SISTEM DETEKSI SERANGAN *DDOS* MENGGUNAKAN ALGORITMA *NAIVE BAYES* PADA JARINGAN *INTERNET OF THINGS*

OLEH:

JOHAN WAHYUDI

09011281320031

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2020

SISTEM DETEKSI SERANGAN *DDOS* MENGGUNAKAN ALGORITMA *NAIVE BAYES* PADA JARINGAN *INTERNET OF THINGS*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH:

JOHAN WAHYUDI

09011281320031

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2020

LEMBAR PENGESAHAN

SISTEM DETEKSI SERANGAN DDOS MENGGUNAKAN ALGORITMA NAÏVE BAYES PADA JARINGAN INTERNET OF THINGS

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:

Johan Wahyudi
09011281320031

Palembang, Juli 2020

Pembimbing I	Pembimbing II
Deris Stiawan, Ph.D.	Ahmad Heryanto, M.T.
NIP. 197806172006041002	NIP. 198701222015041002

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr.Ir. H. Sukemi, M.T
NIP 196612032006041001

Halaman Persetujuan

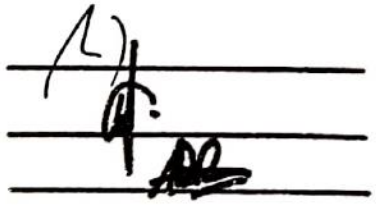
Telah diuji lulus pada :

Hari : **Jumat**

Tanggal : **13 Maret 2020**

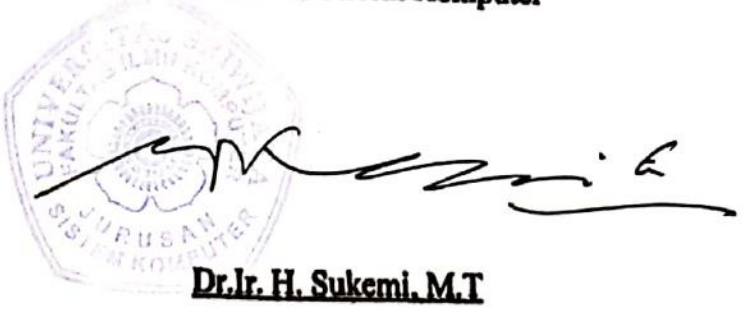
Tim Penguji :

1. **Ketua** : **Adi Hermansyah, M.T**
2. **Anggota I** : **Ahmad Zarkasi, M.T**
3. **Anggota II** : **Aditya Putra Perdana P, M.T**



Mengetahui,

Ketua Jurusan Sistem Komputer



Dr.Ir. H. Sukemi, M.T

NIP 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama	: Johan Wahyudi
NIM	: 09011281320031
Program Studi	: Sistem Komputer
Judul Skripsi	: Sistem Deteksi Serangan DDoS Menggunakan algoritma *Naïve Bayes* Pada Jaringan *Internet of Things*

Hasil Pengecekan Software iThenticate/Turnitin: 15%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan / plagiat dari penelitian orang lain. Apabila ditemukan unsur penjiplakan / plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik yang diberikan oleh Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

Demikian Pernyataan ini saya buat dengan sebenar-benarnya.

Palembang, Juli 2020

Yang menyatakan,

Johan Wahyudi

NIM. 09011281320031

HALAMAN PERSEMBAHAN

*"Terlambat **lulus** atau **lulus tidak** tepat waktu bukanlah sebuah kejahatan, bukan sebuah aib, bukan pula sebagai bahan cemoohan (pengucilan). Alangkah kerdilnya jika mengukur kepintaran seseorang hanya dari siapa yang paling cepat lulus. Bukankah sebaik-baiknya **skripsi** adalah **skripsi** yang selesai dan yang diselesaikan sendiri? Baik itu selesai tepat waktu maupun tidak tepat waktu semuanya ada pada diri kita sendiri, tapi ingatlah semuanya akan indah pada waktu yang tepat."*

يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ ٱسْتَعِينُواْ بِٱلصَّبْرِ وَٱلصَّلَوٰةِ ۚ إِنَّ ٱللَّهَ مَعَ ٱلصَّٰبِرِينَ

Artinya: *"Hai orang-orang yang beriman, jadikanlah sabar dan shalat sebagai penolongmu, sesungguhnya Allah beserta orang-orang yang sabar." (QS. Al-Baqarah [2]: 153).*

Dengan mengucap syukur Alhamdulillah atas rahmat Allah Subhanahu wa Ta'ala, kupersembahkan karya kecil ini untuk . . .

Kedua orang tua tercinta

(Bapak Herman M. Nur (Alm) dan Ibu Yusmawati)

Saudara-saudara ku,

(maidi, Ayu, Novi, dan Linda)

Teman-teman seperjuangan Jurusan,

(Sistem Komputer Angkatan 2013)

Teman-teman lab research,

(Comnets Lab)

Teman-teman komunitas IT Security,

(Sumatra Cyber Security, Born to Protect, Palembang Hacker Link)

Dan semuanya yang secara langsung dan tidak langsung membantu saya

11 Juli 2020

KATA PENGANTAR

Puji syukur penulis panjatkan kehadiran Allah SWT yang telah memberikan rahmat, hidayah serta ijin-Nya sehingga penulis dapat menyelesaikan penulisan tugas akhir dengan judul "***Sistem Deteksi Serangan DDoS Menggunakan algoritma Niave Bayes Pada Jaringan Internet of Things***". Penulisan tugas ahir ini dibuat dalam rangka memenuhi persyaratan untuk menyelesaikan pendidikan di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya untuk memperoleh gelar strata 1.

Pada Kesempatan ini, penulis menyampaikan ucapan terima kasih kepada semua pihak untuk setiap bimbingan, semangat, dukungan, dan doa yang diberikan kepada penulis sehingga terselesaikannya tugas akhir ini. Ucapan terima kasih penulis sampaikan kepada:

1. Allah SWT, yang telah memberikan segalanya kepada penulis berupa Kesehatan, orang tua, pembimbing, teman, rezeki, dll sehingga dapat menyesaikan laporan tugas akhir ini.
2. Orang-orang tercinta, Ibu, Ayah, Saudara kandung, saudara ipar, serta keponakan-keponakan tersayang, yang selalu ada dan tidak pernah lelah dalam mendidik serta memberikan dukungan baik secara moril maupun materil kepada penulis demi lancarnya penulisan tugas akhir ini.
3. Bapak Dr Deris Stiawan, Ph. D dan Bapak Ahmad Heryanto, M.T selaku dosen pembimbing tugas akhir, yang telah memberikan bimbingan, masukan, semangat, dan kemudahan kepada penulis dalam menyelesaikan tugas akhir ini.
4. Bapak Ahmad Zarkasi, M.T dan Bapak Aditya Putra Perdana P, M.T selaku dosen penguji sidang tugas akhir yang telah memberikan masukan serta ilmu yang bermanfaat sehingga tulisan ini menjadi lebih baik.

5. Bapak Sutarno, M.T selaku pembimbing akademik, yang telah membimbing penulis dari semester satu hingga terselesainya tugas akhir ini dengan baik.
6. Bapak Dr.Ir. H. Sukemi M.T selaku ketua jurusan sistem komputer fakultas ilmu komputer Universitas Sriwijaya.
7. Seluruh dosen jurusan sistem komputer fakultas ilmu computer universitas sriwijaya.
8. Staff dijurusan sistem komputer, yang telah banyak membantu penyelesaian proses administrasi.
9. Staff difakultas ilmu komputer, bagian akademik, kemahasiswaan, tata usaha, perlengkapan, dan keuangan, yang telah membantu penyelesaian proses administrasi.
10. Seluruh petinggi atau pimpinan yang ada dilingkungan fakultas ilmu komputer universitas sriwijaya, yang telah membantu proses administrasi selama dikampus.
11. Teman-teman seperjuangan di lab comnets yang telah turut menjaga semangat saya untuk menyelesaikan tugas akhir ini, Dimas Wahyudi, Riki Andika, Rendika, Feliana, Sri Suryani, Melinda, Leny, dan semuanya yang tidak tersebut namanya
12. Teman-teman dikomunitas Sumatra Cyber Security (SCS) yang telah banyak mensupport saya dari belakang.

Semoga dengan terselesainya tugas akhir ini dapat bermanfaat untuk menambah wawasan dan pengetahuan bagi kita semua dalam mempelajari *deteksi serangan DDoS pada jaringan internet of things dengan menggunakan algoritma naïve bayes.*

Dalam Penulisan tugas akhir ini penulis berusaha semaksimal mungkin, jika terdapat kesalahan ataupun perbedaan pendapat bisa kita diskusikan sambal ngopi agar menjadi lebih baik dimasa yang akan datang.

Jakarta, Juli 2020

Penulis

Patterns Recognition of DDoS Attack on Internet of things (IoT) Network Using Naïve Bayes Algorithm

Johan Wahyudi (09011281320031)
Departement of Computer Engineering, Faculty of Computer Science
Sriwijaya University
Email: emailjohanwahyudi@gmail.com

Abstract

Pattern recognition of attack is one of way that can be used to be able to detect attacks that accur on the network. The attacks can be identified by pattern from denial of service attack that occur on internet of things network. in this research, the network build from four nodes with sensors on each nodes, where each sensor will read the data that will be send to the Raspberry Pi machine as an aggregator node which will then be forwarded to the server machine directly as an visualization dashboard using zigbee protocol for communication. DDoS attack makes a flood request thereby make network will be busy with abnormal traffic. attack pattern from DDoS attack can be recognized from the following parameters, such as no_packet, ip_dst, frame_number, protocol, time, package_length, ip_src, and info_packet. in this research, the algorithm used for detection DDoS Attack is Naïve bayes algorithm with the final results obtaining an avarage value 99.94% accuracy, 99.9% Precision, and 99.9% recall value.

Keywords*: DDoS, Internet of things, Zigbee, Pattern recognition, Naïve Bayes.*

Sistem Deteksi Serangan DDoS Menggunakan Algoritma Naïve Bayes pada Jaringan Internet of things

Johan Wahyudi (09011281320031)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Universitas Sriwijaya
Email: emailjohanwahyudi@gmail.com

Abstrak

Fokus penelitian ini ialah pada deteksi serangan *distribute denial of service* (*DDoS*), dengan mengenali pola dari serangan *distribute denial of service* (*DDoS*) yang terjadi pada jaringan *internet of things*, jaringan *internet of things* yang dibangun dalam penelitian ini memiliki empat *node* dengan sensor pada setiap *node*nya, dimana setiap sensor akan melakukan pembacaan data yang akan dikirim ke mesin *Raspberry Pi* yang berfungsi sebagai *node* agregator yang selanjutnya akan di*forward* ke mesin server sekaligus sebagai *dashboard* visualisasi dengan menggunakan protokol komunikasi *zigbee*. Serangan *distribute denial of service* merupakan serangan yang bersifat *connectionless* yang melakukan *flooding request* sehingga dapat membuat jaringan menjadi sibuk dengan traffic yang tidak normal. Pola serangan *distribute denial of service* pada protokol zigbee dapat dikenali dari beberapa parameter berikut, seperti *no_packet, ip_dst, frame_number, protocol, time, packet_length, ip_src, dan info_packet*. Pada penelitian ini, algoritma yang digunakan untuk deteksi serangan DDoS ialah algoritma *Naïve Bayes*, dengan hasil akhir penelitian memperoleh nilai rata-rata akurasi 99,94%, presisi 99,9%, dan nilai recall sebesar 99,9%.

Kata Kunci: *Distribute denial of service, internet of things, DDoS, Naïve bayes, Zigbee*

DAFTAR ISI

Halaman

BAB III. METODOLOGI PENELITIAN

BAB IV. HASIL DAN ANALISA SEMENTARA

BAB V. KESIMPULAN SEMENTARA

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I. PENDAHULUAN

1.1 Latar Belakang

Internet of things (IoT) merupakan istilah untuk jaringan cerdas yang menghubungkan semua hal ke internet untuk tujuan bertukar informasi dengan menggunakan protokol yang telah di sepakati, jadi siapapun dan dimanapun bisa mengakses dari mana saja [1]. Pada jaringan IoT hampir semua perangkat terhubung secara nirkabel dengan sensor-sensor dan semua perangkat IoT dapat berinteraksi satu sama lain tanpa campur tangan manusia. IoT biasa digunakan untuk berbagai layanan, seperti *smart home*, *smart city*, dan *smart environment*. Dengan berkembangnya layanan atau aplikasi IoT, ada begitu banyak isu dan masalah yang timbul, salah satunya ialah isu dari sisi keamanan yang tidak bisa diabaikan. Pada sistem IoT semua perangkat terhubung ke internet yang bisa diakses dari mana saja, sehingga apabila sisi keamanan jaringan IoT tidak diperhatikan maka informasi penting dan rahasia bisa saja bocor ke orang yang tidak memiliki hak [1].

Serangan terhadap layanan atau jaringan IoT dapat dilakukan pada beberapa sektor, seperti pada *Radio Frequency Identifier* (RFID) dan sensor-sensor di *perception layer*, protokol komunikasi seperti *zigbee*, *wifi*, dan GPRS pada *network layer*, serta pada sisi layanan aplikasi di *application and service layer*. Pada penelitian sebelumnya [2],[3],[4] dijelaskan bahwa salah satu serangan yang menjadi ancaman terbesar dalam sistem IoT ialah serangan DDoS (*Distributed Denial of Service*). DDoS merupakan salah satu metode penyerangan yang dilakukan oleh Attacker untuk menghabiskan sumber energi seperti bandwidth dan meningkatkan konsumsi energi yang mengakibatkan sumber energi pada perangkat akan cepat habis.

Pada penelitian [5] menyebutkan ada beberapa hal yang harus diperhatikan dalam membangun sistem IoT diantaranya adalah (1) *Confidentialy* (2) *Integrity* (3) *Availability* (4) *Authenticity*. Ada banyak jenis dari serangan DDoS, diantaranya yaitu (1) *UDP Flood* (2) *ICMP/Ping Flood* (3) *Ping of Death* (5)

Zero-Day DDoS. Untuk mencegah dan mengatasinya dibutuhkan mekanisme dan sistem pendeteksi dini yang mumpuni, salah satunya ialah dengan mengimplementasikan *intrusion detection system* (IDS).

Pada penelitian [4] dijelaskan bahwa IDS adalah suatu proses monitoring kejadian yang terjadi pada sistem komputer atau jaringan, IDS dapat melakukan inspeksi terhadap lalu lintas *inbound* dan *outbound* dalam sebuah sistem atau jaringan, serta menganalisanya untuk mengetahui aktivitas tersebut termasuk normal atau intrusi. Ada beberapa pendekatan yang bisa dilakukan dalam penelitian IDS, diantaranya (1) *Rule* atau *Signature Based Approaches* (2) *Anomaly Based Approaches* (3) *Hybrid Based*.

Pada tugas akhir ini, akan diimplementasikannya IDS pada lingkungan IoT dengan menggunakan algoritma *Naive Bayes*. Algoritma *Naive Bayes* merupakan salah satu metode *machine learning* yang menggunakan perhitungan probabilitas. Algoritma ini memanfaatkan metode probabilitas dan statistik untuk memprediksi probabilitas di masa depan berdasarkan pengalaman di masa sebelumnya [5].

1.2 Tujuan

Adapun tujuan yang hendak dicapai dalam penelitian tugas akhir ini adalah sebagai berikut :

1. Mengimplementasikan *Intrusion Detection System* pada Jaringan IoT.
2. Menerapkan *Instrusion Detection System* berbasis *machine learning* dengan menggunakan algoritma *naive bayes*.
3. Mengetahui kelebihan serta kekurangan dari algortima *naive bayes* sebagai *instrusion detection system* pada jaringan IoT diprotokol *zigbee*.

1.3 Manfaat

Adapun manfaat yang didapat dari penelitian tugas akhir ini diantarnya:

1. Dapat digunakan sebagai alternatif metode keamanan pada jaringan IoT terkhusus pada jaringan yang menggunakan protokol *Zigbee*.

2. Dapat menghasilkan *intrusion detection system* pada jaringan IoT dengan menggunakan algoritma *naive bayes* terkhusus pada serangan *Distributed Denial of service* (DDoS).

1.4 Rumusan Masalah

Berdasarkan latar belakang yang telah ditulis diatas, didapat perumusan masalah sebagai berikut:

1. Bagaimana merancang sebuah sistem pengamanan *intrusion detection system* berbasis *machine learning* dengan algortima *naive bayes* pada jaringan IoT.
2. Bagaimana mengidentifikasi serangan *distributed denial of service* (DDoS) pada jaringan IoT terkhusus pada protokol *zigbee* menggunakan algoritma *naive bayes* yang bersifat statistik.
3. Bagaimana membangun sistem IDS dan cara kerja dari sistem untuk mendeteksi serangan *distributed denial of service* (DDoS).

1.5 Batasan Masalah

Batasan masalah pada tugas akhir ini antara lain :

1. Protokol yang digunakan dalam penelitian ini ialah *Zigbee*.
2. Sistem yang dibangun memiliki 3 (tiga) *end node*, 1 (satu) *router*, dan 1 (satu) koordinator.
3. Mekanisme deteksi berasaskan *Statistical-based Detection*.
4. Algoritma yang digunakan untuk mendeteksi serangan *distributed denial of service* (DDoS) adalah *naive bayes*.
5. Tidak membahas teknik pendeteksian serangan lain, selain serangan *distributed denial of service* (DDoS).
6. Sensor yang digunakan pada sisi *end node* adalah sensor suhu (DHT 22) dan sensor gas atau asap (MQ-2).
7. Pada setiap end node terdapat 2 (dua) buah sensor.
8. Pengujian sistem dilakukan secara *offline*.

1.6 Metodologi Penelitian

Metodologi yang digunakan dalam penelitian ini melalui beberapa tahapan, yaitu:

1. Tahap Pertama (Studi Pustaka)

Tahap ini dilakukan dengan cara mengkaji dan mempelajari literatur dan referensi berupa naskah ilmiah, buku tentang konsep IoT, konsep *machine learning*, serta cara kerja algoritma *naive bayes* dan algoritma lainnya sehingga dapat menunjang metodologi yang akan diterapkan pada penelitian ini.

2. Tahap Kedua (Perancangan Sistem)

Tahap ini merupakan tahap dimana menentukan spesifikasi perangkat keras, tipe sensor dan bahasa pemprograman yang dipakai untuk membangun sistem secara keseluruhan, setelah itu, barulah sistem dibangun dengan mengemplementasikan algoritma *naive bayes* sebagai *intrusion detection system* pada sisi koordinator.

3. Tahap Ketiga (Pengujian)

Setelah semua sistem selesai dibangun dan dikonfigurasi, selanjutnya dilakukan pengujian sesuai dengan batasan masalah dan beberapa parameter pengukuran yang ditetapkan untuk mendapatkan hasil yang optimal.

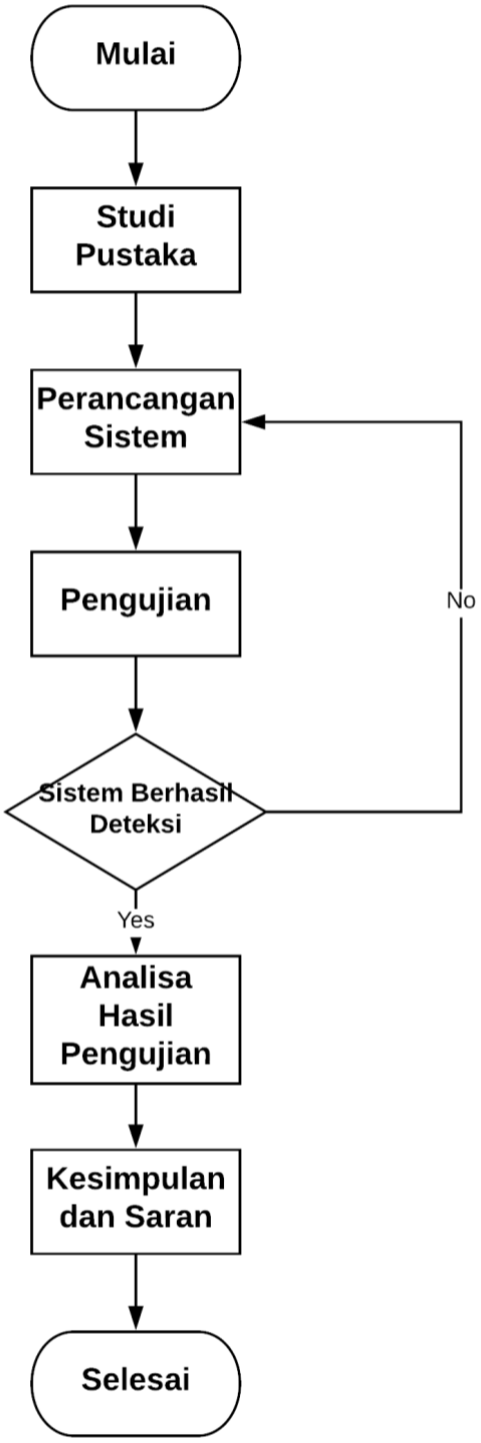
4. Tahap Keempat (Analisa)

Hasil dari pengujian pada tahap sebelumya dilakukan analisa, dengan tujuan mengetahui kekurangan pada hasil perancangan dan faktor apa saja yang menjadi penyebabnya sehingga dapat dilakukan pengembangan pada penelitian selanjutnya.

5. Tahap Kelima (Kesimpulan dan Saran)

Pada tahap ini akan dilakukan penarikan kesimpulan berdasarkan studi pustaka, hasil perancangan sistem dan hasil analisa kerja sistem *intrusion detection system* yang dibangun, dan beberapa poin saran dari penulis untuk penelitian selanjutnya.

Pada gambar 1.1 berikut, ditampilkan metodologi penelitian secara visual dalam bentuk diagram alir yang mempresentasikan proses dari pelaksanaan penelitian :



Gambar 1.1. Diagram Alir Metodologi Penelitian

1.7 Sistematika Penelitian

Untuk lebih memudahkan dalam proses penyusunan tugas akhir dan memperjelas konten dari setiap bab, maka dibuat suatu sistematika penulisan sebagai berikut:

BAB I. PENDAHULUAN

Bab ini berisi penjelasan secara sistematis mengenai landasan topik penelitian yang meliputi latar belakang, tujuan, manfaat, rumusan dan batasan masalah, kemudian metodologi penelitian, dan yang terakhir mengenai sistematika penulisan.

BAB II. TINJAUAN PUSTAKA

bab ini berisi dasar teori penelitian mengenai protokol *zigbee*, *intrusion detection system*, *DDoS attack*, arsitektur *Internet of Things*, dan algoritma *naive bayes* yang berkaitan langsung dengan penelitian ini.

BAB III. METODOLOGI PENELITIAN

Bab ini menjelaskan secara sistematis, bagaimana proses penelitian dilakukan. Penjelasan pada bab ini meliputi tahapan perancangan sistem dan penerapan metode penelitian.

BAB IV. PENGUJIAN DAN ANALISIS

Bab ini menjelaskan hasil pengujian yang dilakukan serta analisis dari data yang diperoleh dari hasil pengujian yang dilakukan.

BAB V. KESIMPULAN

Bab ini berisi kesimpulan tentang hasil penelitian yang dilakuka, serta menjawab setiap tujuan yang hendak dicapai seperti yang tercantum pada BAB 1 (Pendahuluan).

DAFTAR PUSTAKA

[1] E. D. Meutia, J. Teknik, E. Universitas, and S. Kuala, “IoT - Keamanan dan Privasi, ” 2015.

[2] K. Hengst, “DDoS through the Internet of Things,” pp. 1-9, 2016.

[3] A. a, Alfantookh, “DoS Attacks Intelligent Detection using Neural Networks,” J. King Saud Univ. -Comput. Inf. Sci., Vol. 18, no. 2006, pp. 31-51, 2006.

[4] B. B. Zarpelao, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, “A survey of intrusion in IoT,” J. Netw. Compt. Appl., 2017.

[5] V. Hema and C. E. Shyni, “DoS Attack Detection Based on Naive Bayes Classifier,” Middle-East J. Sci. Red. Signal Process. Secur., Vol, 23, pp. 398-405, 2015.

[6] O. Monnier, E. Zigman, and A. Hammer, “Understanding Wireless Connectivity in the Industrial IoT,” Texas Instruments swry016, p. 46, 2015.

[7] S. Raza, L. Wallgren, and T. Voigt, “SVELTE: Real-time intrusion detection in the Internet of Things,” Ad Hoc Networks, vol. 11, no. 8, pp. 2661–2674, 2013.

[8] J. S. Reddy, “ZigBee Security,” pp. 1–22, 2004.

[9] R. Sokullu, “GTS Attack : An IEEE 802 . 15 . 4 MAC Layer Attack in Wireless Sensor Networks,” Int. J., vol. 2, no. 1, pp. 105–116, 2009.

[10] W. Razouk, G. V. Crosby, and A. Sekkaki, “New security approach for ZigBee weaknesses,” Procedia Comput. Sci., vol. 37, pp. 376–381, 2014.

[11] K. Masica and K. Masica, “Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments Networks in Process Control,” Program, no. April, 2007.

[12] I. Alsmadi and D. Xu, “Security of Software Defined Network: A Survey, ” Comput. Secur., vol. 53, pp. 79-108, 2015.

[13] P. Jokar and V. Leung, “Intrusion Detection and Prevention for Zigbee-Based Home Are Network in Smart Grids, ” IEEE Trans. Smart Grid, vol. 3053, no. January, pp. 1-1, 2016.

[14] A. A. Alfantookh, “DoS Attacks Intelligent Detection using Neural Networks,” J. King Saud Univ. - Comput. Inf. Sci., vol. 18, pp. 31–51, 2006.

[15] S. Wang, “Analysis and application of Wireshark in TCP/IP protocol teaching,” p. 4, 2010.

[16] L. K. Wadhwa, R. S. Deshpande, and V. Priye, “PT US CR,” Ad Hoc Networks, 2015.

[17] N. Vidgren, K. Haataja, J. L. Patino-Andres, J. J. Ramirez-Sanchis, and P. Toivanen, “Security threats in ZigBee-enabled systems: Vulnerability evaluation, practical experiments, countermeasures, and lessons learned,” Proc. Annu. Hawaii Int. Conf. Syst. Sci., pp 5132-5138, 2013.

[18] M.R.Zalbina, “Sistem Deteksi HTTP Menggunakan HTTP Inspect Preprocessor dan Rule Options,” pp.8-9, 2016.

[19] A. Abane, M. Daoui, S. Bouzefrane, and P. Muhlethaler, “NDN-over-ZigBee : A ZigBee Support for Named Data Networking,” Futur. Gener. Comput. Syst., 2017.

[20] K. Hong, S. Lee, and K. Lee, “Performance improvement in ZigBee-based home networks with coexisting WLANs,” Pervasive Mob. Comput., pp. 1–11, 2014.

[21] K. Choi, M. Yun, K Chae, and M. Kim, “An enchanced key management using ZigBee Pro for wireless sensor networks,” Int. Conf. Inf. Netw., pp. 399-403, 2012.

[22] S. Arabia, “Low Cost Ultrasonic Wireless Distributed Security System for Intrusion Detection,” no. September, pp. 235–238, 2013.

[23] C. Technology, “HIVE: Home Automation System for Intrusion Detection,” pp. 2–5, 2016.

[24] S. Murugan and M. Sundara Rajan, “Fuzzy based anomaly intrusion detection system for clustered WSN, ” Res. J. Appl. Sci. Eng. Technol., vol. 9, no. 9, pp. 760--769, 2015.

[25] L. Wu, A. Province, L. Kong, Z. Zhang, M. Technology, and J. Province, “Water Environment Monitoring System Based On ZigBee Wireless Sensor Network,” pp. 898–901.

[26] L. Bai, Y. Liu, and S. Qian, “Improved Routing Algorithm Based on Node Depth in ZigBee Network,” pp. 2042–2047, 2016.

[27] K. Sonar and H. Upadhyay, “A Survey: DDoS Attack on Internet of Things, ” vol. 10, no. 11, pp. 58-63, 2014.