BAB I

PENDAHULUAN

1.1 Latar Belakang

Pada saat ini kebutuhan akan teknologi telah menjadi kebutuhan dasar di kalangan masyarakat. Salah satunya adalah pemakaian *smartphone* dan *Wi-Fi (Wireles Fidelity)* dalam mengakses internet untuk kepentingan komunikasi dan berbagi informasi. Semakin banyak pengguna *smartphone* yang menggunakan *Wi-Fi* untuk mengakses internet akan menyebabkan *smartphone* rentan terkena serangan *malware*. Berdasarkan data *Symantec Security*, jumlah *malware* telah meningkat secara eksponensial dari pertama kali kemunculannya pada tahun 1986, dan sekarang jumlah *malware* telah melebihi 74.000 dengan jenis yang berbeda (Mishra dan Anshari, 2012).

Salah satu jenis *malware* yang berbahaya adalah *worm* berbasis *Wi-Fi (Wireles Fidelity)* yang dikenal dengan sebutan *chamelon*. *Chameleon* merupakan jenis *worm* berbasis *Wi-Fi (Wireless Fidelity)* yang dapat diibaratkan seperti organisme yang menular secara biologis, bergerak melalui jaringan *Wi-Fi* seperti penyakit di udara pada manusia. *Chameleon* mampu mereplikasi dirinya untuk mencoba memecahkan kata sandi setiap router *Wi-Fi* baru yang ditemuinya tanpa bantuan manusia. *Chameleon* menyebar melalui *acces point* diantara jaringan *Wi-Fi* dengan tidak mempengaruhi cara kerja dari *acces point* tersebut, tetapi mampu mengumpulkan data-data pengguna *Wi-Fi* lain yang terhubung dengannya, seperti kata sandi, kartu kredit, atau akun bank yang dapat merugikan pengguna (Scharr, 2014). Mayoritas *smartphone* tidak memiliki cara yang efektif untuk mencegah serangan *worm* yang

mengakibatkan terjadinya *vulnerability* yaitu kondisi dimana *smartphone* menjadi rentan terhadap serangan *worm* (Xiao dkk, 2016).

Masalah penyebaran *worm* berbasis *Wi-Fi* dapat dianalisis secara matematis dengan melibatkan model matematika. Penelitian terkait model matematika tentang penyebaran *worm* berbasis *Wi-Fi* telah dilakukan oleh Xiao dkk (2016). Penelitian tersebut membahas model matematika penyebaran *worm* berbasis *Wi-Fi* pada *smartphone* dengan adanya karantina dimana *Wi-Fi base station* menjadi pengontrol koneksi. Xiao dkk (2016) membagi populasi node menjadi sub-sub populasi yaitu populasi node yang rentan terhadap *worm (S)*, populasi node yang terinfeksi *worm* tapi belum bisa menyebarkan *worm* ke node lain *(E)*, populasi node yang terinfeksi *worm (I)*, populasi node yang dikarantina *(Q)* dan populasi node yang pulih *(R)*. Selanjutnya Utoyo dan Nurafifah (2018) mengembangkan model tersebut dengan menganalisis dan memodifikasi model SEIQR yang berbentuk sistem persamaan diferensial biasa ke dalam bentuk sistem persamaan diferensial parsial.

Berdasarkan uraian di atas, penelitian ini membahas model SEIQR yang diperkenalkan oleh Xiao dkk (2016) dengan modifikasi berupa penambahan populasi *Wi-Fi* yaitu populasi *Wi-Fi* yang rentan terhadap *worm* dan populasi *Wi-Fi* yang terinfeksi *worm*. Hal ini diperlukan karena *Chameleon* merupakan jenis *worm* berbasis *Wi-Fi* yang dalam penyebarannya, *worm* ini menginfeksi *Wi-Fi* terlebih dahulu sebelum menginfeksi *smartphone* yang terhubung dengannya (Scharr, 2014). Proteksi Wi-Fi yang lemah akan menyebabkan *Vulnerability* atau kondisi dimana *Wi-Fi* menjadi rentan terhadap serangan *worm* akan terjadi apabila *Wi-Fi* memiliki proteksi yang lemah.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, maka rumusan masalah pada penelitian ini adalah

1. Bagaimana model epidemi SEIQR-SI penyebaran *worm* berbasis *Wi-Fi* pada *smartphone*?
2. Bagaimana kestabilan titik setimbang pada model epidemi SEIQR-SI penyebaran *worm* berbasis *Wi-Fi* pada *smartphone*?
3. Bagaimana simulasi dari model epidemi SEIQR-SI penyebaran *worm* berbasis *Wi-Fi* pada *smartphone*?

1.3 Tujuan Penelitian

Penelitian ini bertujuan :

1. Membentuk model epidemi SEIQR-SI penyebaran *worm* berbasis *Wi-Fi* pada *smartphone*.
2. Menganalisis kestabilan titik setimbang pada model epidemi SEIQR-SI penyebaran *worm* berbasis *Wi-Fi* pada *smartphone*.
3. Melakukan simulasi dari model matematika SEIQR-SI penyebaran *worm* berbasis *Wi-Fi* pada *smartphone*.

1.4 Manfaat Penelitian

Manfaat penelitian ini adalah:

1. Menambah wawasan ilmu pengetahuan tentang pemodelan matematika khususnya yang terkait dengan penyebaran worm berbasis *Wi-Fi* pada *smartphone*.
2. Dapat digunakan sebagai acuan untuk penelitian selanjutnya.