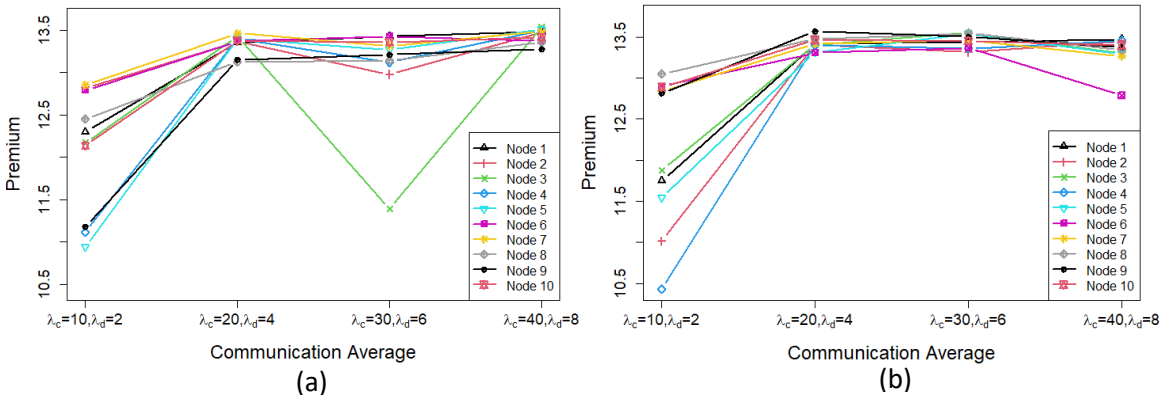

Fig. 3. Cyber insurance premium of every node using different communication average for (a) prism topology and (b) Petersen topology with $F_C(c) \sim Poisson(\lambda_c)$ and $F_D(d) \sim Poisson(\lambda_d)$.

For λ_C = 10 and λ_d = 2, every node in prism and Petersen topology has varying premiums. Premium ranges from 10 to 13.5 in unit price. Higher communication results in higher premiums and closer to a value. Although not consistently increasing, the decrease in premium prices for λ_c = 30 and λ_d = 6 (high communication) in the prism topology is an effect of the random behavior of node weights. Node 3, for example, is close to the premium for λ_c = 10 and λ_d = 2 (low communication) after increasing at λ_c = 20 and λ_d = 4 (medium communication). Similarly at node 6 in the Petersen topology, after rising, the premium decreases for λ_c = 40 and λ_d = 8 (very high communication). This pattern only occurs on a few nodes. Most of the premiums increase when the communication frequency increases. The upward trend is confirmed by the premium for all nodes (network) given in Fig. 4. Both premiums have different fluctuations. Prism topology (blue line) has decreased for medium communication, and Petersen topology (red line) has decreased for very high communication. As discussed earlier, this is because random communication has many realizations. In this case, one of the different means of communication is considered. It does not lose the generality of this result. Although fluctuating, Fig. 4 shows an increasing trend for higher communication frequencies.

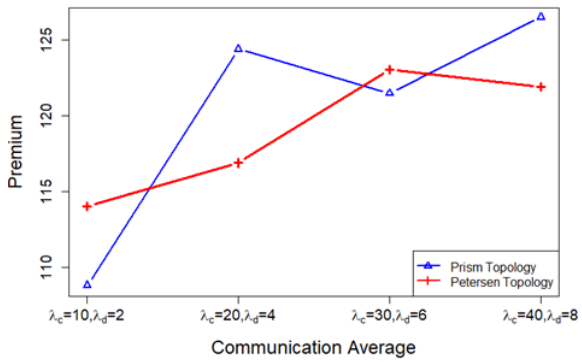

Fig. 4. Cyber insurance premiums of the network using different communication average for prism and Petersen topology with $F_C(c) \sim Poisson(\lambda_c)$ and $F_D(d) \sim Poisson(\lambda_d)$.

Low communication premiums are always below the premium for medium, high, and very high communications. These results indicate that cyber insurance premiums can be adjusted according to the level of computer activity. A network with a lower level of communication provides a lower premium. These results can also address the issue of cyber insurance premiums that are usually offered at high prices. The level of communication can influence the risk of cyberattacks spreading and lead to a more rational premium. The amount of premium adjustment is measured by the relative percentage Δ_r in equation (2).

Table 2. Adjustment percentage Δ_r value for prism topology and Petersen topology.

Node (λ_c, λ_d)	Δ_r (%) of Prism topology				Δ_r (%) of Petersen topology			
	(10,2)	*(20,4)*	*(30,6)*	*(40,8)*	*(10,2)*	*(20,4)*	*(30,6)*	*(40,8)*
v_1	9.06	0.45	−0.10	−0.49	13.47	−0.64	−0.78	−1.04
v_2	5.31	1.03	4.03	0.23	22.13	0.39	1.05	0.05
v_3	10.26	−0.04	17.82	−0.89	12.05	−0.76	−1.82	0.02
v_4	20.88	0.32	2.44	−0.43	28.28	−0.17	0.15	−0.60
v_5	21.32	−0.92	0.08	−1.66	17.08	1.50	−0.17	1.67
v_6	4.05	−0.44	−0.87	−0.43	3.57	0.42	−0.04	4.50
v_7	4.25	−0.47	0.64	−0.64	3.10	−1.34	−1.68	−0.23
v_8	7.45	1.96	1.83	0.19	2.64	−0.64	−1.11	0.40
v_9	18.10	0.42	−0.05	−0.52	4.59	−1.25	−0.76	0.19
v_{10}	9.90	−0.28	−0.14	−0.55	5.29	0.77	0.87	1.27
Network	20.99	5.87	8.40	4.11	15.78	12.96	7.32	8.31

Fig. 5 shows the change from the value of d for each communication level for each node and network (bold blue line). In contrast to the premium, the relative percentage gets closer to 0 as the communication level network increases. The pattern is opposite to the premium in Fig. 3 and Fig. 4. Table 2 shows the percentage relative of adjustment price for the prism and Petersen topology.

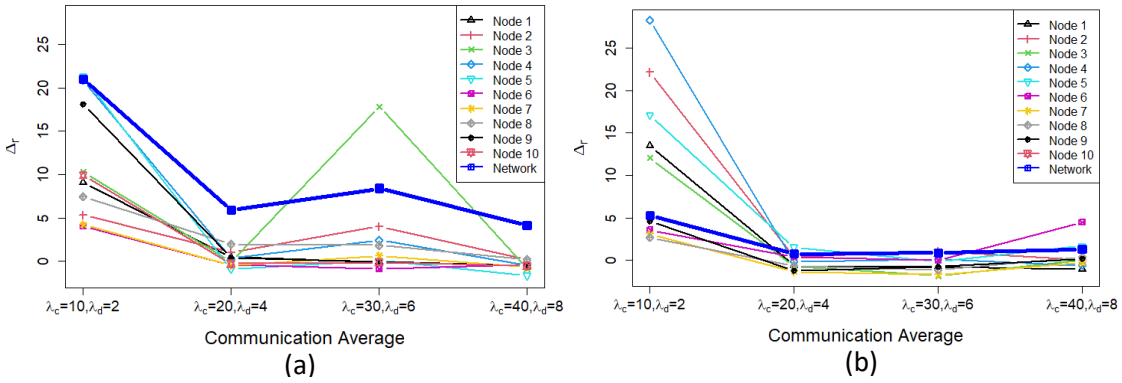

Fig. 5. Adjustment percentage Δ_r relative between initial premium and adjustment premium of every node and network for (a) prism topology and (b) Petersen topology.

A positive value shows that the initial premium is higher than the premium based on communication level. Conversely, a negative value indicates that the initial premium is lower than the premium based on communication level. The negative values ranged from 0.04% to 1.66%. This means that although some premium adjustments using communication level are higher than the initial premium, the value is not too different (it can still be considered equal). A positive value represents an interesting result. The initial premium of node 5 using the infection rate β_0 is 21.32% higher than the premium with low communication (λ_c = 10, λ_d = 2) in prism topology. The initial premium of node 4 is 28.28% higher than the premium with low communication (λ_c = 10, λ_d = 2). The relative percentage is close

to 0 for increasing communication. For one network, the initial premium for prism topology is 20.99% higher than the premium for low communication, 5.87% for medium communication, 8.40% for high communication, and 4.11% for very high communication. In the Petersen topology, the initial premium is 15.78% higher than the premium for low communication, 12.96% for medium communication, 7.32% for high communication, and 8.31% for very high communication. Thus, the premium can be adjusted according to the active level of the computer/server.

4. Conclusion

Cyberattacks have been a growing concern of researchers in recent years. From the design and topology evaluation side, it is necessary to consider the network security factor and topology robustness. We use two types of topologies offered by the graph theory approach: prism topology and Petersen topology. Because of the same characteristics, the vulnerability of the two networks is equal if all computers/servers and their contact types are set similarly. The simulation results with different communication levels show that a higher communication level network is more vulnerable. Thus, route optimization and network effectiveness need to consider the high risk of transmission. We have successfully introduced a method for adjusting the premium based on communication level. This is based on cybersecurity factors where high communication causes a high risk of transmission. For comparison purposes, the simulation considers four communication levels: low (λ_c = 10, λ_d = 2), medium (λ_c = 20 λ_d = 4), high (λ_c = 30, λ_d = 6), and very high (λ_c = 40, λ_d = 8). The simulation results show that the premium price can be adjusted based on frequency in a communication network. To measure the amount of adjustment, we use the relative percentages metric. At a low level, the premium price from a node can reach 28.28% lower than the initial premium, and the network premium is 20.99% lower than the initial network premium. These results can answer the challenge of high cyber insurance prices by adjusting premiums. From a practical perspective, this method can apply using network traffic or network flow data.

Acknowledgment

This work was fully supported by funding from the National Agency for Research and Innovation of the Republic of Indonesia under research grant No. 2/E1/KP.PTNBH/2020. YA would like to thank the Ministry of Education and Culture of the Republic of Indonesia for the full financial support through the PMDSU scholarship.

Declarations

Author contribution. All authors contributed equally to the main contributor to this paper. All authors read and approved the final paper.
Funding statement. This work was fully supported by funding from the National Agency for Research and Innovation of the Republic of Indonesia under research grant No. 2/E1/KP.PTNBH/2020.
Conflict of interest. The authors declare no conflict of interest.
Additional information. No additional information is available for this paper.

References

[1] M. F. Carfora, F. Martinelli, F. Mercaldo, A. Orlando, and A. Yautsiukhin, "Cyber Risk Management: A New Challenge for Actuarial Mathematics," 2018, doi: 10.1007/978-3-319-89824-7_36.

[2] S. Rass, S. Schauer, S. König, and Q. Zhu, "Insurance," 2020, pp. 137–158, doi: 10.1007/978-3-030-46908-5_7.

[3] M. F. Carfora, F. Martinelli, F. Mercaldo, and A. Orlando, "Cyber risk management: An actuarial point of view," *J. Oper. Risk*, 2019, doi: 10.21314/JOP.2019.231.

[4] P. Dreyer *et al.*, *Estimating the Global Cost of Cyber Risk: Methodology and Examples*, 2018, doi: 10.7249/rr2299.

[5] S. Morgan, "2019 Official Annual Cybercrime Report," *2019 Rep. by Cybersecurity Ventur. Spons. by Herjavec Gr.*, 2019. Available at: Google Scholar.

[6] S. Dambra, L. Bilge, and D. Balzarotti, "SoK: Cyber Insurance – Technical Challenges and a System Security Roadmap," 2020, doi: 10.1109/sp40000.2020.00019.

[7] A. Marotta, F. Martinelli, S. Nanni, A. Orlando, and A. Yautsiukhin, "Cyber-insurance survey," 2017, doi: 10.1016/j.cosrev.2017.01.001.

[8] M. Eling and N. Loperfido, "Data breaches: Goodness of fit, pricing, and risk measurement," *Insur. Math. Econ.*, 2017, doi: 10.1016/j.insmatheco.2017.05.008.

[9] S. Romanosky, L. Ablon, A. Kuehn, and T. Jones, "Content analysis of cyber insurance policies: How do carriers price cyber risk?," *J. Cybersecurity*, 2019, doi: 10.1093/cybsec/tyz002.

[10] M. Xu and L. Hua, "Cybersecurity Insurance: Modeling and Pricing," *North Am. Actuar. J.*, vol. 23, no. 2, pp. 220–249, Apr. 2019, doi: 10.1080/10920277.2019.1566076.

[11] M. A. Fahrenwaldt, S. Weber, and K. Weske, "Pricing of cyber insurance contracts in a network model," *ASTIN Bull.*, 2018, doi: 10.1017/asb.2018.23.

[12] S. W. Indratno and Y. Antonio, "A Gillespie Algorithm and Upper Bound of Infection Mean on Finite Network," in *Communications in Computer and Information Science*, 2019, doi: 10.1007/978-981-15-0399-3_29.

[13] Y. Antonio and S. W. Indratno, "Cyber Insurance Rate Making Based on Markov Model for Regular Networks Topology," *J. Phys. Conf. Ser.*, vol. 1752, no. 1, p. 012002, Feb. 2021, doi: 10.1088/1742-6596/1752/1/012002.

[14] Y. Antonio, S. W. Indratno, and S. W. Saputro, "Pricing of cyber insurance premiums using a Markov-based dynamic model with clustering structure," *PLoS One*, vol. 16, no. 10, p. e0258867, Oct. 2021, doi: 10.1371/journal.pone.0258867.

[15] L. Wang and R. Jones, "Big Data Analytics in Cyber Security: Network Traffic and Attacks," *J. Comput. Inf. Syst.*, pp. 1–8, Jan. 2020, doi: 10.1080/08874417.2019.1688731.

[16] Q. A. A. Ruhimat, G. W. Fajariyanto, D. M. Firmansyah, and Slamin, "Optimal computer network based on graph topology model," *J. Phys. Conf. Ser.*, vol. 1211, p. 012007, Apr. 2019, doi: 10.1088/1742-6596/1211/1/012007.

[17] T. Raeder and N. V. Chawla, "Market basket analysis with networks," *Soc. Netw. Anal. Min.*, vol. 1, no. 2, pp. 97–113, Apr. 2011, doi: 10.1007/s13278-010-0003-7.

[18] N. Adhikari, A. Singh, and N. K. Swain, "Reliable, Effective and Fault-Tolerant Design of Leafy Cube Interconnection Network Topology," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 12, pp. 3163–3170, Oct. 2019, doi: 10.35940/ijitee.L2707.1081219.

[19] A. H. Mousa, N. T. Mohammed, and E. A. Mohammed, "EFCNT: An evaluation framework for computer's network topologies," 2019, p. 050010, doi: 10.1063/1.5123126.

[20] B. Elshqeirat, S. Soh, S. Rai, and S. Manaseer, "On Maximizing Reliability of Network Topology Design Using a Practical Dynamic Programming Approach," *Mod. Appl. Sci.*, vol. 12, no. 12, p. 163, Nov. 2018, doi: 10.5539/mas.v12n12p163.

[21] A. B. Khedkar and V. L. Patil, "Computer Network Optimization Using Topology Modification," 2015, pp. 117–127, doi: 10.1007/978-3-319-11227-5_11.

[22] J. M. Kizza, *Guide to Computer Network Security*, 2017, doi: 10.1007/978-3-319-55606-2.

[23] Q. A. A. Ruhimat, G. W. Fajariyanto, D. M. Firmansyah, and Slamin, "Optimal computer network based on graph topology model," *J. Phys. Conf. Ser.*, vol. 1211, no. 1, p. 012007, Apr. 2019, doi: 10.1088/1742-6596/1211/1/012007.

[24] G. A. Schwartz and S. S. Sastry, "Cyber-insurance framework for large scale interdependent networks," in *HiCoNS 2014 - Proceedings of the 3rd International Conference on High Confidence Networked Systems (Part of CPS Week)*, 2014, doi: 10.1145/2566468.2566481.

[25] I. F. Videla-Cavieres and S. A. Ríos, "Extending market basket analysis with graph mining techniques: A real case," *Expert Syst. Appl.*, vol. 41, no. 4, pp. 1928–1936, Mar. 2014, doi: 10.1016/j.eswa.2013.08.088.

[26] B. Nguyen, "Modelling Cyber Vulnerability using Epidemic Models," in *Proceedings of the 7th International Conference on Simulation and Modeling Methodologies, Technologies and Applications*, 2017, pp. 232–239, doi: 10.5220/0006401902320239.

[27] S. W. Indratno and Y. Antonio, *A Gillespie Algorithm and Upper Bound of Infection Mean on Finite Network*, 2019, vol. 1100, doi: 10.1007/978-981-15-0399-3_29.

[28] M. Xu and L. Hua, "Cybersecurity Insurance: Modeling and Pricing," *North Am. Actuar. J.*, 2019, doi: 10.1080/10920277.2019.1566076.

[29] P. Van Mieghem and E. Cator, "Epidemics in networks with nodal self-infection and the epidemic threshold," *Phys. Rev. E*, vol. 86, no. 1, p. 016116, Jul. 2012, doi: 10.1103/PhysRevE.86.016116.

[30] P. Van Mieghem and J. Omic, "In-homogeneous Virus Spread in Networks," Jun. 2013. Available at: Google Scholar.

[31] F. Harary, *Graph theory*, 2018, doi: 10.1201/9780429493768.

[32] J. O. Bennett and W. L. Briggs, *Using & Understanding Mathematics: A Quantitative Reasoning Approach*, 7th Editio. Pearson, 2018. Available at: Google Scholar.

[33] S. A. Klugman, H. H. Panjer, and G. E. Willmot, *Loss Models?: From Data to Decisions*, 5th edition. John Wiley and Sons, Inc., 2019. Available at: Google Books.