TUGAS MANAJEMEN JARINGAN

Athena: A Framework for Scalable Anomaly Detection in Software-Defined Networks

Disusun Oleh :

Nama : Dinar Agustina

NIM : 09011181520023

Kelas : SK7P

Dosen : Deris Stiawan, M.T., Ph.D.

SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2018

Athena: A Framework for Scalable Anomaly Detection in Software-Defined Networks

a. Framework

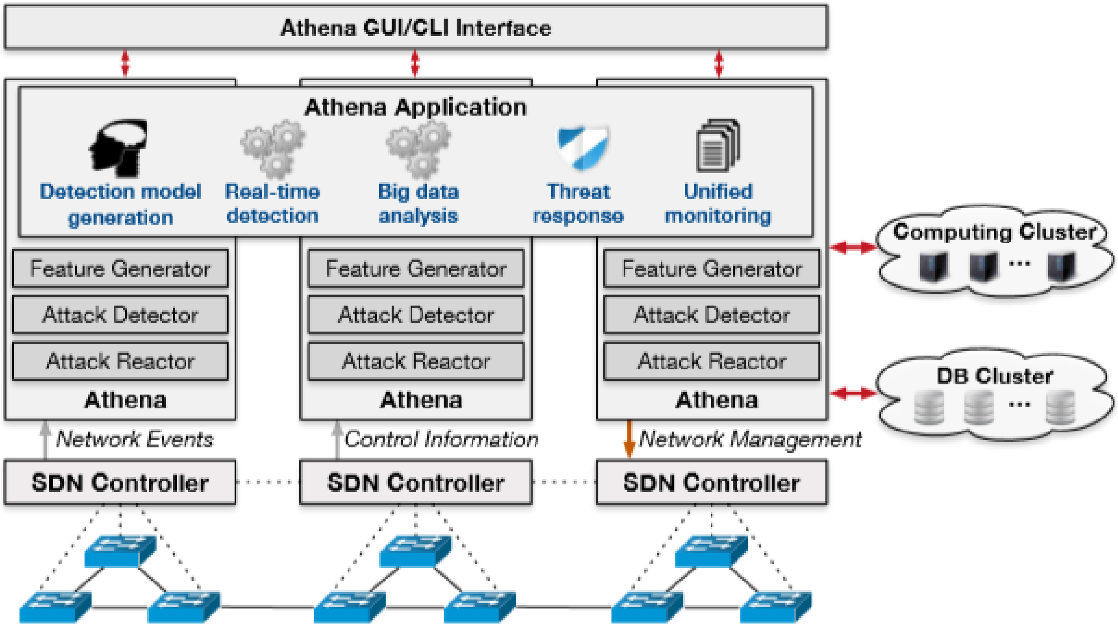

Fig. 2. *Athena's* conceptual architecture; An illustration of the *Athena* anomaly detection framework hosted over a wide-area SDN with distributed controllers. Each controller hosts an instance of *Athena* that instantiates the anomaly detection task per instance. These components can also integrate with the third-party DB cluster and computing cluster. *Athena* applications perform diverse anomaly detection tasks, and operators control the *Athena* applications via a graphical user interface.

Athena is a fully-distributed network anomaly detection framework, in which an Athena instance is hosted above each distributed SDN controller, such as with ONOS instances deployed across a wide area network. For example, Figure 2 illustrates three Athena instances that are distributed across three SDN controllers. Each Athena instance monitors the network behavior that is associated with its hosted network controllers and the data plane hosted by the controllers.

As shown in Figure 2, conceptually, Athena incorporates the Feature Generator, which collects SDN control messages issued by the local control and data plane, generates network features, and publishes features to a distributed database (a DB cluster) for feature management. The Attack Detector detects potential network problems using the developer-defined detection algorithm. The Attack Reactor has responsibility for mitigating detected threats by issuing mitigation actions to the data plane. Operators need not modify their existing SDN stack to host Athena, as its inputs are SDN control messages, along with small code stubs within the controller. We discuss the details of Athena's architecture in Section III-A.

Above the framework, Athena provides the set of components that compose its user-friendly development environment. Athena exports a high-level API called as the Athena NB API, which allows developers to create anomaly detection applications in amanner that is agnostic to the underlying SDN implementation. Athena offers an abstraction to the controller and data plane implementations and versions, enabling rapid prototyping and minimizing deployment costs.

Athena provides 8 core and 70 utility APIs, described in Table II. Developers implement anomaly detection tasks as Athenaapps(showninFigure2),usingtheAthenaNorthbound API (NB API). These applications generate anomaly detection models, perform real-time detection, and implement live threat responses.

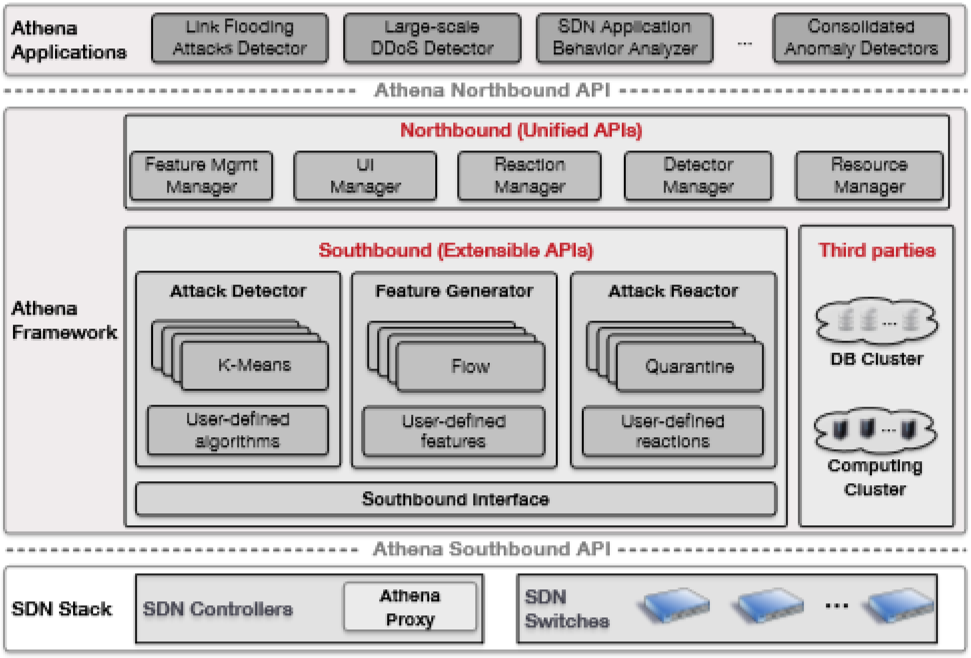

Fig. 3. An overview of the *Athena* system architectural components. The *Athena* framework is composed of the extensible southbound element, the unified northbound element, and the *Athena* application instantiation layer.

c. Hasil

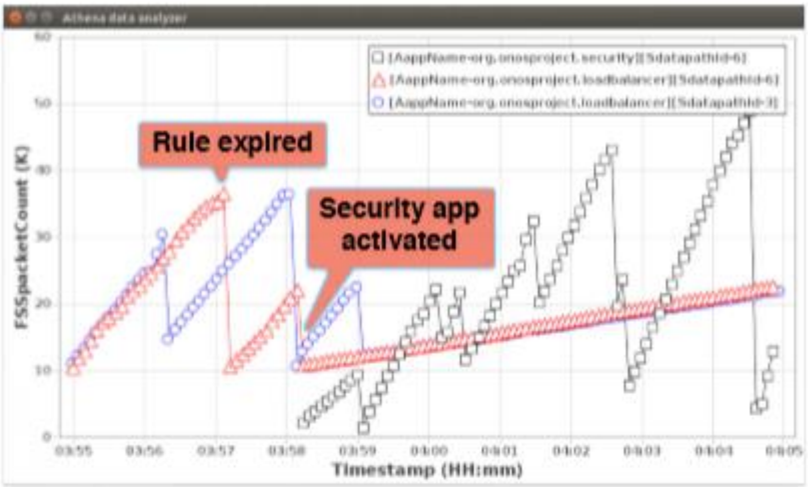

Fig. 9. The coarse-grained analysis result alerted by the *Athena* UI manager, when applications obey the user-defined SLA.

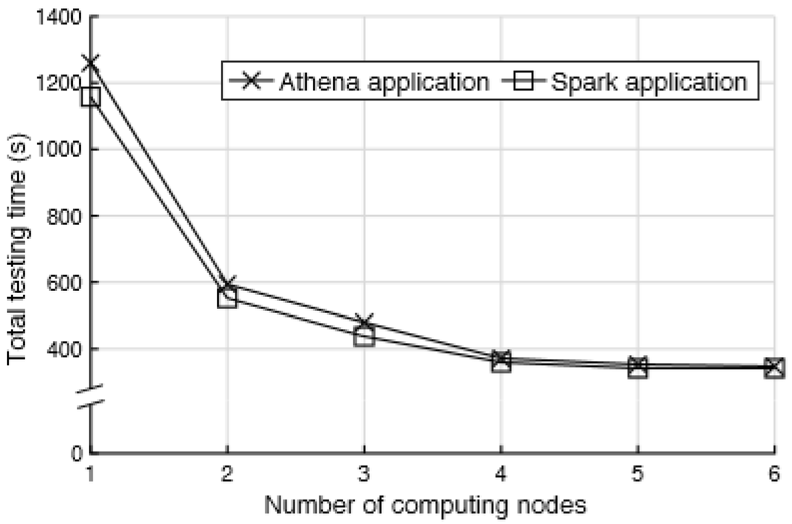

Fig. 10. A performance assessment of the DDoS application while performing anomaly detection tasks per the number of computing nodes.

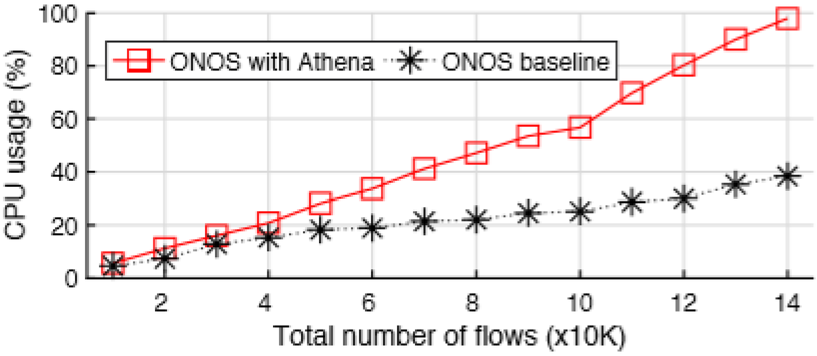

Fig. 11. Average CPU usage while handling flow events with/without *Athena*.

d. kesimpulan

Kami mengeksplorasi beberapa tantangan dalam merancang layanan deteksi anomali skalabel di lingkungan SDN skala besar. Kami mengevaluasi implementasi prototipe awal solusi kami, Athena, melalui ONOS open source yang mendistribusikan pengontrol SDN. Kami membahas bagaimana Athena memungkinkan para peneliti keamanan dan pengembang untuk membuat aplikasi deteksi anomali dengan upaya pemrograman minimal melalui lapisan abstraksi API-nya.

Kami juga membahas penggunaan umum dari strategi off-the-shelf untuk mendorong anomali pengembangan algoritma deteksi jaringan dan memperkenalkan anomali SDN-spesifik yang baru. Athena menggunakan basis data terdistribusi dan platform komputasi berkerumun, yang dapat menerapkan algoritme deteksi ini di seluruh bidang kontrol terdistribusi berskala besar. Kerangka kerja Athena dirancang untuk beroperasi pada infrastruktur SDN yang ada, yang memungkinkan operator untuk menerapkannya dengan cara yang efisien. Evaluasi kami menunjukkan bahwa Athena dapat mendukung layanan deteksi anomali jaringan yang terkenal dengan cara yang efisien, dengan skala ke dataset skala besar dari lingkungan jaringan fisik pusat data skala besar.