Ringkasan Pekerjaan pada Sistem Deteksi Intrusi Dalam Jaringan Ad-hoc

mahasiswa Teknik Komputer
Fakultas Informatika
Intitut Teknologi Batam
Batam, Indonesia
Email: johanwilian455@gmail.com

***Abstract*—Deteksi intrusi dalam jaringan sangat pentinga karena sering terjadi serangan pada jaringan sehingga deteksi intrusi ini perlu diterapkan. Penyerang akan melakukan upaya untuk masuk ke sistem kita. Ada baiknya sistem kita terus dipantau dengan menggunakan intrusi untuk mendeteksi hal-hal yang mencurigakan, dan meresposnya ketika disusupi.**

I. PENDAHULUAN

mendeteksi serangan lalu lintas jaringan, intrusi dan sebagainya.Saat ini, tantangan utama yang terkait dengan domain ini adalah untuk menjaga keamanan jaringan.

sistem deteksi intrusi (IDS) Untuk mendeteksi intrusi di VANET, pembelajaran mesin, dan pembelajaran algoritma diberbagai tingkatan.

susunan makalah disusun pada bab 2 akan menjelaskan tentang jaringan Ad-hoc. Bagian 3, menyajikan detail latar belakang dan membahas tentang teknologi berbeda yang terkait dengan pembelajaran mesin dan itu digunakan di VANET. Bagian 4 membahas tentang teknik logika fuzzy pada VANET

II. SISTEM DETEKSI INTRUSI

Komunikasi kendaraan memiliki tujuan utama untuk mendeteksi berbagai serangan lalu lintas dan mencegahnya dengan menggunakan Intrusion Detection System (IDS) tiga utama: komponen yang ditunjukkan pada Gambar 1 seperti pengumpulan data, vektorisasi dan mesin klasifikasi. IDS juga termasuk satu alasan utama untuk mendeteksi serangan kendaraan dari sistem, yang diketahui atau tidak diketahui. Umumnya IDS tergantung pada beberapa komponen perangkat keras. Menjalankan perangkat keras seperti itu komponen membutuhkan perangkat lunak yang konsisten dan kuat [2] [1].

gambar 1 komponen IDS

alat komunikasi memiliki tujuan utama untuk mendeteksi berbagai serangan lalu lintas dan mencegahnya dengan menggunakan Intrusion Detection System (IDS),

Mesin klasifikasi adalah bagian paling kompleks dari IDS karena termasuk keputusan vektor fitur yang dikonversi sebagai aturan penyusupan.

IDS ini mengandung beberapa fakta, seperti:

sistem komunikasi yang kompleks dan memiliki lebih banyak jumlah kesalahan.

Mereka digunakan untuk mendeteksi kesalahan dan juga untuk memperbaikinya. Beberapa sistem pencegahan intrusi keluar tetapi tidak itu tidak akan mencegah semua serangan. Pada saat itu, IDS memainkan peran penting.

Intrusion detection system is of two types: 1. Misuse based IDS 2. Anomaly based IDS.

Jenis IDS berdasarkan deteksi serangan yang banyak diketahui telah ditentukan sebelumnya tetapi gagal untuk mengidentifikasi serangan yang tidak diketahui. Serangan tidak dikenal dengan alarm palsu tinggi dideteksi dengan menggunakan pendekatan berbasis anomali [2].

III. PEKERJAAN YANG BERHUBUNGAN

Gozde Karatas et. Al. [3] [3] mengusulkan Deteksi Intrusi Sistem [IDS] untuk menganalisis kinerja fungsi pelatihan dari sistem. Sistem yang diusulkan didasarkan pada sistem saraf jaringan yang berisi 2 lapisan tersembunyi untuk mendeteksi intrusi jaringan. Untuk analisis kinerja, Piala KDD 99 kumpulan data digunakan.

Akash Garg et. Al. [4] [4] mempresentasikan penggunaan berbasis penyalahgunaan atau IDS berbasis tanda tangan yang berfungsi saat data dikirim ke jaringan dan selanjutnya server memverifikasi data ini. Jika ada data kasar diperoleh, kemudian server membuang paket yang lain meneruskannya ke jaringan. Selanjutnya, data tiba di server diperiksa dengan menggunakan alat akurasi tinggi untuk mendeteksi paket jaringan dari database dan kemudian membuang paket jaringan lain itu akan memindahkan data ke sistem jaringan.

Dalam [5] [5], disajikan studi tentang deteksi intrusi di VANET dan menganalisis solusi yang layak untuk berbagai jenis serangan seperti DOS, DDOS dll Tuan a Tang et. al [6] [6] memberikan deskripsi terperinci tentang jaringan yang ditentukan perangkat lunak sebagai solusi yang dipilih untuk mendeteksi intrusi di jaringan. Penulis terutama berfokus pada serangan DDoS di IDS untuk meningkatkan akurasi model NIDS yang diusulkan dengan menggunakan teknik pembe-

lajaran mendalam, yang mendeteksi intrusi dan menganalisis model NIDS.

Konstantinos Pelechrinis et. Al. [7] [7] menyajikan detail ulasan tentang serangan jamming yang direkam di koran oleh tambahan menjelaskan berbagai teknik yang disarankan untuk mendeteksi keberadaan jammer. Akhirnya, pekerjaan itu memiliki meninjau mekanisme yang banyak, yang bermanfaat untuk melindungi jaringan dari berbagai serangan jamming.

Bellardo et al [8] [8], mempresentasikan analisis eksperimental dari serangan tertentu dalam jaringan. Dalam penelitian ini diterapkan sistem untuk deteksi intrusi berdasarkan lapisan 802.11 MAC dan menganalisis efisiensi sistem

Ismail Butun, dkk. Al. [10] [9] memberikan informasi tentang klasifikasi IDS, berisi klasifikasi rinci pf sistem deteksi intrusi sebagai persyaratan IDS, klasifikasi, pengambilan keputusan di IDS dan intrusi tanggapan. IDS yang diusulkan untuk Mobile Ah-hoc NETworks (MANET) disajikan dan penerapannya untuk jaringan sensor nirkabel dibahas.

IV. Kategori Serangan

Serangan lalu lintas dalam sistem komunikasi adalah berbeda sebagai berikut:

- normal
- DOS
- U2R
- R2L
- Probe

Serangannya terdiri dari 22 jenis, masing-masing milik serangan kategori di atas [11] [10].

DOS: Sebuah upaya untuk membuat layanan tidak tersedia untuk pengguna dikenal sebagai DoS (Denial of Service). Di serangan ini, tujuan penyerang adalah agar node tidak dapat melakukan yang lain tugas yang perlu dan esensial. Ini yang paling parah dan serangan yang kompleks sama sekali. Serangan ini dapat membebani sumber daya node jaringan dengan mengganggu saluran dengan cara jaringan. Ini adalah serangan lapisan fisik yang mengandung sub-tipe DDoS (Penolakan Serangan Terdistribusi).

U2R: Serangan utama pada pengguna untuk melakukan root (U2R) adalah buffer overflow yang menyalin terlalu banyak data ke dalam buffer statis tanpa memeriksa apakah sudah diperbaiki dengan benar atau tidak.

R2L: Serangan ini mempengaruhi besar jumlah jaringan/sistem di dunia setiap hari

Probe: Attacker tries to gain information about the target host.

V. Teknik Machine Learning

Untuk mendeteksi intrusi dalam komunikasi kendaraan beberapa pembelajaran mesin dan algoritma pembelajaran mendalam digunakan. Beberapa algoritma ditinjau di sini di bawah ini juga:

Deep Belief Network (DBN): Jaringan Kepercayaan Dalam memiliki jaringan saraf umpan maju dengan kedalaman arsitektur terdiri dari banyak lapisan tersembunyi. Beberapa terlihat lapisan disebut sebagai lapisan input dan juga beberapa lapisan output adalah menyajikan. Dalam [12] [11] digunakan protokol routing cerdas berbasis based jaringan kepercayaan yang mendalam untuk layanan multimedia dalam pengetahuan VANET sentris. DBN melakukan deteksi intrusi melalui berbagai eksperimen setelah pelatihan dengan beberapa kumpulan data juga meningkatkan jaringan keamanan dengan standar algoritma IDS. DBN sebagian besar jatuh sekarang dan jarang digunakan dibandingkan dengan algoritma pembelajaran generatif lainnya tetapi masih diakui untuk peran penting mereka dalam pembelajaran yang mendalam.

Algoritma K-Means: Algoritma K-mean dapat digunakan untuk mengembangkan sistem deteksi intrusi. [12] [12] Algoritma ini tidak menentukan jumlah cluster dan cluster adalah dibuat menggunakan nilai optimal berdasarkan fungsi fitness untuk membantu mengidentifikasi jenis serangan.

Support Vector Machine (SVM): In [14] [13] implemented SVM against network intrusion using MATLAB. KDD dataset is used as bench market dataset for intrusion detection and shows SVM is limited because they need long training time to show the result.

Convolutional Neural Network (CNN): CNN sangat dalam algoritma pembelajaran yang digunakan untuk mengklasifikasikan gambar dan mengenali yang benar dengan akurasi tinggi. Model ini terdiri dari neuron dengan data yang dapat dipelajari yang dilewatkan dari berbagai lapisan seperti lapisan yang sepenuhnya terhubung, penyatuan, filter, dan fungsi. Di [15] [14] memberikan perbandingan deep learning CNN dengan DBN. Menurut hasil kinerja CNN menunjukkan bahwa akurasi dan deteksi model CNN dalam intrusi deteksi sedikit lebih tinggi dari model DBN.

Memori jangka pendek panjang (LSTM): Jangka pendek panjang jaringan memori adalah jaringan saraf berulang yang mampu urutan pembelajaran dalam urutan masalah prediksi. LSTM adalah area pembelajaran mendalam yang kompleks. Supriya P. Shende et. Al. [16] [15] menyimpulkan bahwa biner serta klasifikasi multiclass untuk deteksi menggunakan LSTM dalam keamanan jaringan. Berdasarkan akurasi penulis LSTM dalam keamanan jaringan pembelajaran mendalam untuk biner 99,2 persen

VI. Penggunan Data Set

Kumpulan data yang paling umum digunakan untuk deteksi intrusi di IDS adalah: KDD Cup99, NSL-KDD, CIC IDS 2017, CSE CIC-IDS 2018

KDD Cup99: Dataset KDD Cup99 dibuat pada tahun 1999 untuk mendeteksi intrusi. Dataset digunakan dalam penambangan data dan teknik pembelajaran mesin. Dataset ini berisi sekitar 4.9 juta keping data, di mana 83jenis serangan.

NSL-KDD: Algoritme pembelajaran mesin pada KDD Cup99 dapat melakukan pra-proses dengan baik dan membuat kumpulan data KDD NSL baru dengan menghapus catatan duplikat darinya. Begitu sebelumnya, banyak perbedaan telah ditemukan di yang baru kumpulan data dibandingkan dengan kumpulan data lama

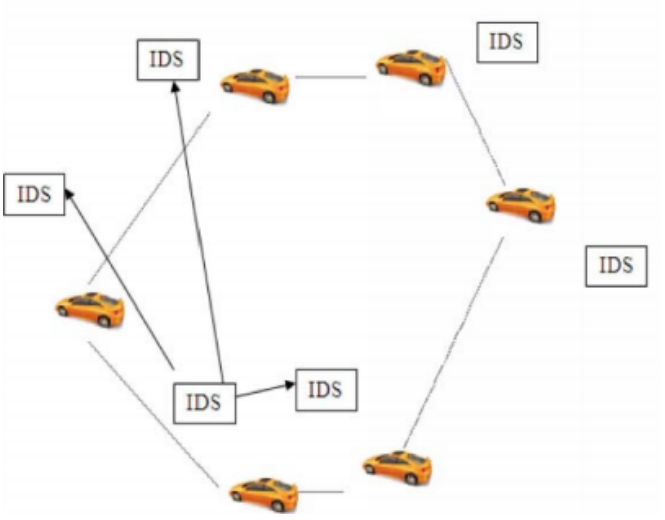
CIC IDS 2017: Dataset ini mencakup serangan umum seperti data dunia nyata, menggabungkan berbagai kriteria

untuk mengidentifikasi serangan serta memberikan hasil yang tepat untuk pembelajaran mesin dan pembelajaran yang mendalam.

CS E-CIC-IDS 2018: Untuk sistem kendaraan, detail informasi serangan disertakan di dalamnya. Kumpulan data ini berisi: tujuh jenis serangan beberapa terkait dengan kendaraan komunikasi seperti serangan DoS, serangan DDOS, Brute serangan paksa, dll.

VII. Arsitektur yang DiUsulkan

Operasi jaringan kendaraan harus menyediakan setiap node dengan teknik deteksi intrusi sehingga setiap node dapat berpartisipasi dalam deteksi intrusi. Node tetangga bisa membentuk asosiasi dan mengawasi jaringan satu sama lain. VANET berisi agen untuk mendeteksi intrusi setiap node dan agen-agen ini bertindak secara independen dan mengendalikan kegiatan komunikasi dalam jangkauan radio. Jika ada perubahan data lokal, agen dari node tetangga akan membantu mendeteksi penyusupan. [16]



Gambar 2. Kerangka kerja Sistem Deteksi Intrusi di VANET Sistem deteksi intrusi yang diusulkan dapat mendeteksi intrusi menggunakan data audit jika ada perubahan data. Ini melibatkan beberapa perilaku umum untuk deteksi intrusi node. Data audit yang dikumpulkan terhadap intrusi diperiksa.

Authors	Technique/Methods	Dataset	Attack Type	Contribution	Advantage
M. Ali Aydın et. al. [1]	hybrid IDS (PHAD + NETAD)	IDEVAL	Anomaly	Proposed the hybrid approach for anomaly detection using packet header and network traffic anomaly based on intrusion detection system.	More than 27 type of attack detected. More powerful than signature based IDS. Unknown attack has been detected
Qingqing Zhang et. al. [2]	Data Mining	KDD	Scan Attack DOS	Proposed the hybrid approach for intrusion detection based on data fusion and data mining techniques.	Highly efficient in real time detection False positive rate has been reduced More Flexible
Gozde Karatas et.al. [3]	ANN	KDD Cup'99	Normal DOS R2L U2R	Implemented the intrusion detection system based on the neural network	Minimize the error rate. Great Execution
Tuan A Tang et. al. [6]	DNN	NSL-KDD	DDoS DOS R2L U2R	Proposed the intrusion detection system based on deep learning technique and analyzes the result in NIDS framework	Good detection Rate
John Bellardo et. al. [8]	802.11 MAC layer	--	DOS	Proposed the intrusion detection based on 802.11 MAC layer and analyze the vulnerabilities.	Highly Efficient in detection. Low Overhead

IDS	Model	Technique	Method
Watchdog Pathrater	Stand-alone	• Observe the nodes next to each other • To find optimal rout for node it must synchronize	Monitoring of Router Nodes
Confidant	Distributed Cooperative	• Observe the nodes next to each other • Observe side-by-side nodes • To find optimal rout for node it must synchronize • malicious node must be detected and removed	Reputation
CORE	Distributed Cooperative	• Game Theory • Observe the nodes next to each other • Detecting of optimal rout • malicious node must be detected and removed	Reputation
Zhang et Lee IDS	Distributed Cooperative	• Detection locally and independently • Detect globally and cooperatively by voting	Cooperative Detection
ZBIDS	Clustered	• Markove Chaine	Cooperative Detection
SNORT	Distributed Cooperative	• Pattern Matching	Signature
Jaydip Sen clustered IDS	Clustered	• Detecting the Local Intrusion	Signature
Sterne IDS	Clustered	• Data Fusion/Integration/Reduction	Signature

References

[1] Q. Zhang, H. Yang, K. Li, and Q. Zhang, "Research on the intrusion detection technology with hybrid model," in *2010 The 2nd Conference on Environmental Science and Information Application Technology*, vol. 2. IEEE, 2010, pp. 646–649.

[2] M. A. Aydın, A. H. Zaim, and K. G. Ceylan, "A hybrid intrusion detection system design for computer network security," *Computers & Electrical Engineering*, vol. 35, no. 3, pp. 517–526, 2009.

[3] G. Karatas and O. K. Sahingoz, "Neural network based intrusion detection systems with different training functions," in *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*. IEEE, 2018, pp. 1–6.

[4] A. Garg and P. Maheshwari, "A hybrid intrusion detection system: A review," in *2016 10th International Conference on Intelligent Systems and Control (ISCO)*. IEEE, 2016, pp. 1–5.

[5] F. Gonçalves, B. Ribeiro, O. Gama, A. Santos, A. Costa, B. Dias, J. Macedo, and M. J. Nicolau, "A systematic review on intelligent intrusion detection systems for vanets," in *2019 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*. IEEE, 2019, pp. 1–10.

[6] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in *2016 international conference on wireless networks and mobile communications (WINCOM)*. IEEE, 2016, pp. 258–263.

[7] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *IEEE Communications surveys & tutorials*, vol. 13, no. 2, pp. 245–257, 2010.

[8] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions." in *USENIX security symposium*, vol. 12. Washington DC, 2003, pp. 2–2.

[9] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking*, 2000, pp. 275–283.

[10] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE communications surveys & tutorials*, vol. 16, no. 1, pp. 266–282, 2013.

[11] A. A. Olusola, A. S. Oladele, and D. O. Abosede, "Analysis of kdd'99 intrusion detection dataset for selection of relevance features," in *Proceedings of the world congress on engineering and computer science*, vol. 1. WCECS, 2010, pp. 20–22.

[12] T. Zhang, X. Chen, and C. Xu, "Intelligent routing algorithm based on deep belief network for multimedia service in knowledge centric vanets," in *2018 International Conference on Networking and Network Applications (NaNA)*. IEEE, 2018, pp. 1–6.

[13] J. A. Sukumar, I. Pranav, M. Neetish, and J. Narayanan, "Network intrusion detection using improved genetic k-means algorithm," in *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. IEEE, 2018, pp. 2441–2446.

[14] M. K. Lahre, M. T. Dhar, D. Suresh, K. Kashyap, and P. Agrawal, "Analyze different approaches for ids using kdd 99 data set," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 1, no. 8, pp. 645–651, 2013.

[15] L. Yong and Z. Bo, "An intrusion detection model based on multi-scale cnn," in *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*. IEEE, 2019, pp. 214–218.

[16] S. Shende and S. Thorat 2nd, "Long short-term memory (lstm) deep learning method for intrusion detection in network security," *International Journal of Engineering Research and. V9*, 2020.