

BAB I

PENDAHULUAN

1.1 Latar Belakang

Wireless Sensor Network (WSN) merupakan suatu perangkat sistem yang di dalamnya terdapat banyak *sensor node (SNs)* yang berfungsi sebagai penangkap informasi dan data yang dilengkapi dengan peralatan sistem komunikasi yang terkoneksi dengan jaringan internet **(Batista dkk., 2020)**. *WSN* telah digunakan dalam berbagai aspek kehidupan seperti pada sektor kesehatan, pertanian, keamanan, militer, industri dan lain-lain. Mencakup berbagai aplikasi di era ini termasuk jaringan kontrol industri, perawatan kesehatan, sensor bencana alam, aplikasi di bidang militer, pemantauan produksi *real-time*, dan lain sebagainya **(Babbar dan Rani, 2020)**.

Pengguna *WSN* mengalami berbagai ancaman dalam penggunaan perangkat tersebut, seperti serangan *malware* yang dapat merusak sistem keamanan dan data dari perangkat *WSN*. *Malware* atau *malicious software* adalah suatu program yang dirancang untuk mengganggu sistem operasi dari sebuah perangkat yang menjadi target ancamannya. Serangan *malware* dapat menyebabkan kebocoran data, kerusakan sistem, kerugian finansial, kebocoran privasi, penyalahgunaan sumber daya, dan kerusakan lainnya pada sistem-sistem yang menjadi target ancamannya **(Gao dan Zhuang, 2019)**.

Beberapa tahun terakhir, penyebaran *malware* melalui perangkat *WSN* mendapat perhatian lebih karena pemanfaatan *Internet of Things (IoT)* di era ini menjadi hal yang mudah ditemui di kehidupan sehari-hari. Telah banyak penelitian yang dikembangkan untuk mendeteksi penyebaran *malware* pada perangkat *WSN*, salah satunya pada perangkat yang terkoneksi dengan jaringan internet maupun *cloud server* yang mengakibatkan penyebaran *malware* secara cepat menjadi ancaman serius terhadap keamanan jaringan secara luas. Banyaknya serangan *malware* jauh lebih besar dapat terjadi jika berada dalam domain yang lebih luas, seperti *malware* pada *sensor node*

dapat menyebar melalui susunan kerapatan *node* dan melalui *sink node*, *malware* dapat merusak informasi dan data yang dikirimkan ke komputer melalui jaringan internet (Khanh, 2016).

Berdasarkan laporan pemantauan oleh *U.S. Cybersecurity and Infrastructure Security Agency (CISA)* sebanyak 69% dari semua serangan *malware* pada perangkat *WSN* yang menargetkan organisasi melibatkan distributor *malware* melonjak 30% dibandingkan kuartal yang sama di tahun 2020. Pada tahun 2021, peneliti OTORIO menemukan total 13 kerentanan di *router* IR615. Daftar ini mencakup pemalsuan permintaan lintas situs (*CSRF*), eksekusi kode jarak jauh, injeksi perintah, dan masalah kebijakan kata sandi yang lemah, serta otorisasi yang tidak tepat dan kerentanan skrip lintas situs (*XSS*) yang sangat parah. Volume serangan manipulasi yang menargetkan sistem juga meningkat dari 36% di kuartal pertama 2021 menjadi 53% di kuartal kedua 2021 (CISA, 2021).

Berdasarkan tingginya angka serangan *malware* yang terjadi, berbagai bidang keilmuan tertarik untuk mempelajari penyebaran *malware* dan perawatan untuk mengurangi dampak kerusakan dari *malware* tersebut. Salah satunya pada bidang matematika, yaitu dengan pendekatan model matematika. Perkembangan model matematika penyebaran *malware* pada perangkat *WSN* telah banyak dilakukan oleh peneliti. Rey, dkk. (2017) telah mengembangkan model penyebaran *malware* pada perangkat *WSN* dalam lima kompartemen *Susceptible-Carrier-Infectious-Recovered-Susceptible* (SCIRS). Perangkat pembawa (*carrier*) yaitu populasi yang terinfeksi namun dalam kondisi laten karena adanya antivirus dan perangkat sembuh, pada model ini juga memperhatikan tingkat penurunan sistem pertahanan yang mengakibatkan terjadinya serangan ulang *malware*. Acarali, dkk. (2019) mengembangkan model penyebaran *malware* pada perangkat *WSN*, model dalam bentuk *Susceptible-Infected-Susceptible* (SIS) dengan memberikan kontrol berupa *scanning* untuk keberadaan *malware* pada sistem. Selanjutnya, Gao dan Zhuang (2019) mengembangkan sebuah penelitian tentang penyebaran *malware* untuk perangkat yang terkoneksi dengan

internet dalam bentuk *Vulnerable-Exposed-Infectious-Quarantined-Secured* (VEIQS). Dalam model tersebut digunakan interaksi *saturated incidence rate* dan penambahan kontrol berupa vaksinasi serta karantina untuk perangkat yang terinfeksi *malware*. **Ojha, dkk. (2020)** juga mengembangkan model matematika penyebaran *malware* dengan memperhatikan pengaruh karantina untuk *nodes* yang terinfeksi dan pengaruh sistem yang telah terprogram antivirus dalam bentuk *Susceptible-Exposed-Infectious-Quarantined-Recovered-Vaccinated* (SEIQRV). Model ini juga memperhatikan kerapatan susunan *node* pada perangkat *WSN* yang mempengaruhi tingkat penyebaran *malware*. **Hu, dkk. (2021)** mengembangkan penelitian mereka mengenai penyebaran *malware* pada perangkat yang terkoneksi dengan jaringan Wi-Fi ke dalam bentuk *Susceptible-Exposed-Infectious-Quarantined-Recovered* (SEIQR) dengan menggunakan interaksi *saturated incidence rate* dan strategi kontrol optimal berupa efek penghambatan terhadap serangan *malware*.

Dari penelitian yang dikembangkan oleh beberapa ilmuwan di atas, umumnya belum ada yang mengkaji model penyebaran *malware* dengan memperhatikan sistem pertahanan yang terbentuk setelah serangan ulang *malware*. Pada model yang dikembangkan oleh **Ye, dkk. (2021)** dibahas model matematika penyebaran *malware* pada perangkat *WSN* dengan memperhatikan sistem pertahanan yang terbentuk setelah serangan *malware* yang sama untuk kedua kalinya dalam bentuk *Susceptible-Infectious-Basically Recovered-Completely Recovered* (SIR_1R_2). *SNs* yang telah terinfeksi dan dapat sembuh diasumsikan memiliki pertahanan dasar dalam melawan serangan ulang untuk jenis *malware* yang sama. Namun *SNs* ini tidak memiliki pertahanan untuk *malware* jenis baru.

Penulis melakukan modifikasi model penyebaran *malware* yang dikembangkan oleh **Ye, dkk. (2021)** dengan menambahkan kompartemen Q (*Quarantined*) sebagai upaya penyembuhan *SNs* yang terinfeksi dengan cara memisahkan *SNs* sehingga tidak melakukan komunikasi lebih lanjut dengan populasi yang lain dan mengubah interaksi *bilinier incidence rate* menjadi *saturated incidence rate*. Modifikasi ini didasari pada

jumlah penyebaran serangan *malware* yang tinggi dikarenakan tingkat pertahanan cukup rendah. *Saturated incidence rate* memperhatikan efek jenuh perangkat terinfeksi, ketika jumlah perangkat terinfeksi semakin meningkat, maka perangkat tersebut akan di isolasi dari jaringannya dan dilakukan karantina sehingga perangkat sehat tidak mudah tertular. Penulis juga menambahkan variabel kontrol berupa pemasangan antivirus dan reparasi *node* untuk perangkat yang terinfeksi.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka rumusan masalah yang akan dibahas dalam penulisan ini adalah sebagai berikut:

1. Bagaimana analisis kestabilan titik setimbang dari hasil modifikasi model matematika penyebaran *malware* pada perangkat *Wireless Sensor Network (WSN)*?
2. Bagaimana bentuk kontrol optimal model matematika penyebaran *malware* pada perangkat *Wireless Sensor Network (WSN)*?
3. Bagaimana hasil simulasi numerik model matematika penyebaran *malware* pada perangkat *Wireless Sensor Network (WSN)* sebelum dan sesudah penambahan variabel kontrol?

1.3 Tujuan

Berdasarkan rumusan masalah yang telah diuraikan di atas, maka tujuan yang akan dicapai adalah sebagai berikut:

1. Menganalisis kestabilan titik setimbang model matematika penyebaran *malware* pada perangkat *Wireless Sensor Network (WSN)*.
2. Mengetahui bentuk kontrol optimal model matematika penyebaran *malware* pada perangkat *Wireless Sensor Network (WSN)*.
3. Mengetahui hasil simulasi numerik model matematika penyebaran *malware* pada perangkat *Wireless Sensor Network (WSN)* sebelum dan sesudah pemberian kontrol.

1.4 Manfaat

Adapun manfaat dari penelitian ini adalah sebagai berikut:

1. Bagi penulis, penelitian ini bermanfaat untuk sarana belajar dalam mengkaji suatu permasalahan di kehidupan nyata dengan menggunakan ilmu matematika.
2. Bagi pembaca, penelitian ini bermanfaat sebagai informasi terkait penyebaran *malware* pada perangkat *Wireless Sensor Network (WSN)* yang terhubung dengan jaringan internet. Sehingga para pengguna *Internet of Things (IoT)* dapat melakukan pencegahan risiko penyebaran *malware*.

1.5 Batasan Masalah

Batasan masalah yang dipakai dalam penelitian ini adalah sebagai berikut:

1. Model dasar matematika penyebaran *malware* pada perangkat *WSN* yang digunakan dalam penelitian ini merujuk pada jurnal internasional yang ditulis oleh (Ye, dkk., 2021).
2. Variabel kontrol yang digunakan pada penelitian ini berupa pemasangan antivirus (u_1) dan reparasi *node* (u_2).