Pengenalan Pola pada Lalu Lintas Data Dengan Deep Packet Inspection

Tasmi
Megister Teknik Informatika
Fakultas Ilmu Komputer
Univeristas Sriwijaya
tasmi@ilkom.unsri.ac.id

Sasut Analar Valianta
Megister Teknik Informatika
Fakultas Ilmu Komputer
Univeristas Sriwijaya
a.valeyys@gmail.com

Deris Stiawan
Program Studi Sistem Komputer
Fakultas Ilmu Komputer
Univeristas Sriwijaya
deris@ilkom.unsri.ac.id

***Abstract*—**Peningkatan jumlah aplikasi dan layanan Internet mengakibatkan kompleksitas pada manajemen jaringan, misalnya dalam penyalahgunaan bandwidth dan keamanan jaringan. Akibatnya, identifikasi lalu lintas jaringan memainkan peranan yang semakin penting dalam manajemen jaringan. Deep Packet Inspection (DPI) adalah salah satu metode untuk menganalisis lalu lintas pada jaringan informasi dengan mengenali string. DPI diperlukan untuk mencocokkan pola dalam payload dari sebuah paket mentah data.

Kata kunci: Deep Packet Inspection, Net-DPIs, network management system, algoritma

I. PENDAHULUAN

Semakin banyak layanan internet maka banyak penomeran port yang digunakan dalam mengirim data dan pesan. Dalam pengamatan [1] Port yang digunakan banyak yang tidak sesuai dengan layanan jaringan, akibatnya sistem jaringan tidak hanya mengindentifikasi lalu lintas data, jenis protocol dan nomor port.

Penelitian sebelumnya [2] mengatakan, ada banyak tantangan dalam melakukan pengklasifikasian lalu lintas data, sebagai contoh menjalankan aplikasi jaringan dapat menghasilkan serangkaian paket di jaringan nyata . Sebuah paket terdiri dari header, payload dan informasi header membawa beberapa lapisan-lapisan. Alamat IP [3] pada lapisan ketiga dan nomor port adalah di lapisan empat. Payload membawa protokol lapisan aplikasi dan data. Layanan jaringan mengirimkan data melalui protokol aplikasi. Misalnya, HTTP menggunakan GET atau PUT sebagai metode, contoh lain, misalnya MSN menggunakan NLN atau BSY sebagai penggunaan status. String pada payload ini umumnya unik sehingga mereka bisa dianggap sebagai pola atau signature dari aplikasi jaringan

Disisi lain dikatakan bawah Deep Packet inspection (DPI) salah satu cara yang efektif untuk memeriksa dan mendeteksi serangan berbahaya pada jaringan [5]. DPI adalah metode analisis kareteristik lalu lintas dan pemantuan jaringan dengan cara menangkap dan menganalisis header paket. DPI akan memeriksa isi komunikasi data dan mengidentifikasi ancaman keamanan dan memastikan sesuai dengan kebijakan keamanan. Data yang diambil dapat dianalisis atau dapat ditulis untuk file log [15].

Dalam naskah ini, akan dijelaskan Algoritma Knuth-Morris-Pratt (KMP) [8] dan algoritma Wu-Manber [12] yang digunakan untuk mengklasifikasikan layanan jaringan dan juga pendekatan dalam pencocokan string dengan memperkenalkan perangkat lunak untuk system DPI.

II. METODE YANG DIGUNAKAN

Banyak algoritma telah diperkenalkan untuk melakukan pencocokan string yang dikemukaka oleh [7]. dimana algoritma pencocokan string mempunyai dua faktor yang mempengaruhi throughput data yang diproses: (1) operasi perhitungan untuk membuat perbandingan pola dan data, dan (2) Berapa jumlah pola yang perlu dibandingkan dengan traffik yang masuk. Disisi lain, Brute force (BF) adalah algoritma pertama yang digunakan untuk pencocokan string yang membandingkan karakter pertama dalam pola dengan aliran data [2]. Ada banyak algoritma yang telah digunakan sebelumnya [1,10] untuk pencocokan pola. Namun, algoritma perangkat lunak yang paling terkenal berbasis Knuth-Morris-Pratt (KMP) Boyer-Moore (BM), Aho-Corasick (AC) , algoritma AC BM, Wu- manber, dan Commentz Walter (C).

Algoritma Knuth-Morris-Pratt (KMP) dalam analisa proposal [1] adalah algoritma yang digunakan sebagai perangkat tambahan untuk algoritma brute force sebagai preliminary untuk pencocokan pola. Kelebihan algoritma KMP dibanding dengan BF adalah KMP dapat melompati karakter ketika ketidakcocokan terjadi pada fase perbandingan. Pengabaian dengan kemampuan melompati ini digunakan untuk mengenali karakter, namun tergantung pada fase preprocessing dari KMP ke pola sebelumnya.

Ide dasar dari algoritma KMP yang diterangkan oleh [8] adalah mendeteksi ketidakcocokan pola, dimana backup pointer dalam pola hanya bergantung pada karakter yang tidak bergantung pada text. Akibanya, pointer dalam teks tersebut tidak pernah dikurangi. Untuk mencapai hal ini, pola diproses dengan training awal untuk mendapatkan sebuah urutan yang memberikan indeks dalam pola karakter yang akan digunakan.

III. KESIMPULAN

DPI adalah suatu pendekatan untuk memeriksa bagian isi paket yang mengalir melalui jaringan secara real time. Secara khusus, DPI bukan hanya melakukan pemeriksaan paket individu dari payload, tetapi dengan kemampunya dapat memeriksa string secara detail dan menganalisis ratusan atau ribuan paket secara realtime. Dalam naskah ini dijelaskan

beberapa algorithma yang digunakan dalam DPI. Ada beberapa algortima yang digunakan untuk sistem pencocokan payload: Algoritma Knuth-Morris-Pratt (KMP), algoritma Wu-Manber dengan trie dan algoritma Wu-Manber yang digunakan untuk mengklasifikasikan layanan jaringan.

REFERENCES

[1] Tamer AbuHmed,Abedelaziz Mohaisen, and DaeHun Nyang "*A Survey on Deep Packet Inspection for Intrusion Detection Systems*" arXiv:0803.0037v1 [cs.CR] 1 Mar 20008

[2]. Thaksen J, Pravin Chandra," *A Novel Approach to Deep Packet Inspection for intrusion Detection*" International conference on adnvance computing technologies and applications (ICACTA-2015

[3] Chang-Su Moon and Sun-Hyung Kim, "*A Study on the Integrated Security System based Real-time Network Packet Deep Inspection*" International Journal of Security and Its Applications Vol.8, No.1 (2014)

[4] Sailesh Kumar, Jonathan Turner, John Williams "*Advanced Algorithms for Fast and Scalable Deep Packet Inspection*"

[5] DanielSmallwood, AndrewVance "*Intrusion Analysis with Deep Packet Inspection*" 2011InternationalConferenceon Cloud and ServiceComputing

[6] Thaksen J. Parvat, Pravin Chandra USET, USICT, G.G.S.Indratrastha "*Performance Improvement of Deep Packet Inspection for Intrusion Detection*" 2014 IEEE Global Conference on Wireless Computing and Networking (GCWCN)

[7] Kefu Xu, Jianlong Tan, Li Guo, Binxing Fang, "*Traffic-Aware Multiple Regular Expression Matching Algorithm for Deep Packet Inspection*" JOURNAL OF NETWORKS, VOL. 6, NO. 5, MAY 2011

[8] Mireille REGNIER "*Knuth-Morris-Pratt Algorithm: An Analysis*"

[9] Géza Szabó, Zoltán Turányi, László Toka "*Automatic Protocol Signature Generation Framework forDeep Packet Inspection*"

[10] M.-Y. Liao,M.-Y. Luo,C.-S. Yang,C.-H. Chen, P.-C. Wu, Y.-W. Chen "*Design and evaluation of deep packet inspection system: a case study*" Published in IET Networks Received on 20th December 2011 Revised on 19th February 2012

[11] Y oung H. Cho and William H. Mangione-Smith "*Programmable Hardware for Deep Packet Filtering on a Large Signature Set*" The University of California, Los Angeles, CA 90095

[12] Lucas Vespa, Ning Weng "*SWM: Simplified Wu-Manber for GPU-based Deep Packet Inspection*"

[13] Manish Shrivastava "*Evaluation of different software based approaches for Deep Packet Inspection*" International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 5, May 2015

[14] Jakub Svoboda "*Network Traffic Analysis with Deep Packet Inspection Method*" Brno, Spring 2014

[15] R. Yasin "10 technologies to watch in 2010: *Deep packet inspection adds a layer of defense*," Government Computer News, January 2010