Cyber Insurance Rate Making Based on Markov Model for Regular Networks Topology

Y Antonio and S W Indratno

1 Statistics Research Division, Faculty of Mathematics and Natural Sciences, Institut Teknologi Bandung, Center for Advanced Sciences Building, Bandung 40132, Indonesia.

*e-mail : yeftanus@students.itb.ac.id

Abstract. Computers and Internet play a key role in the processes of data transaction, data exchange and data storage in a business. Malicious software or computer viruses is one of the biggest threats that can attack computer networks and cause huge losses due to loss of data and information. As a way to transfer risk, cyber insurance requires precise and appropriate calculations even though many challenges are faced including the effects of differences in network structure. Standards of cyber insurance that have not been established as in the mortality table for life insurance open the possibility to set a standard calculation based on network structure by determining cyber insurance rates. This study uses a general susceptible-infectious-susceptible model with Markovian property to simulate the process of spreading computer virus and calculate the total loss for each computer. Rate making will consider the number of infected neighbours on a node as an exposure to set insurance rates on regular network topology. The simulation process shows that the rates at each node are affected by the probability of initial infection, the degree of each node on the network, and the parameters of infection or recovery.

Keywords: Cyber Insurance Rate, Markov Model, Networks Topology

1. Introduction

The development of Industry 4.0 has pushed the integration of automation technology and cyber technology. Data storage, exchange, analysis and collection take place in a single interconnected network that has a significant impact on company profits [1]. This revolution is not without risk. Cyber attacks such as denial of service, data theft, malicious software, extortion, and other types of crime can occur on computer networks and cause substantial financial losses. The World Economic Forum issued a global risk report in 2019 and placed cyber attacks in the second of the top ten risks by interconnection [2]. In the past two years, computer virus or malicious software attacks have become one of the biggest cyber attacks. The WannaCry ransomware attack has spread and quickly spread in 150 countries and infected more than 230,000 computers in May 2017. This attack caused a loss of around 1.5 billion to 3 billion U.S. Dollar. One year later, the Taiwan Semiconductor Manufacturing Co. (TSMC) company that supplies iPhone core processors was also attacked by a virus which caused 80% of virus-infected equipment. Losses due to this infection are estimated at 255 million U.S. Dollar.

Large losses on a company caused by cyber attacks require a risk management strategy that can be played by cyber insurance [3–5]. Security measures and standards, changes in attack patterns, data availability, dependence on network structure, and other issues related to complexity in calculating...
premiums are challenges for determining cyber insurance [6]. Xu and Hua have made important discoveries for modeling and pricing cyber insurance by considering the Markov and non-Markov epidemic models with independent assumptions then modeling dependences between nodes using copula [7]. It was using epidemic models at the node level [8] and doing simulations to obtain premiums for each node and whole network. Premium prices obtained through the simulation are strongly influenced by the network structure, so it is interesting to study the case for a company that uses a regular network topology. The term regular network is taken from a graph theory called "regular graph" [9] where every node on the regular network has the same degree. Two common types of regular network topology in computer network systems are mesh topology and ring topology [10].

This study will compare the upper bound of generalized epidemic SIS model (ε-SIS) [11] and the upper bound obtained by reducing the Kolmogorov differential equation system to a single equation form using the assumption of node homogeneity in the regular graph [8]. Generalized SIS model is derived from the SIS model by adding the assumption that attacks from outside the network can cause infection. the simulation is done differently by entering the exposure effect for rate making which explains a quantity that corresponds to the risk of the policyholder [12].

This article was compiled with the following organization. Section 2 discusses the upper limit of the Markov model and its reduction in regular graphs and numerical studies as a comparison. The discussion of risk and exposure models used is in section 3. The simulation and calculation will be carried out in section 4. The last part is the conclusion and discussion.

2. Upper bound for regular networks

We will build ε-SIS model on computer networks to explain the transmission of viruses through connection between computers in the following section. Analysis of this model on network topology or as a mathematical object known as a graph makes it possible to study the effects of topology against the virus propagation process [13]. Suppose a undirect graph \( \Gamma = (\mathcal{N}, \mathcal{L}) \) where \( \mathcal{N} \) is a set of nodes and \( \mathcal{L} \) is a set of links or edges that represent the regular network in a company. Nodes represent computers and edges represent communication between computers in a network. For any \( x \in \mathcal{N} \) and \( y \in \mathcal{N} \) in the graph \( \Gamma \) are connected if \( (x, y) \in \mathcal{L} \) which means that the node can attack each other. In this case, the regular network shows a class of networks with \( \text{deg}(x) = \text{deg}(y) \) for all \( x, y \in \mathcal{N} \) where \( \text{deg}(x) \) is the degree of node \( x \) (the number of nodes connected to node \( x \)). The total number of nodes on the network \( \mathcal{N} \) is denoted by the cardinality of \( \mathcal{N} \) i.e. \( |\mathcal{N}| \). Adjacency matrix \( A \) is a matrix that describes a network that is a square matrix with entries

\[
a_{xy} = \begin{cases} 
1, & \text{if } (x, y) \in \mathcal{L} \\
0, & \text{if } (x, y) \notin \mathcal{L}.
\end{cases}
\]  

Figure 1. Regular network topology with degrees \( \xi \) from top left to bottom right for \( \xi = 2,3,4,5,6,7 \).
Matrix $A$ explains the relationship to a graph $\Gamma_\xi$ with the total of each row will be equal to $\xi$ which is the degree of a regular graph. Suppose a company has eight computers and wants to know if it is connected to a regular network whether there is an effect of the degree at each node on the spread of the virus or not. The following discussion will consider eight $\xi$-regular networks where $\xi = 2,3,4,5,6,7$ as in Figure 1(a)-1(f). The graph provides topology for Figure 1(a) is regular network with $\xi=2$. Figure 1(b) is regular network with $\xi=3$, and so on up to Figure 1(f) is regular network with $\xi=7$. The figure also shows that the network 1(a) is the ring topology class and network 1(f) is the mesh topology (fully connected network) class [10].

The $\epsilon$-SIS model assumes two threats faced by each node, they are threats caused by accessing dangerous sites via the internet or receiving e-mails containing worms called as pull-based attack (self-infection) and threats caused by infected neighbours attacking the node called as push-based attack (link-infection). Infected nodes can be recovered or cleaned and returned to safe status. Consider Bernoulli random variables $I_x(t)$ with two states at time $t$ namely $I_x(t) = 1$ if computer $x$ is infected and $I_x(t) = 0$ if computer $x$ is vulnerable. At the time of $t$, each node can be infected with probability $p_x(t) = P(I_x(t) = 1)$ and vulnerable with probability $1 - p_x(t) = P(I_x(t) = 0)$. Infection process from neighbours, self-infection process, and recovery process follows a homogeneous Poisson process with the rate $\beta$ per link of infected neighbours, $\epsilon$, and $\gamma$ are assume same for every node. Transition probability in short interval of time $h$ can be written as

$$p_{x,ij}(h) = P(I_x(t+h) = j|I_x(t) = i) = \{\beta \sum_{z=1}^{N} a_{xz} I_z(t) + \epsilon\} h + o(h); \quad i = 0, j = 1$$

where the infection rate depends on connection and infection status of the neighbour of node $x$. Equation (2)-(3) can be used to generate the probability in time $t + h$ and it follows

$$P(I_x(t+h) = 1|I_x(t)) = (1 - I_x(t))(\beta \sum_{z=1}^{N} a_{xz} I_z(t) + \epsilon) h + I_x(t)(1 - \gamma h) + o(h).$$

Variable $I_x(t)$ is a Bernoulli random variable implied the conditional probability can be express as conditional expectation. By the law of total expectation [14], the dynamic of expectation holds

$$\frac{dE[I_x(t)]}{dt} = \beta \sum_{z=1}^{N} a_{xz} E[I_z(t)] + \epsilon - (\epsilon + \gamma) E[I_x(t)] - \beta \sum_{z=1}^{N} a_{xz} E[I_x(t)I_z(t)].$$

Term in right side cannot be derived by direct method. So, the information about $E[I_x(t)I_z(t)]$ is needed. Cator was proof that a couple of node are non-negatively correlated [15] or using mathematical formula $E[I_x(t)I_z(t)] \geq E[I_x(t)]E[I_z(t)]$ then equation (4) changes to inequality

$$\frac{dp_x(t)}{dt} \leq \beta \sum_{z=1}^{N} a_{xz} p_z(t) + \epsilon - (\epsilon + \gamma) p_x(t) - \beta \sum_{z=1}^{N} a_{xz} p_x(t)p_z(t).$$

The upper bound for the probability of infection is obtained by solving the differential equation (5) generates the following Theorem

**Theorem 2.1.** Let $Q = \beta diag \left( \frac{\gamma}{\gamma + \epsilon} \right) A - diag(\epsilon + \gamma)$ and for an exponential matrix $e^{Qt} = \sum_{k=1}^{\infty} \frac{Q^t k}{k!}$

The dynamic upper bound for the infection probability is given by

$$\bar{p}(t) = e^{Qt}\bar{p}(0) + Q^{-1}[e^{Qt} - I]\epsilon$$

where $\bar{p}(0)$ is the initial infection probability and $\epsilon$ is the $N$-dimensional column vector with same entries $\epsilon$. 

---
**Proof.** Transforming equation (5) to vector and matrix form and taking the upper bound of matrix equation then it is become non-homogeneous differential equation. Using the integration factor \( u(t) = e^{-\int q \, dt} \) for solve the matrix equation and finally equation (6) is hold. For complete proof see [7].

Assume that every computer is identical so for every \( t \) and every \( x = 1, 2, \ldots, N \) applies \( p_x(t) = p_y(t) \). Thus, for regular graphs \( \Gamma_x \) with degrees \( \xi \), part \( \sum_{z=1}^{N} a_{xz} p_x(t) \) of equation (5) can be written as \( \xi p_x(t) \) based on the property of regular graph where each node always has the same number of neighbors. The inequality system (5) can be reduced to one differential equation for all nodes and carries to the upper bound theorem for regular graphs.

**Theorem 2.2.** Suppose \( \xi \) is the degree of a regular graph, assuming that each computer is identical so \( p_x(t) = p_y(t) \) for all \( x, t \), then the dynamic upper bound for infection probability for each node is

\[
p_x(t) = \frac{\tanh\left(\frac{t\sqrt{\phi^2 + 4\beta^*\varepsilon}}{2} - \arctanh\left(\frac{-2p_x(0)\beta^* + \phi}{\sqrt{\phi^2 + 4\beta^*\varepsilon}}\right)\right)\sqrt{\phi^2 + 4\beta^*\varepsilon} + \phi}{2\beta^*}
\]

where \( \phi = \beta^* - \varepsilon - \gamma \) and \( \beta^* = \beta \xi \).

**Proof.** Assume that all computers are identical. So, equation (5) can be reduced to the following form

\[
p_x'(t) = \beta \xi p_x(t)(1 - p_x(t)) - (\varepsilon + \gamma)p_x(t) + \varepsilon.
\]

Let \( \phi = \beta^* - \varepsilon - \gamma \) and \( \beta^* = \beta \xi \). Equation (8) can be separated into

\[
\frac{dp_x(t)}{\phi p_x(t) - \beta^* p_x(t)^2 + \varepsilon} = dt
\]

Quadratic equation (9) has two roots \( p_x(1) = \frac{\phi - \sqrt{\phi^2 + 4\beta^*\varepsilon}}{2\beta^*} \) and \( p_x(2) = \frac{\phi + \sqrt{\phi^2 + 4\beta^*\varepsilon}}{2\beta^*} \). The use of algebraic manipulation and integration of \( p_x(t) \) gives the following equation

\[
\frac{1}{2}\ln\left(1 + \frac{-2p_x(t)\beta^* + \phi}{\sqrt{\phi^2 + 4\beta^*\varepsilon}}\right) - \frac{\sqrt{\phi^2 + 4\beta^*\varepsilon}}{2} + C = \frac{1}{2}\ln\left(\frac{1 + \sqrt{1 + \phi^2 + 4\beta^*\varepsilon}}{1 - \sqrt{1 + \phi^2 + 4\beta^*\varepsilon}}\right)
\]

Defining an inverse hyperbolic tangent function \( \text{arctanh}(x) = \frac{1}{2}\ln\left(\frac{1 + x}{1 - x}\right) \), then \( C \) in equation (10) can be obtained \( C = \text{arctanh}\left(\frac{-2p_x(t)\beta^* + \phi}{\sqrt{\phi^2 + 4\beta^*\varepsilon}}\right) \). By substitution and forming \( p_v(t) \) we have obtained equation (7).

The next discussion will show a numerical comparison of the upper bounds on Theorem 2.1 and Theorem 2.2 by generated the upper bounds of infection probability and parameter sensitivity.
2.1. Parameter Sensitivity

Before doing numerical analysis and rate making, it is necessary to analyse the sensitivity of the parameters. The beta parameter value will be selected so that the infection probability does not exceed one. Consider two possibilities of $\gamma$ values are equal to 1 or 1.5 which means the average time taken to repair a node is one day or 16 hours. Then also two possibilities of $\varepsilon$ values are equal to 0.1 or 0.25 which means on average, one in ten computers is infected or 25 out of one hundred computers are infected per day. The $\beta$ parameter will be run for network topology in Figure 1 until it reaches the infection probability is equal to one.

![Graphs showing sensitivity of $\beta$ parameter in the regular topology.]

(a) $\varepsilon=0.1$ and $\gamma = 1$
(b) $\varepsilon=0.25$ and $\gamma=1$
(c) $\varepsilon=0.1$ and $\gamma = 1.5$
(d) $\varepsilon=0.25$ and $\gamma=1.5$

Figure 2. Sensitivity of $\beta$ parameter in the regular topology with degrees $\xi=2,\ldots,7$ of Theorem 1.

Figure 2(a) -2(d) gives the sensitivity of $\beta$ so the infection probability does not exceed 1. Consider figures 2(a) versus 2(b) and 2(c) versus 2(d) with $\gamma=1$ or 1.5 which explains the effect of the increase parameter $\varepsilon$ makes the infection probability more slowly for $\varepsilon=0.25$ than $\varepsilon=0.1$ to reach the value of $\beta$ equal to one. In other words, the $\beta$ parameter that can be used is greater for the value $\varepsilon=0.25$ than $\varepsilon=0.1$. When the $\gamma$ parameter is enlarged, the beta parameter rises more slowly for $\gamma=1.5$ than $\gamma=1$. Thus the $\beta$ parameter that can be used for $\gamma=1.5$ is greater than $\gamma=1$. This section only discusses parameter sensitivity for $\beta$ in Theorem 2.1 to bring the comparison of Theorem 2.1. and Theorem 2.2 in the next section.

2.2. Numerical Study of Upper Bounds

In this section, numerical studies will be conducted to compare the upper bound of Theorem 2.1. and the upper bound of theorem 2.2. to obtain the upper bounds for regular networks. Consider the networks provided by Figure 1.
Figure 3. Upper bounds of Theorem 2.1 and Theorem 2.2.

Upper bounds for infection probability with networks topology defined in Figure 1 generated by Theorem 2.1 and Theorem 2.2 is shown in Figure 3. It can be obtained that theorem 2.2 gives the upper bounds with a smaller value than Theorem 2.1. The effect of degrees on regular topology uses theorem 2.1. yields the same distance compared to using Theorem 2.2., which is greater infection probability for a large degree $\xi$ than a small degree $\xi$. The enlarged of $\beta$ and $\varepsilon$ parameters also provide an higher upper bounds of stationary infection probability.

3. Risk model
Suppose an infection in node $x$ results in two types of losses. The first loss caused by information loss, data damage, scattered privacy, and deletion of licenses. The second loss is caused by a computer does not operate within a certain time because it requires repairs. Let $\ell_{x(i)}$ declare $i$-th loss due to loss of information of node $x$. The cost function of this loss is explained by $\mu_x(\ell_{x(i)})$. The second loss related to the length of time to recovery is modelled by the cost function $\xi_x(\mathcal{R}_{x(i)})$, where $\mathcal{R}_{x(i)}$ is the length of time to recovery. Losses of node $x$ up to one year of contract (365 days) are represented as

$$s_x(365) = \sum_{i=1}^{M_x(365)} \left( \mu_x(\ell_{x(i)}) + \xi_x(\mathcal{R}_{x(i)}) \right)$$
Total of losses faced by a network during one-year contract period are notated as follows

\[ S(365) = \sum_{x=1}^{N} s_x(365) = \sum_{x=1}^{N} \sum_{i=1}^{M_x(365)} \left( \mu_x(\ell_x(i)) + \zeta_x(R_x(i)) \right) \]

where \( M_x(365) \) is the number of infections from node \( x \) for 365 days.

Assume that the wealth of a computer \( x \) is \( \omega_x \) and it is assumed that the loss follow Generalized Beta distribution with density function is defined as

\[ f_{\mu_x}(u) = \frac{1}{\omega_x^{ac+b+c-1}} \frac{1}{B(a,b)} u^{ac-1} (\omega_x - u)^{c(b-1)}; 0 < u < \omega_x \]

where \( a, b, c > 0 \) are shape parameters and \( B \) is beta function. Cost function are defined as

\[ \mu_x(\ell_x(i)) = \alpha \ell \]
\[ \zeta_x(R_x(i)) = \alpha_2 \omega + \alpha_3 \tau \]

quadratic function explains the costs assumed to be a linear function of quadratic coefficient of loss for the cost of information loss and due to repair time.

As discussed earlier, the number of infected neighbours will be used as an exposure stating the quantity that corresponds to the risk of the policyholder. Rate is the premium of an insurance contract per unit of exposure which is a unit of measurement for pricing insurance. Rates will be calculated by considering the three premium principles. Three premium principles will be considered to rate making [16]. They are (1) expected value premium principle

\[ \mathcal{H}_1(U) = (1 + \lambda)E[U], \]

(2) standard deviation premium principle

\[ \mathcal{H}_2(U) = E[U] + \lambda \sqrt{Var(U)}, \]

and (3) variance premium principle

\[ \mathcal{H}_3(U) = E[U] + \lambda Var(U). \]

where \( \lambda \) is loading factor and \( U \) is the total loss.

Rate is the premium value divided by the exposure unit. Let \( \eta_x(i) \) is the number of neighbours of computer \( x \) that have been successfully infected at \( i \)-th event. Due to \( \eta_x(i) \) influences the risk of node \( x \) become infected, it is mean more neighbours of \( x \) are infected then the risk of \( x \) will increase. So, \( \eta_x(i) \) can be seen as a quantity corresponds to the risks faced by policyholders. Thus, for \( U=s_x(365) \) the rate is defined by

\[ \mathcal{R}_x(365) = \mathcal{H}_i \left( \sum_{i=1}^{M_x(365)} \left( \frac{\mu_x(\ell_x(i))}{\eta_x(i)} + \zeta_x(R_x(i)) \right) \right) \]

for \( i=1,2,3. \)

4. Simulation and rate making

The simulation will be carried out with the fact that the alternating renewal process with exponential distribution for all processes will give the same results of the \( \epsilon \)-SIS model (see [7,14]). Assume that
where $Y_{x_1}, Y_{x_2}, \ldots, Y_{x_{D_x}}$ are random variables of time to infection caused by link-infection of $x$ and $D_x = \sum_{z=1}^{N} a_{xz} l_z(t)$ with expectation equal to $E[D_x(t)] = \sum_{z=1}^{N} a_{xz} p_z(t)$. Random variable $O_x$ is the random variable of time taken for self-infection to occur and $R_x$ is random variable of time needed until computer $x$ recover. Define the random variable $T_x = \min(Y_{x_1}, Y_{x_2}, \ldots, Y_{x_{D_x}}, O_x)$ which is the time taken until the infection occurs on the computer $x$. Vector of random variable $(T_x, R_x)$ is assumed to have independent and identical distribution. It has been proven that this model will produce the same stationary probability as $\varepsilon$-SIS model [7]. The steps taken to conduct the simulation are

Step 1 Define the adjacency matrix $A$, network status and the length of the contract period $T = 365$ then determine the distribution of the recovery infection process and the loss function. The next step is done for $t \leq T$.

Step 2 Calculate the number of infected nodes $m$ at time $t$ by adding up the network status. Generate $r_1, r_2, \ldots, r_m$, random variable of recovery time based on the exponential distribution with mean equal to $\frac{1}{\gamma}$.

Step 3 Generate $y_{1x}, \ldots, y_{dx}$ and $a_x$ for every secure node $x$ based on exponential distribution with mean equal to $\frac{1}{\beta}$ and $\frac{1}{\varepsilon}$ where $d_x$ is obtained by multiplying the $x$-th row of matrix $A$ by the status vector.

Step 4 Determine $t_1 = \min\{r_1, \ldots, r_m, y_{1x}, \ldots, y_{dx}, a_x\}$ for $x = 1, \ldots, N$, where $t_1$ is the time of first event occurs.

Step 5 If $t_1$ equal to the infection time then change node status from 0 to 1 and calculate the loss divide by the number of infection neighbors of node $x$. If $t_1$ equal to the recovery time then change node status from 0 to 1 and calculate the loss.

Step 6 Return the time $t = t + t_1$ and vector status.

Step 7 Repeat Step 2- Step 6 until the number of simulations is met.

The simulation is carried out as much as 1000 times to get rate for each node per number of neighbours which are infected at time $t$. Consider the topology in Figure 1 with $\xi = 2, 3, 4, 7$ which will be simulated for rate making using the steps previously described. The vector of the loss function parameter is given by

$$\begin{bmatrix} a \\ b \\ c \\ a_1 \\ a_2 \\ a_x \end{bmatrix} = \begin{bmatrix} 2 \\ 4 \\ 0.8 \\ 0.96 \\ 0.25 \times 10^{-6} \\ 0.6 \times 10^{-4} \\ 1500 \end{bmatrix}$$

Table 1 and Table 2 shows the simulation results of rate making for regular graphs with $\xi = 2, 3, 4, 7$. The results indicate degrees of regular network affects the process of spreading virus. Networks with a degree $\xi = 2$ are infected with a smaller number for each node than for $\xi = 3$. Networks with a degree $\xi = 4$ are infected with a smaller number for each node than for $\xi = 7$. The resulting rate tends to be greater, especially seen in the total which is rate for whole network. Table 1 and Table 2 are done using the same parameters, the infection will increase if the degree of the regular graph also increases.
Table 1. Mean, standard deviation, minimum and maximum infection of each node and $E[U]$ using for regular network with $\xi = 2$ and $\xi = 3$

| Regular Graph $\xi = 2$ | Regular Graph $\xi = 3$ |
|--------------------------|--------------------------|
| Mean SD Min. Max.        | Mean SD Min. Max.        |
| $N_1$ 47.5 4.904646 41 56 | $N_1$ 56.5 4.326918 51 66 |
| $N_2$ 48.7 5.677441 41 59 | $N_2$ 55.9 6.62403 44 67 |
| $N_3$ 45.6 4.78876 37 52 | $N_3$ 58.8 6.214678 52 68 |
| $N_4$ 44.9 9.515485 23 56 | $N_4$ 53.4 4.299871 47 58 |
| $N_5$ 43.3 8.590046 30 56 | $N_5$ 55.8 5.138093 49 65 |
| $N_6$ 44.4 6.41526 32 53 | $N_6$ 54 5.416026 47 64 |
| $N_7$ 46.8 5.921712 36 55 | $N_7$ 55.9 6.75689 46 66 |
| $N_8$ 48 11.45038 30 70 | $N_8$ 53.9 6.419588 45 66 |

| $S_1$ 0.752294 0.417021 0.225869 1.528389 | $S_1$ 0.675277 0.31674 0.24675 1.344862 |
| $S_2$ 0.76131 0.60046 0.138281 2.142192 | $S_2$ 0.867462 0.556264 0.22503 2.068005 |
| $S_3$ 0.663281 0.41856 0.177731 1.563986 | $S_3$ 1.026143 0.467293 0.300079 1.873604 |
| $S_4$ 0.930536 0.70589 0.226879 2.027948 | $S_4$ 0.830266 0.52521 0.240892 1.836572 |
| $S_5$ 0.61474 0.351477 0.236866 1.253785 | $S_5$ 0.638612 0.245738 0.252052 1.007729 |
| $S_6$ 0.488892 0.361778 0.075778 1.133622 | $S_6$ 0.82406 0.619263 0.210265 2.1657 |
| $S_7$ 0.592231 0.417886 0.055558 1.283748 | $S_7$ 0.505731 0.348751 0.149399 1.287258 |
| $S_8$ 0.979401 0.614644 0.092043 1.882885 | $S_8$ 0.891913 0.75147 0.192171 2.631628 |
| $S$ 5.782685 1.668855 3.22036 9.046063 | $S$ 6.259464 1.179222 4.044552 7.842544 |

Table 2. Mean, standard deviation, minimum and maximum infection of each node and $E[U]$ for regular network with $\xi = 4$ and $\xi = 7$

| Regular Graph $\xi = 4$ | Regular Graph $\xi = 7$ |
|--------------------------|--------------------------|
| Mean SD Min. Max.        | Mean SD Min. Max.        |
| $N_1$ 67.3 7.334091 55 78 | $N_1$ 114.9 12.14221 97 134 |
| $N_2$ 63.5 9.395626 41 75 | $N_2$ 112.1 8.020114 99 125 |
| $N_3$ 68.6 6.850791 61 82 | $N_3$ 114.7 5.078276 108 121 |
| $N_4$ 69 8.02773 62 90 | $N_4$ 112.9 9.170605 99 130 |
| $N_5$ 69 8.628119 48 80 | $N_5$ 114.9 7.992358 104 130 |
| $N_6$ 65.9 9.550451 50 87 | $N_6$ 115.1 8.672434 104 127 |
| $N_7$ 66.6 7.07421 58 84 | $N_7$ 116.4 7.471427 107 128 |
| $N_8$ 64.9 5.279941 57 76 | $N_8$ 116.8 10.40085 101 133 |
| $S_1$ 0.993202 0.464185 0.212618 1.558594 | $S_1$ 0.889685 0.276355 0.501854 1.382017 |
| $S_2$ 0.884613 0.5459 0.315705 1.866712 | $S_2$ 0.825272 0.424498 0.2466 1.558682 |
| $S_3$ 0.902795 0.463855 0.432822 1.644805 | $S_3$ 0.921456 0.48042 0.220846 1.533954 |
| $S_4$ 0.800308 0.434256 0.210697 1.385468 | $S_4$ 0.993192 0.466331 0.276145 1.746096 |
| $S_5$ 0.733281 0.363477 0.176956 1.171913 | $S_5$ 0.648833 0.29662 0.200624 1.161648 |
| $S_6$ 0.763353 0.344936 0.364143 1.580813 | $S_6$ 0.914179 0.507129 0.496476 2.056068 |
| $S_7$ 0.921778 0.545988 0.297703 1.767436 | $S_7$ 1.151175 0.383084 0.662035 1.763226 |
| $S_8$ 0.643516 0.400891 0.055605 1.388219 | $S_8$ 1.028761 0.606052 0.2227 2.110484 |
| $S$ 6.642844 1.289279 5.004095 8.625717 | $S$ 7.372552 0.82361 6.256506 8.736649 |
Table 3. Rate making using three premium principles for $\xi = 2,3,4,7$.

|          | Regular Graph $\xi = 2$ | Regular Graph $\xi = 3$ | Regular Graph $\xi = 4$ | Regular Graph $\xi = 7$ |
|----------|-------------------------|-------------------------|-------------------------|-------------------------|
|          | $H1$ | $H2$ | $H3$ | $H1$ | $H2$ | $H3$ | $H1$ | $H2$ | $H3$ | $H1$ | $H2$ | $H3$ | $H1$ | $H2$ | $H3$ |
| $N_1$    | 0.87 | 0.81 | 0.78 | 0.78 | 0.72 | 0.69 | 1.18 | 1.06 | 1.03 | 1.04 | 0.93 | 0.90 |
| $N_2$    | 0.88 | 0.85 | 0.82 | 1.00 | 0.95 | 0.91 | 1.07 | 0.97 | 0.93 | 0.98 | 0.89 | 0.85 |
| $N_3$    | 0.76 | 0.73 | 0.69 | 1.18 | 1.10 | 1.06 | 1.08 | 0.97 | 0.94 | 1.10 | 0.99 | 0.96 |
| $N_4$    | 1.07 | 1.04 | 1.01 | 0.95 | 0.91 | 0.87 | 0.95 | 0.87 | 0.83 | 1.18 | 1.06 | 1.03 |
| $N_5$    | 0.71 | 0.67 | 0.63 | 0.73 | 0.68 | 0.65 | 0.87 | 0.79 | 0.75 | 0.76 | 0.69 | 0.66 |
| $N_6$    | 0.56 | 0.54 | 0.51 | 0.95 | 0.92 | 0.88 | 0.90 | 0.82 | 0.78 | 1.10 | 0.99 | 0.95 |
| $N_7$    | 0.68 | 0.65 | 0.62 | 0.58 | 0.56 | 0.52 | 1.11 | 1.00 | 0.97 | 1.35 | 1.21 | 1.17 |
| $N_8$    | 1.13 | 1.07 | 1.04 | 1.03 | 1.00 | 0.98 | 0.77 | 0.70 | 0.67 | 1.25 | 1.12 | 1.08 |
| Net.     | 6.65 | 6.03 | 6.20 | 7.20 | 6.44 | 6.47 | 7.93 | 6.84 | 6.89 | 8.60 | 7.50 | 7.47 |

Table 2 describes the results of the rate making for each graph topology using the principles of $H1$, $H2$ and $H3$ premiums for each node and the whole network. Based on the results from Table 2, the first premium principle gives the highest rate. As high as the degree in the network, all three networks produce a greater rate.

5. Conclusion

Modifications to the calculation of premiums by determining an exposure that can be obtained from simulations allow us to determine the rate. Regular network topology is one form of network topology that is interesting to study where mesh topology and ring topology are often used on computer networks. The degree of the regular network is very influential on the upper bounds of infection probability, the number of infections, and the rate making. This discussion still uses general assumptions. Thus, it can be developed through more specific assumptions regarding the different infection and recovery rates for each node and using an inhomogeneous Poisson process to accommodate time-dependent parameters.

Acknowledgments

This research has been fully supported by the funding scheme for master’s and doctor’s research programs (PMDSU) with contract number 262/SP2H/LT/DRPM/2019. We would like to thank the Ministry of Research, Technology and Higher Education for providing this grant.

References

[1] Nagy J, Oláh J, Erdei E, Máté D and Popp J 2018 The role and impact of industry 4.0 and the internet of things on the business strategy of the value chain-the case of hungary Sustain.
[2] WEF 2019 The Global Risks Report 2019 - World Economic Forum
[3] Ishikawa T and Sakurai K 2016 A study of security management with cyber insurance ACM IMCOM 2016: Proceedings of the 10th International Conference on Ubiquitous Information Management and Communication
[4] Elnagdy S A 2017 Cost Reduction Strategy for Cybersecurity Risk Management and Risk Transfer to Insurance in Financial Industry
[5] Bodin L D, Gordon L A, Loeb M P and Wang A 2018 Cybersecurity insurance and risk-sharing J. Account. Public Policy 37 527–44
[6] Marotta A, Martinelli F, Nanni S, Orlando A and Yautsiukhin A 2017 Cyber-insurance survey Comput. Sci. Rev.
[7] Xu M and Hua L 2019 Cybersecurity Insurance: Modeling and Pricing North Am. Actuar. J.
[8] Van Mieghem P, Omic J and Kooij R 2009 Virus spread in networks IEEE/ACM Trans. Netw.
171–14

[9] Diestel R 2017 *Graph Theory* vol 173

[10] Tanenbaum A S and Wetherall D J 2011 *Computer Networks, 5th Edition* vol 52

[11] Van Mieghem P and Cator E 2012 Epidemics in networks with nodal self-infection and the epidemic threshold *Phys. Rev. E - Stat. Nonlinear, Soft Matter Phys.* 86

[12] Gray R J and Pitts S M 2012 Risk modelling in general insurance: From principles to practice

[13] Van Mieghem P 2010 Performance analysis of complex networks and systems

[14] Ross S M 2009 *Introduction to Probability Models: Tenth Edition*

[15] Cator E and Van Mieghem P 2014 Nodal infection in Markovian susceptible-infected-susceptible and susceptible-infected-removed epidemics on networks are non-negatively correlated *Phys. Rev. E - Stat. Nonlinear, Soft Matter Phys.*

[16] Tse Y K 2009 *Nonlife actuarial models: Theory, methods and evaluation*