Pengembangan metode entropy untuk deteksi Serangan Distributed Denial of Service (DDoS) pada Software Defined Network (SDN) dengan penerapan Feature Selection = Development of entropy method for detection of Distributed Denial of Service (DDoS) Attacks on Software Defined Network (SDN) by implementing Feature Selection

Mochamad Teguh Kurniawan, author

Abstrak

Software Defined Networking (SDN) adalah perkembangan infastruktur jaringan yang mana bidang kontrol dan bidang data dipisah sehingga kecerdasan jaringan secara logis terpusat pada bidang kontrol berbasis perangkat lunak, sedangkan perangkat jaringan (OpenFlow Switches) menjadi perangkat penerusan paket atau bidang data yang dapat diprogram melalui interface (protokol OpenFlow). Namun pemisahan bidang kontrol dan bidang data menimbulkan berbagai tantangan salah satunya adalah tantangan keamanan. Tantangan keamanan yang besar di SDN adalah serangan Distributed Denial of Service (DDoS). Terdapat beberapa titik serangan DDoS pada SDN. Jika DDoS menyerang bidang kontrol mengakibatkan kegagalan seluruh jaringan, sementara jika menyerang bidang data atau saluran komunikasi antara bidang kontrol dan bidang data mengakibatkan paket drop dan tidak tersedianya layanan SDN. Berbagai solusi keamanan untuk mengurangi dan mencegah serangan DDoS pada SDN sudah ditawarkan, salah satunya adalah dengan metode entropy. Metode entropy adalah konsep dari teori informasi, yang merupakan ukuran ketidakpastian atau keacakan yang terkait dengan variabel acak atau dalam hal ini paket yang datang melalui jaringan. Metode entropy adalah solusi yang efektif dan ringan dalam hal sumber daya yang digunakannya karena serangan DDoS dapat menghabiskan sumber daya pengontrol, bandwidth link dan sumber daya switch OpenFlow yang memiliki kapasitas yang terbatas maka solusi yang di usulkan pun harus ringan dan tidak menghabiskan sumber daya atau overhead pada sumber daya jaringan. Penelitian sistem deteksi dengan metode entropy saat ini masih memiliki beberapa kelemahan, metode entropy masih menghasilkan nilai akurasi yang masih rendah dan false positive yang masih cukup tinggi hal ini dikarenakan fitur yang di hitung entropy-nya hanya menggunakan satu fitur dan dua fitur. Hal ini berpeluang untuk menyebabkan kesalahan deteksi, selain itu, belum ada nya pemilihan fitur mana yang paling berpengaruh terhadap serangan DDoS sehingga ketika memperhitungkan semua fitur metode deteksi akan memberatkan kerja kontroller. Maka perlu adanya pemilihan fitur dan perhitungan yang mempertimbangkan lebih dari satu fitur. Penelitian ini mengembangkan metode entropy dengan memperhitungkan tiga fitur serangan DdoS yang menjadi titik maksimal sesuai dengan karakteritik SDN dan DDoS. Ketiga fitur tersebut adalah source_IP, destination_IP dan source_MAC didapatkan akurasi deteksi DDoS dengan menggunakan pengembangan entropy sebesar 99.43%. Dengan False positive 0.08 % dan kecepatan deteksi sebesar 10.5s. .....Software Defined Networking (SDN) is a development of network infrastructure in which the control planes and data planes are placed separately so that network control intelligence is logically translated into software-based fields. In contrast, the network devices (OpenFlow Switches) become packet-forwarding devices or data fields that can be programmed through interfaces (OpenFlow protoco l). However, the conversion of control fields and field data cause various challenges for instance a security challenge. The big security challenge in SDN is Distributed Denial of Service (DDoS) attacks. There are multiple DDoS attack

points on SDN for example If a DDoS attacks the control plane, it may cause failure of the entire network, while if it attacks the data plane or the communication channel between the control plane and the plane data it will result a dropped packets and SDN services will no longer available again. There are a bunch of security solutions have been offered to reduce and prevent DDoS attacks on SDN. One of them entropy method. This method derives from information theory, which is a the baseline of the uncertainty or randomness associated with random variables or in this case packets that may go through a network. The entropy method is an effective and friendly resource-usage solution. it's because when DDoS attacks the control plane, it required a lot of controller resources, link bandwidth and OpenFlow switch resources which have limited capacity. Hence, the proposed solution sould be resource friendly or overhead on network resources. Research on detection systems using the entropy method currently still has several weaknesses for example the entropy method still produces low accuracy values and a high-false positives since the calculated entropy features only use one and two features. This procedure will cause errors detection. In addition there is no selection of which features have the most influence on DDoS attacks, so when considering all the features the detection method, it will burden the controller's work. So, it is necessary to select features and calculations that consider more than one feature. This research develops the entropy method which engaged the three features of DDoS attacks that may become the maximum point according to the characteristics of SDN and DDoS. The three features inlcude source_IP, destination_IPand source-MAC, result the accuracy DDoS detection using an entropy expansion of 99.43% with a False positive of 0.08% and a detection speed of 10.5s