# ABSTRAK

*Named Data Networking* (NDN) merupakan suatu rancangan arsitektur jaringan baru dimana paket NDN membawa nama data (*name*) dan bukan alamat sumber atau alamat tujuan (alamat IP). Pada jaringan komputer, perutean jaringan merupakan hal penting untuk menunjang komunikasi data. Perutean jaringan pada jaringan IP hanya mengandalkan *Routing Information Base* (RIB*)* yang berasal dari IP *table* pada *router*, sehingga apabila terdapat permasalahan pada jaringan seperti terjadi serangan berbahaya pada salah satu *node*-nya, maka *router* IP harus menunggu sampai IP *table* ter-*update*, baru kemudian melakukan pemindahan jalur perutean**.** NDN memiliki kelebihan berupa *adaptive forwarding*. Dengan mencatat *pending Interest* dan mengamati paket *Data* yang dikirimkan, tiap *router* NDN dapat mengukur performansi *forwarding plane* pada tiap jalur. Informasi ini dapat digunakan untuk mengambil data serta jalur terbaik yang tersedia, dan untuk mendeteksi dan memulihkan permasalahan *forwarding* yang dapat disebabkan oleh kegagalan fisik maupun serangan berbahaya. Kelebihan ini menyebabkan *routing plane* pada jaringan NDN hanya perlu melakukan *update routing* secara berkala.

*Prefix hijack* merupakan salah satu jenis serangan berbahaya yang dapat terjadi pada jaringan. Ketika terjadi serangan *hijack*, paket pada jaringan IP akan diserap oleh node yang terkena *hijack* dan tidak akan diteruskan sampai ke tujuan. Sedangkan pada jaringan NDN, *router* NDN dapat mendeteksi terjadinya serangan *hijack* dengan mengamati status *pending Interest*, sehingga *router* dapat mengalihkan pengiriman paket melalui jalur lain yang tidak terserang *hijack* (memilih jalur alternatif).

Pada Tugas Akhir ini, akan dilakukan simulasi untuk meneliti mekanisme *forwarding* pada jaringan NDN dan melihat pengaruh mekanisme *forwarding* NDN pada kasus *prefix hijack* jika dibandingkan dengan mekanisme *forwarding* IP, serta akan diteliti secara lanjut pengaruh strategi *forwarding* pada NDN terhadap kasus *prefix hijack*. Berdasarkan penelitian yang dilakukan, didapatkan hasil bahwa NDN dapat mengatasi permasalahan hijack yang terjadi pada jaringan, dan strategi *best route* merupakan strategi yang paling baik dalam menghadapi serangan *hijack*, karena *best route* memiliki jumlah *packet loss* yang paling kecil.

**Kata Kunci**: NDN, *forwarding plane, adaptive forwarding, prefix hijack*