ROUTING ATTACKS PADA PROTOKOL KOMUNIKASI *INTERNET OF THINGS* MENGGUNAKAN *SMART INTRUSION DETECTION SYSTEM*

Skripsi

diajukan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana Pendidikan Program Studi Pendidikan Teknik Informatika dan Komputer

Oleh

Eka Lailatus Sofa

NIM. 5302414006

PENDIDIKAN TEKNIK INFORMATIKA DAN KOMPUTER

JURUSAN TEKNIK ELEKTRO

FAKULTAS TEKNIK

UNIVERSITAS NEGERI SEMARANG

2019

PERSETUJUAN PEMBIMBING

Nama	: Eka Lailatus Sofa
NIM	: 5302414006
Program Studi	: S-1 Pendidikan Teknik Informatika dan Komputer
Judul Skripdi	: ***Routing Attacks* Pada Protokol Komunikasi *Internet Of Things* Menggunakan *Smart Intrusion Detection System***

Skripsi ini telah disetujui pembimbing untuk diajukan ke panitia sidang ujian skripsi Program Studi S-1 Pendidikan Teknik Informatika dan Komputer, Jurusan Teknik Elektro, Fakultas Teknik, Universitas Negeri Semarang.

Semarang, 14 Februari 2019

Pembimbing

Dr. Ir. Subiyanto, S.T., M.T
NIP. 197411232005011001

PENGESAHAN

Skripsi dengan judul ***Routing Attacks*** **Pada Protokol Komunikasi** ***Internet Of Things*** **Menggunakan** ***Smart Intrusion Detection System*** telah dipertahankan di depan panitia sidang ujian skripsi Fakultas Teknik UNNES pada tanggal 27 bulan Februari tahun 2019.

Oleh

Nama	: Eka Lailatus Sofa
NIM	: 5302414006
Program Studi	: S-1 Pendidikan Teknik Informatika dan Komputer

Panitia:

Ketua

Dr.-Ing. Dhidik Prastiyanto,S.T.,M.T
NIP. 197805312005011002

Sekretaris

Ir. Ulfah Mediaty Arief, M.T.,IPM
NIP. 196605051998022001

Penguji I

Dr. Hari Wibawanto,M.T
NIP. 196501071991021001

Penguji II

Anggraini Mulwinda,S.T.,M.Eng
NIP. 197812262005012002

Penguji III

Dr. Ir. Subiyanto,S.T.,M.T
NIP. 197411232005011001

Mengetahui:
Dekan Fakultas Teknik UNNES

Dr. Nur Qudus, M.T
NIP. 196011301990031001

PERNYATAAN KEASLIAN

Dengan ini saya menyatakan bahwa :

1. Skripsi ini adalah asli dan tulisan ini belum pernah diajukan untuk mendapatkan gelar akademik (Sarjana, Magister, dan/atu Doktor), baik di Universtas Negeri Semarang (UNNES) maupun di perguruan tinggi lain.
2. Karya tulis ini murni gagasan, rumusan, dan penelitian saya sendiri tanpa bantuan pihak lain, kecuali arahan pembimbing dan masukan Tim Penguji.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan dicantumkan dalam daftar pustaka.
4. Persyaratan ini saya buat dengan sesungguhnya dan apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pecabutan gelar yang telah diperoleh karena karya ini, serta sanksi lainnya sesuai dengan norma yang berlaku di perguruan tinggi ini.

Semarang, Februari 2019

Yang membuat pernyataan,

Eka Lailatus Sofa
NIM. 5302414006

MOTTO DAN PERSEMBAHAN

Motto:

- Belajar untuk hidup, hidup untuk belajar.
- Orang bijak belajar ketika mereka bisa. Orang bodoh belajar ketika mereka harus (Arthur Wellesley).
- Hiduplah seolah engkau mati besok. Belajarlah seolah engkau hidup selamanya (Mahatma Gandhi).

Persembahan:

1. Kedua orang tua (Bapak Pujo Yuwono dan Ibu Fatiah) atas doa dan dukungan yang telah diberikan.
2. Ketiga adik dan seluruh keluarga besar yang telah membantu.
3. Teman-teman PTIK UNNES angkatan 2014.
4. Tim Unnes Electrical Engineering Student Research Group (UEESRG).
5. Teman-teman Kos Jus Pete.

RINGKASAN

Eka Lailatus Sofa. 2019. ***Routing Attacks* Pada Protokol Komunikasi *Internet Of Things* Menggunakan *Smart Intrusion Detection System***. Skripsi. Pendidikan Teknik Informatika dan Komputer. Jurusan Teknik Elektro. Fakultas Teknik. Universitas Negeri Semarang. Dr. Ir. Subiyanto, S. T., M. T.

Internet of Thing (IoT) saat ini sudah mulai berkembang, dilihat dari perwujudannya mulai dari adanya *smart city, smart home, smart street, smart industry* yang memanfaatkan internet untuk memantau informasi yang dibutuhkan oleh manusia. Meskipun sudah dienkripsi dan diautentikasi, jaringan IPv6 dan 6LoWPAN yang dapat menghubungkan benda-benda yang terbatas sumber daya di IoT masih belum dapat diandalkan. Hal ini dikarenakan benda-benda tersebut masih dapat terpapar oleh serangan nirkabel *(routing attacks)* yang berasal dari jaringan 6LoWPAN dan internet. Oleh karena itu, *Intrusion Detection System* (IDS) diperlukan untuk mengatasi *routing attacks* dan menganalisis aktivitas mencurigakan yang ada dalam jaringan.

Pada skripsi ini, *Smart Intrusion Detection System* berbasis *Compression Header Analyzer* akan diinvestigasi lebih lanjut dalam menganalisis varian baru model *routing attacks* pada jaringan IoT. *Features selection* berupa *Best First Search* (BFS) dan *Greedy Stepwise* (GS) dengan *Correlation Feature Selection* (CFS) digunakan untuk memilih fitur signifikan yang dapat membedakan antara serangan dan non-serangan. Sedangkan *machine learning algorithm* (*Random Forest, J48, Logistic, MLP, Naïve Bayes* dan *SMO*) digunakan untuk mengklasifikasikan serangan di IoT.

Hasil simulasi menunjukkan bahwa *Smart Intrusion Detection System* berbasis *Compression Header Analyzer* dapat mendeteksi antara serangan dan non-serangan. Selain itu, enam *machine learning algorithm* yang digunakan dapat menunjukkan tingkat akurasi dalam mendeteksi *routing attacks* yang ada.

Kata kunci : *Compression header, feature selection*, IoT, *machine learning algorithm, smart intrusion detection system*

PRAKATA

Puji syukur penulis panjatkan kehadirat Allah SWT atas segala nikmat, rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan skripsi yang berjudul **"*Routing Attacks* Pada Protokol Komunikasi *Internet Of Things* Menggunakan *Smart Intrusion Detection System*"**.

Skripsi ini disusun dalam rangka menyelesaikan studi strata yang merupakan salah satu syarat untuk memperoleh gelar Sarjana Pendidikan pada Program Studi Pendidikan Teknik Informatika dan Komputer, Jurusan Teknik Elektro, Fakultas Teknik, Universitas Negeri Semarang. Penulis menyadari sepenuhnya dalam menyelesaikan skripsi ini tidak lepas dari bantuan orang lain. Oleh karena itu, penulis mengucapkan terimakasih kepada :

1. Prof. Dr. Fathur Rokhman, M. Hum, Rektor Universitas Negeri Semarang.
2. Bapak Dr. Nur Qudus, M.T., Dekan Fakultas Teknik Universitas Negeri Semarang.
3. Bapak Dr. Ir. Subiyanto, S.T., M.T., Dosen Pembimbing yang telah memberikan bimbingan dan arahan kepada penulis dalam penyusunan skripsi ini.
4. Dosen Penguji yang telah memberikan masukan yang sangat berharga untuk menambah bobot dan kualitas skripsi ini.
5. Segenap dosen dan karyawan Jurusan Teknik Elektro Universitas Negeri Semarang.
6. Bapak, Ibu serta keluarga yang selalu memberikan doa, semangat, serta motivasi.
7. Serta berbagai pihak yang telah memberikan bantuan untuk karya tulis ini, yang tidak dapat disebutkan satu per satu.

Penulis berharap semoga skripsi ini dapat bermanfaat bagi semua pihak khususnya bagi penulis dan pembaca pada umumnya.

Semarang, Februari 2019

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB I

PENDAHULUAN

1.1 Latar Belakang

Internet of Things (IoT) merupakan suatu konsep teknologi yang bertujuan untuk memperluas manfaat dari konekvitas internet yang ada saat ini. *Internet of Thing* memungkinkan pertukaran data melalui ketersediaan semua objek yang berkaitan dengan pengguna (Kim & Lee, 2017). Dengan adanya IoT, meningkatkan penggunaan benda-benda fisik menjadi objek digital, mulai dari *smart city*, *smart home, smart street*, dan *smart industry*, yang menggunakan internet untuk memantau informasi yang dibutuhkan manusia (Sonar & Upadhyay, 2016).

Internet of Things menyediakan kemampuan bagi manusia dan komputer untuk belajar dan berkomunikasi dari miliaran hal yang meliputi sensor, aktuator, layanan dan objek yang terhubung ke internet lainnya (Ngu *et al.*, 2016). Teknologi utama dalam realisasi sistem IoT adalah *middleware,* yang biasanya digambarkan sebagai sistem perangkat lunak yang dirancang untuk menjadi perantara antara perangkat dan aplikasi IoT (Ngu *et al.*, 2016). *Middleware* memainkan peran penting karena bertanggung jawab atas sebagian besar kecerdasan dalam IoT, mengintegrasikan data dari perangkat, memungkinkan perangkat untuk berkomunikasi, dan membuat keputusan berdasarkan data yang dikumpulkan (Cruz *et al.*, 2018).

Sistem IoT sendiri mengacu pada penggunaan protokol internet standar untuk komunikasi manusia ke benda maupun benda ke benda dalam jaringan

tertanam (Heer *et al.*, 2011). Protokol internet pada objek di IoT menggunakan IPv6 untuk mengakomodasi ruang di internet, karena ruang alamat pada IPv4 yang terbatas (Pavan Pongle, 2015). Shelby & Bormann (2009) menyebutkan bahwa ukuran *frame* pada protokol internet tradisional memerlukan tautan dengan panjang *frame* yang cukup (minimum 1280 byte untuk IPv6), dan protokol aplikasi yang berat membutuhkan *bandwidth* yang besar. Hal tersebut merupakan salah satu persyaratan yang membatasi IoT ke perangkat dengan prosesor yang kuat, sistem operasi dengan tumpukan TCP/IP lengkap, dan tautan komunikasi yang mampu mengakses IP.

Kemudian perusahaan *Internet Engineering Task Force* (IETF) menciptakan 6LoWPAN untuk mengatasi masalah tersebut dan secara khusus mengaktifkan IPv6 untuk digunakan dengan perangkat dan jaringan yang tertanam kabel (Shelby & Bormann, 2009). 6LoWPAN (IPv6 *over Low-power Wireless Personal Area Network*) memungkinkan untuk digunakan di lingkungan IoT (Pongle & Chavan, 2015). 6LoWPAN telah banyak digunakan sebagai lapisan adaptasi antara protokol standar IPv6 dan lapisan tautan IEEE 802.15.4 (Napiah *et al.*, 2018).

Beberapa penelitian telah meneliti keamanan pesan untuk IoT, yaitu menggunakan *lightweight* DTLS (Kothmayr, 2011), IPsec (Raza, S., Duquennoy, 2011), dan keamanan lapisan tautan IEEE 802.15.4 (Kamesh & Sakthi Priya, 2014). Namun meskipun sudah diamankan dengan enkripsi dan otentikasi, jaringan IPv6 dan 6LoWPAN tidak dapat diandalkan untuk menghubungkan perangkat-perangkat yang terbatas sumber daya di IoT. Hal ini karena perangkat-perangkat tersebut

masih dapat terpapar oleh serangan nirkabel dari dalam jaringan 6LoWPAN dan internet (Wallgren *et al.,* 2013). Serangan yang beroperasi di lapisan jaringan disebut dengan *routing attacks* (Amish & Vaghela, 2016). *Routing attacks* meliputi *wormhole, sinkhole, blackhole, spoofing*, *hello flood*, *selective forwarding* dan sebagainya (CHELLI, 2015).

Oleh karena itu, untuk mengatasi *routing attacks* yang ada maka *Intrusion Detection System* (IDS) perlu diterapkan untuk mengatasi serangan di IoT (Raza *et al.*, 2013). IDS menganalisis aktivitas di jaringan dan mencoba mendeteksi perilaku jahat dan/atau penyusup yang mengganggu jaringan (Raza *et al.,* 2013). Ada dua kelas penting dalam IDS, yaitu IDS berbasis *signature* dan IDS berbasis *anomaly*. Sedangkan IDS berbasis *hybrid* merupakan gabungan dari *signature* dan *anomaly* (Alrajeh *et al.,* 2013).

Penelitian yang dilakukan oleh Aydin *et al* (2009) mengusulkan IDS berbasis *hybrid* dengan menggabungkan *Packet Header Anomaly Detection* (PHAD) dan *Network Traffic Anomaly Detection* (NETAD) menggunakan SNORT. Model ini bergantung pada cepatnya perubahan statistik jaringan dalam jangka pendek.

Raza *et al* (2013) mengusulkan sebuah IDS baru untuk IoT yang disebut dengan SVELTE. Target SVELTE yaitu serangan *routing* yang meliputi *sinkhole, selective forwarding, spoofing* dan dapat diperluas untuk mendeteksi serangan lain. SVELTE menggunakan RPL yang memiliki dua komponen utama yaitu 6LoWPAN *Mapper (6Mapper)* dan modul deteksi intrusi. SVELTE juga menggunakan IDS

berbasis hibrida. Selain itu, Pongle & Chavan (2015b) mengusulkan IDS untuk IoT yang mampu mendeteksi serangan *wormhole*. Metode yang diusulkan menggunakan informasi lokasi *node* dan informasi *neighbor* untuk mengidentifikasi serangan *wormhole*. Penempatan sistem IDS berbasis hiribida, dimana modul terpusat pada IPv6 *border router* (6BR) dan modul terpusat pada *node* sensor bekerja sama untuk mendeteksi serangan.

Akan tetapi SVELTE (Raza *et al.*, 2013) dan IDS (Pongle & Chavan, 2015) kurang efektif untuk menentukan serangan kompleks, karena hanya mendeteksi serangan tertentu. Kemudian Napiah *et al* (2018) mengusulkan *Compression Header Analyzer Intrusion Detection System* (CHA-IDS) yang dapat menganalisis data *compression header* 6LoWPAN untuk mengurangi berbagai serangan individu dan kombinasi yang terdapat pada jaringan IoT. Evaluasi CHA-IDS menggunakan tiga jenis serangan antara lain *hello flood, sinkhole,* dan *wormhole attack.* Diuji mengunakan lima *machine learning algorithm* yaitu *J48, Logistic, MLP, Naïve Bayes,* dan *Random Forest*.

Menurut Jabez & Muthukumar (2015) *machine learning* dapat digunakan untuk mendeteksi dan mengklarifikasi serangan pada jaringan. *Machine learning* telah dikembangkan untuk menemukan algoritma terbaik dalam mesin pendeteksi pada IDS. Penelitian Meenakshi & Geetika (2014) melakukan perbandingan teknik klasifikasi yang berbeda menggukan WEKA. Tujuan dari penelitian tersebut adalah menyelidiki kinerja berbagai metode klasifikasi pada suatu data. *Bayes net* mencapai nilai akurat paling tinggi sebesar 93,33%, dibandingkan dengan algoritma lain seperti *J48, Logistic, Naïve Bayes, Rule Jrip*.

Penelitian yang dilakukan oleh Kolias *et al* (2016), menggunakan beberapa *machine learning algorithm* untuk menganalisis 156 fitur yang dikumpulkan dari jaringan 802.11. Pemilihan fitur ini dilakukan untuk memilih hanya fitur penting yang digunakan untuk mengurangi konsumsi sumber daya perangkat. Penelitian mengenai pemilihan fitur juga dilakukan oleh Kang (2015). Dalam penelitian tersebut mengusulkan algoritma pemilihan fitur berdasarkan algoritma pencarian lokal untuk memilih subset fitur yang optimal untuk IDS yang mendeteksi serangan DoS.

Dalam penelitian ini, *Intrusion Detection System* (IDS) dikembangkan untuk menganalisis tipe *routing attacks* lainnya yang ada dalam jaringan IoT. IDS menggunakan *compression header* 6LoWPAN yang dapat membedakan aktivitas normal dan abnormal. *Feature Selection* dan *Machine Learning Algorithm* digunakan untuk mendeteksi *routing attacks* pada jaringan IoT. Simulasi *routing attacks* menggunakan *Cooja Simulator* yang terdapat dalam *software Contiki* dan diuji menggunakan *software Wireshark*. *Software Weka* digunakan untuk mengklasifikasikan antara serangan dan *non*-serangan pada jaringan IoT.

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah dijelaskan, maka dapat diidentifikasi masalah dalam penelitian ini adalah jaringan IPv6 dan 6LoWPAN tidak dapat diandalkan untuk menghubungkan perangkat-perangkat yang terbatas sumber daya di IoT, meskipun sudah diamankan dengan enkripsi dan otentikasi. Hal ini

disebabkan karena perangkat-perangkat tersebut masih dapat tepapar oleh *routing attacks* dari dalam jaringan 6LoWPAN dan internet.

1.3 Pembatasan Masalah

Berdasarkan identifikasi masalah di atas, maka penelitian ini dibatasi permasalahannya dengan asumsi sebagai berikut :

1. Pada skripsi ini membahas mengenai *Smart Intrusion Detection System* berbasis *Compression Header Analyzer* dalam menganalisis varian baru model *routing attacks* yang terdapat pada *Internet of Things.*
2. Skripsi ini hanya sebatas simulasi mengenai *routing attacks* menggunakan *software Cooja Simulator* di dalam *Contiki OS.*
3. *Smart Intrusion Detection System* menggunakan fitur yang terdapat pada *compression header* 6LoWPAN.
4. Penentuan fitur signifikan pada *compression header* 6LoWPAN menggunakan algoritma pencarian *Best-First Search* (BFS) dan *Greedy-Stepwise* (GS) dengan *Correlation Features Search* (CFS).
5. *Machine learning algorithms* yang digunakan untuk klasifikasi *routing attacks* ada 6, antara lain *Random Forest, J48, Logistic,* MLP, *Naïve Bayes,* dan *SMO.*
6. Model *Routing attacks* yang terdeteksi meliputi *selective forwarding attack* dan *sinkhole attack.*
7. *Software* yang digunakan yaitu *Contiki* 3.0, *VMware* 9.0, *Weka* 3.9 dan *Wireshark* 1.9.2.

1.4 Rumusan Masalah

Pada identifikasi masalah yang telah dijelaskan bahwa perangkat IoT masih dapat terkena serangan dari jaringan 6LoWPAN dan internet, sehingga perlu diterapkannya IDS untuk mengatasi serangan pada jaringan IoT. Pada saat ini, telah dikembangkan model CHA-IDS yang dapat menganalisis model *routing attacks*. Akan tetapi, CHA-IDS belum diselidiki lebih lanjut untuk mendeteksi tipe *routing attacks* yang lainnya. Oleh karena itu, dalam penelitian ini akan membahas Bagaimana kinerja *Smart Intrusion Detection System* berbasis *Compression Header Analyzer* dalam menganalisis model *routing attacks* lainnya yang ada di jaringan IoT?

1.5 Tujuan Penelitian

Berdasarkan rumusan masalah tersebut, maka tujuan dari penelitian ini adalah untuk mengetahui kinerja *Smart Intrusion Detection System* berbasis *Compression Header Analyzer* dalam menganalisis model *routing attacks* lainnya pada jaringan IoT. Cara yang dapat dilakukan yaitu menerapkan kerangka CHA-IDS yang dapat menangkap dan mengelola data mentah yang diperoleh dari *compression header* 6LoWPAN untuk mengumpulkan data, menganalisis, dan menentukan tindakan sistem, sehingga berbagai *routing attacks* pada jaringan IoT dapat dikurangi.

1.6 Manfaat Penelitian

Berdasarkan tujuan penelitian yang telah diuraikan, manfaat yang diharapkan dalam penelitian ini adalah :

1. Hasil penelitian ini dapat memberikan pengetahuan mengenai *Smart Intrusion Detection System* berbasis *Compression Header Analyzer* kepada masyarakat secara umum dan industri secara khusus.
2. Menjadi pemodelan implementasi *Smart Intrusion Detection System* yang nantinya dapat diimplementasikan pada jaringan IoT di dunia nyata.
3. Menjadi referensi pada penelitian selanjutnya yang berkaitan dengan IDS pada jaringan IoT.

1.7 Penegasan Istilah

Agar tidak terjadi penafsiran yang berbeda pada penelitian ini, maka diberikan penjelasan istilah sebagai berikut :

1. *Routing Attacks*

   Serangan yang beroperasi atau menganggu lapisan jaringan.

2. Protokol Komunikasi

   Sebuah aturan yang mengatur terjadinya hubungan, komunikasi dan perpindahan data antara dua atau lebih komputer.

3. *Internet of Things* (IoT)

   Sistem yang terdiri dari berbagai perangkat atau sensor yang terhubung dengan internet.

4. *Smart Intrusion Detection System*

   Sebuah metode *Intrusion Detection System* (IDS) berbasis *Compression Header Analyzer* untuk menganalisis *routing attacks* yang ada pada IoT.

5. Simulasi

   Proses penggambaran atau peniruan dari sesuatu yang nyata dengan peragaan berupa model statistik atau pemeranan.

BAB II

KAJIAN PUSTAKA DAN LANDASAN TEORI

2.1 Kajian Pustaka yang Relevan

Berbagai penelitian yang telah dilakukan oleh peneliti terdahulu mengenai penelitian ini, antara lain:

1. Penelitian Aydin *et al* (2009) dengan judul *"A hybrid intrusion detection system design for computer network security"*. Mengusulkan IDS berbasis hibrida dengan menggabungkan dua pendekatan dalam satu sistem. IDS hibrida diperoleh dengan menggabungkan *Packet Header Anomaly Detection* (PHAD) dan *Network Traffic Anomaly Detection* (NETAD) yang merupakan IDS berbasis anomali dengan menggunakan *tools open source* seperti SNORT. Sistem dievaluasi dengan membandingkan jumlah serangan yang terdeteksi oleh IDS dan menunjukkan bahwa IDS hibrida adalah sistem yang lebih kuat dari IDS lainnya.
2. Penelitian Raza *et al* (2013) dengan judul *"SVELTE : Real-Time Intrusion Detection in Internet of Things"*. Mengusulkan sebuah IDS untuk IoT yang disebut dengan SVELTE. Metode ini menargetkan *routing attacks* seperti *sinkhole, spoofing, selective forwarding,* dan serangan lainnya. RPL sebagai protokol *routing* dan pendekatan hibrida digunakan dalam metode ini. SVELTE memiliki tiga modul terpusat utama yang ditempatkan di IPv6 *Border Router* (6BR), yaitu:

a. Modul pertama, yang disebut dengan 6LoWPAN *Mapper (6Mapper)*, mengumpulkan informasi tentang jaringan RPL dan merekonstruksi jaringan di 6BR.
b. Modul kedua adalah komponen deteksi intrusi yang menganalisis data yang dipetakan dan mendeteksi intrusi.
c. Modul ketiga, *mini firewall* distribusi dirancang untuk melindungi jaringan 6LoWPAN melawan penyerang global dari internet.

SVELTE diterapkan dan dievaluasi menggunakan *Cooja Simulator* yang terdapat di *OS Contiki*. Namun *True Positive rate* (TP) dalam sistem ini tidak 100%. Selain itu, *overhead* SVELTE cukup kecil untuk digunakan pada *node* terbatas, dengan kapasitas energi dan memori yang terbatas.

3. Penelitian Pongle & Chavan (2015a) dengan judul *"Real Time Intrusion and Wormhole Attack Detection in Internet of Things"*. Mengusulkan IDS untuk IoT yang mampu mendeteksi serangan *wormhole*. Metode ini menggunakan informasi lokasi *node* dan *neighbor* untuk mengidentifikasi serangan *wormhole* dan kekuatan sinyal yang diterima untuk mengidentifikasi *node* penyerang. Penempatan sistem IDS menggunakan pendekatan hibrida, dimana modul terpusat pada modul 6BR dan modul distribusi pada *node* sensor bekerja sama untuk mendeteksi serangan. Simulasi sistem dijalankan pada *Cooja Simulator* yang terdapat pada *OS Contiki*. Metode yang diusulkan mempunyai tingkat deteksi 94% yang baik untuk lingkungan yang dibatasi sumber daya. Selain itu, konsumsi RAM/ROM sangat kecil dibandingkan dengan ukuran total yang tersedia.

4. Penelitian Napiah *et al* (2018) dengan judul *"Compression Header Analyzer Intrusion Detection System (CHA-IDS) for 6LoWPAN Communication Protocol"*. CHA-IDS menganalisis data *compression header* 6LoWPAN untuk menguragi serangan individu dan kombinasi. Pengujian sistem menggunakan enam algoritma untuk menemukan metode klasifikasi yang dapat membedakan antara serangan dan *non*-serangan. Dievaluasi dengan tiga jenis serangan antara lain *hello flood, sinkhole, wormhole*. Selain itu akurasi deteksi, overhead energi, dan konsumsi energi dibandingkan dengan penelitian sebelumnya.
5. Penelitian Meenakshi & Geetika (2014) dengan judul *"Survey on Classification Methods Using WEKA"*. Melakukan perbandingan teknik klasifikasi yang berbeda menggunakan WEKA. Tujuannya adalah untuk menyelidiki kinerja berbagai metode klasifikasi pada suatu data. Perhitungan menggunakan contoh *dataset healthcare*. *Bayes net* menunjukkan tingkat akurat yang paling tinggi mencapai 93,33%, dibandingkan dengan algoritma lain seperti *J48, Logistic, Naïve Bayes, Rule Jrip*. Klasifikasi *Bayes net* memiliki kesalahan rata-rata terendah dibandingkan dengan yang lain.
6. Penelitian (Sahu & Mehtre, 2015) dengan judul *"Network Intrusion Detection System Using J48 Decision Tree"*. Menggunakan *dataset* Kyoto 2006+ untuk evaluasi pada *Network Intrusion Detection System* (NIDS). Selain itu, algoritma *Decision Tree* (J48) digunakan untuk mengklasifikasikan paket jaringan dalam NIDS. Untuk *training* dan *testing*,

menggunakan contoh jaringan sebesar 134665. Keakuratan mencapai 97,2% dalam mendeteksi koneksi yaitu *no attack, known attack,* dan *unknown attack.*

7. Penelitian Abbas Hassan *et al* (2015) dengan judul *"Intrusion Detection System Using Weka Data Mining Tool"*. Merancang *Intrusion Detection System* (IDS) menggunakan *Weka Data Mining Software* untuk memeriksa keberadaan intrusi dan mengklasifikasikannya ketika terdeteksi untuk mengetahui jenis intrusi. Dalam penelitian ini, menggunakan *dataset* intrusi deteksi KDD CUP 99. Ada sembilan model yang digunakan untuk perhitungan yaitu *J48, Random Tree, Random Forest, Simple Chart, J48 Graft, Naïve Bayes, SMO, RBFnetwork*. Hasil dari perhitungan tersebut, menunjukkan bahwa *Random Forest* mencapai hasil yang paling baik dalam akurasi yaitu 97,53%.
8. Penelitian Kolias *et al* (2016) dengan judul *"Intrusion Detection in 802.11 Networks: Empirical Evaluation of Threats and a Public Dataset"*. Menggunakan beberapa *machine learning algorithm* untuk menganalisis 156 fitur yang dikumpulkan dari jaringan 802.11. Kemudian hanya 20 fitur penting dari 156 fitur yang dapat digunakan sebagai indikator IDS untuk mendeteksi adanya serangan. Pemilihan fitur ini dilakukan untuk memilih hanya fitur penting sekaligus untuk mengurangi konsumsi sumber daya pada perangkat.
9. Penelitian Kang (2015) dengan judul *"A Feature Selection Algorithm to Find Optimal Feature Subsets for Detecting DoS Attacks"*. Mengusulkan

algoritma pemilihan fitur berdasarkan algoritma pencarian lokal untuk memilih subset fitur yang optimal untuk IDS yang mendeteksi serangan DoS. Untuk mengevaluasi kinerja algoritma yang diusulkan, perbandingan dengan set fitur yang terdiri dari 41 fitur dilakukan di atas kumpulan data NSL-KDD menggunakan *Multi Layer Perceptron* (MLP). Penelitian tersebut mengkonfirmasikan bahwa meskipun hanya menggunakan sekitar setengah dari 41 fitur, tingkat akurasi dan pendeteksian serangan DoS lebih tinggi dari 41 fitur tersebut.

10. Penelitian Desale and Ade (2015) dengan judul *"Genetic Algorithm based Feature Selection Approach for Effective Intrusion Detection System"*. Mengusulkan pendekatan evolusioner untuk pemilihan fitur didasarkan pada prinsip *intersection* (irisan) pada matematika. *Genetic algorithm* (GA) digunakan sebagai metode pencarian saat memilih fitur dari *dataset* NSL-KDD. Seleksi fitur dilakukan menggunakan teknik *Feature Selection* (FS). Dari hasil eksperimen dapat disimpulkan bahwa metode yang diusulkan membantu dalam memilih jumlah minimum fitur dari data set NSL-KDD yang meningkatkan akurasi penggolongan *Naïve Bayes* bersama dengan kompleksitas waktu yang berkurang.

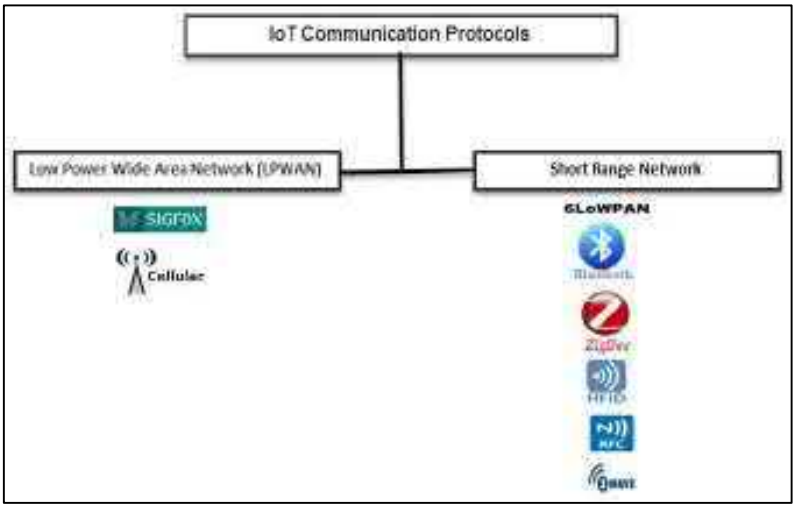
Berdasarkan kajian pustaka tersebut, maka penelitian ini bermaksud untuk mengevaluasi kinerja *Smart Intrusion Detection System* dalam menganalisis varian baru model *routing attacks* pada jaringan IoT. *Smart Intrusion Detection System* ini didasarkan pada *Compression Header Analyzer*. *Feature Selection* digunakan

dalam memilih fitur terbaik untuk mendeteksi serangan dan *Machine Learning Algorithm* digunakan untuk mengklasifikasi serangan.

2.2 *Internet of Things* (IoT)

Internet of Things (IoT) adalah sistem global dan hal-hal virtual yang terkait dengan internet. IoT akan mendorong miliaran perangkat, individu dan administrasi untuk saling terhubung dengan data trade dan informasi yang bermanfaat. Aplikasi IoT menyebar di berbagai bidang kehidupan seperti bidang kesehatan, tata kelola, pendidikan, industri, produksi, transportasi, dan sebagainya (Bauer *et al.*, 2017).

IoT terdiri dari perangkat cerdas yang berkomunikasi satu sama lain, yang saling mengumpulkan data dan bertukar data. Banyak teknologi dan protokol komunikasi nirkabel yang berbeda dapat digunakan untuk menghubungkan perangkat cerdas seperti *Internet Protocol Version* 6 (IPv6), over *Low Power Wireless Personal Area Network* (6LoWPAN), *Zigbee, Bluetooth Low Energy* (BLE), *ZWave*, dan *Near Field Communication* (NFC), yang merupakan protokol jaringan standar jangka pendek. Sedangkan *SigFox* dan *Cellular* adalah protokol standar *Low Power Wide Area Network* (LWPAN) (Al-sarawi *et al.*, 2017). Gambar 2.1 menunjukkan protokol komunikasi pada IoT.

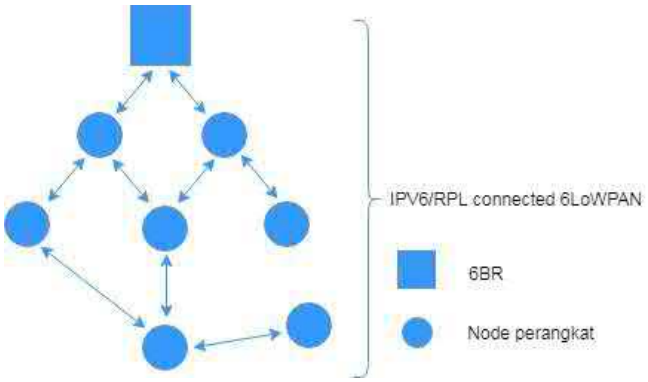


Gambar 2.1 Protokol Komunikasi IoT

(Al-sarawi *et al.*, 2017)

2.3 *IPv6 over Low-power Wireless Personal Area Network* (6LoWPAN)

6LoWPAN adalah perluasan IPv6 yang efisien kedalam lingkungan nirkabel, sehingga memungkinkan jaringan dan fitur IP *end-to-end* untuk berbagi aplikasi *embedded* (Shelby & Bormann, 2009). Semua node perangkat terhubung ke internet melalui *gateway* yang dikenal sebagai 6LoWPAN *Border Router* (6BR) yang serupa dengan *node sink* di jaringan WSN, seperti pada Gambar 2.2.



Gambar 2.2 Komunikasi Perangkat di Jaringan 6LoWPAN dengan 6BR

(Napiah *et al.*, 2018)

Destination Oriented Directed Acyclic Graph (DODAG) adalah *Routing Protocol for Low-Power and Lossy Network* (RPL) IPv6 yang bentuknya seperti topologi *tree* dengan satu *root* yang dikenal dengan *node sink*. Pembentukkan topologi ini memerlukan transmisi pesan DODAG *Information Object* (DIO) (Pongle & Chavan, 2015).

2.4 *Header Compression* 6LoWPAN

Adaptation layer menyediakan 4 tipe header dasar yang didefinisikan di 6LoWPAN, antara lain *Dispatch Header*, *Mesh Header*, *Fragmentation Header*, dan HC1 (*Header Compression* IPv6). Dalam *header compression*, 6LoWPAN mendefinisikan HC1 *encoding* sebagai skema kompresi yang dioptimalkan untuk komunikasi *link-local* IPv6. Beberapa *fields header* yang berasal dari *adaptation*, *network*, dan *transport layer* biasanya membawa nilai yang sama. Oleh karena itu, mekanisme *header compression* digunakan untuk mengkompresi *fields header* tersebut ke beberapa bit sementara (Ee *et al.*, 2010). *Header compression* merupakan parameter penting untuk mengurangi biaya *overhead* di 6LoWPAN (Shah *et al.*, 2016). Perbandingan antara *header* IPv6 dan *fields header compression* 6LoWPAN ditunjukkan pada Gambar 2.3.

Header Field	IPv6 header length	6LoWPAN HC1 length	Explanation
Version	4 bits	------	Assuming communicating with IPv6.
Traffic class	8 bits	1 bit	0 = Not compressed. The field is in full size. 1 = Compressed. The traffic class and flow label are both zero.
Flow label	20 bits		
Payload length	16 bits	------	Can be derived from MAC frame length or adaptation layer datagram size (6LoWPAN fragmentation header).
Next header	8 bits	2 bits	Compressed whenever the packet uses UDP, TCP or Internet Control Message Protocol version 6 (ICMPv6).
Hop limit	8 bits	8 bits	The only field always not compressed.
Source address	128 bits	2 bits	If Both source and destination IPv6 addresses are in link local, their 64-bit network prefix are compressed into a single bit each with a value of one. Another single bit is set to one to indicate that 64-bit interface identifier are elided if the destination can derive them from the corresponding link-layer address in the link-layer frame or mesh addressing header when routing in a mesh.
Destination address	128 bits	2 bits	
HC2 encoding	------	1 bit	Another compression scheme follows a HC1 header.
Total	40 bytes	2 bytes	Fully compressed, the HC1 encoding reduces the IPv6 header to two bytes.

Gambar 2.3 Perbandingan antara *Header Compression* IPv6 dan 6LoWPAN

(Ee *et al.*, 2010)

2.5 *Intrusion Detection System* (IDS)

TARIQAHMAD SHERASIYA (2016) menjelaskan bahwa *Intrusion Detection System* (IDS) digunakan untuk memantau lalu lintas berbahaya di *node* dan jaringan tertentu. IDS bertindak sebagai pertahanan kedua dari penyusup. Intrusi merupakan aktivitas yang tidak diinginkan atau berbahaya bagi *node* sensor. Tujuan IDS adalah untuk mengamati jaringan dan *node*, mendeteksi berbagai intrusi dalam jaringan, dan memberi tahu pengguna setelah penyusupan terdeteksi.

IDS bekerja sebagai pengamat alarm atau jaringan, sehingga menghindari kerusakan sistem dengan menghasilkan peringatan sebelum penyerang mulai menyerang. IDS dapat mendeteksi serangan *internal* yang berasal dari *node* jahat atau jaringan itu sendiri, dan serangan luar yang berasal dari jaringan luar. Ada tiga komponen pada IDS, antara lain :

1. *Monitoring*, berfungsi untuk memantau lau lintas, pola dan sumber daya.
2. *Analysis and detection*, berfungsi untuk mendeteksi intrusi sesuai algoritma yang ditentukan.
3. *Alarm*, berfungsi untuk menimbulkan alarm jika intrusi terdeteksi.

2.5.1 *Signature based* IDS

Setiap serangan bisa dideteksi sesuai pola atau *signature* yang telah ditentukan sebelumnya, yang tersimpan di *database*. Teknik ini membutuhkan pengetahuan yang spesifik tentang serangan individu. Memerlukan ruang penyimpanan lebih banyak dengan meningkatkan jumlah serangan. Teknik ini tidak dapat mengidentifikasi serangan baru, kecuali *signature* atau pola mereka ditambahkan secara manual kedalam *database*. Sehingga *database* perlu diperbarui secara teratur dengan *signature* baru untuk serangan. Terdapat dua kelemahan pada *signature based* IDS ini, yaitu dibutuhkan pengetahuan untuk membentuk pola serangan dan tidak dapat menemukan serangan baru dan sebelumnya tidak diketahui (TARIQAHMAD SHERASIYA, 2016).

2.5.2 *Anomaly based* IDS

Anomaly based IDS dikenal juga sebagai *even-based detection*. Teknik ini mengidentifikasi aktivitas berbahaya dengan menganalisis kejadian tersebut. Dalam pendekatan ini, *node* berbahaya dapat dideteksi dengan mencocokkan spesifikasi protokol saat ini dengan keadaan protokol yang didefinisikan sebelumnya. Pendekatan ini lebih efisien daripada *signature based* IDS. Namun

pendekatan ini mahal untuk objek yang dibatasi sumber daya (TARIQAHMAD SHERASIYA, 2016).

2.5.3 *Hybrid based* IDS

IDS ini merupakan penggabungan dua pendekatan dalam satu sistem, yaitu *signature* IDS dan *anomaly* IDS. *Hybrid* memungkinkan untuk mendeteksi penyalahgunaan atau serangan anomaly (TARIQAHMAD SHERASIYA, 2016). IDS berbasis *hybrid* memiliki dua modul deteksi: modul yang digunakan untuk deteksi serangan, dan modul lain yang digunakan untuk mempelajari pola normal dan abnormal (jahat) (Alrajeh *et al.*, 2013).

2.6 *Machine Learning Algorithm*

Machine learning algorithm merupakan kecerdasan buatan yang diperalajari atau disesuaikan dengan lingkungan baru. Algortima ini banyak digunakan dalam keamanan jaringan untuk lingkungan *wireless sensor network* (WSN) (Napiah *et al.*, 2018). Perbedaan *machine learning* dengan statistik yaitu statistik lebih menekankan pada pengujian hipotesis, sedangkan *machine learning* lebih mementingkan proses generalisasi sebagai pencarian melalui hipotesis yang ada (Witten *et al.*, 2011). Nath (2016) menyebutkan bahwa ada tiga kategori *machine learning*, antara lain :

2.6.1 *Supervised Learning*

Menyimpulkan fungsi dari satu set data yang diberikan (*input* dengan *output* masing-masing). Algoritma ini mengawasi data *training* dan menghasilkan *general rule (function)* yang dapat digunakan untuk memetakan *input* baru. Ada dua kategori *supervised learning*, yaitu :

a. Regresi : target *output* adalah bilangan real atau seluruh vektor bilangan real, seperti harga saham dalam 6 bulan atau suhu pada siang hari.
b. Klasifikasi : target *output* adalah label kelas seperti dalam kasus pemilihan antara positif dan negatif.

2.6.2 *Unsupervised Learning*

Tujuannya adalah untuk menemukan representasi internal yang baik dari input. Algoritma ini lebih sulit karena komputer harus belajar untuk melakukan tugas-tugas tertentu tanpa membertitahukan bagaimana melakukannya.

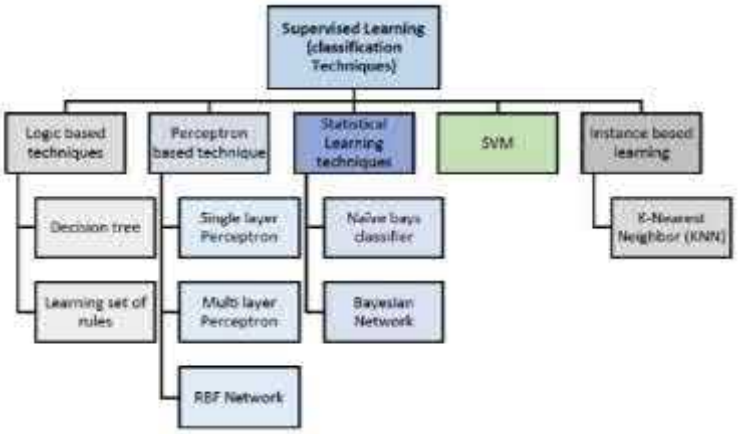
2.6.3 *Reinforcement Learning*

Pada *machine learning* ini, algoritma belajar suatu kebijakan tentang bagaimana tindakan yang diberikan pengamat tanpa mengetahui apakah telah mencapai tujuan atau tidak.

2.7 *Machine Learning Classification*

Classification (klasifikasi) adalah teknik pada *data mining (machine learning)* yang digunakan untuk memprediksi keanggotaan grup untuk contoh data

(data instance) (Soofi & Awan, 2017). Model *supervised learning* (teknik klasifikasi) ditunjukkan pada Gambar 2.4.



Gambar 2.4 *Supervised Learning* Teknik Klasifikasi

(Soofi & Awan, 2017)

Ada beberapa macam teknik klasifikasi, antara lain *Naïve Bayes*, C4.5, *K-Means Clustering*, *Support Vector Machines* (SVM), K-NN *Classifier*, dan sebagainya (Suresh & Anitha, 2011).

2.7.1 *Random Forest*

Random Forest adalah metode pembelajaran *ensemble* untuk klasifikasi (dan regresi) yang beroperasi dengan membangun banyak *decision tree* selama kelas *training* dan *output* yang merupakan mode kelas *output* oleh setiap pohon (Sarica *et al.*, 2017; Livingston, 2005). *Random Forest* membangun klasifikasi *CART tree* menggunakan mekanisme *bagging*. Dengan menggunakan *bagging*, setiap *tree node* hanya memilih sejumlah kecil fitur untuk pemisahan, yang

memungkinkan algoritma dengan cepat mengklasifikasikan data berdimensi tinggi (Rameshpant *et al.*, 2008).

2.7.2 J48

J48 adalah salah satu algoritma *decision tree*, yang mengembangkan dan meminimalkan kekurangan dari algoritma ID3 (Soofi & Awan, 2017). *Decision tree* terdiri dari *decision node* dan *leaf node*, dimana *decision node* menentukan tes untuk atribut, dan *leaf node* mewakili nilai kelas (Sahu & Mehtre, 2015). J48 memiliki tingkat akurasi yang lebih tinggi daripada algoritma *decision tree* lainnya. Dalam data mining pada *software Weka*, J48 merupakan implementasi J*ava open source* dari algoritma C4.5 (Kaur & Chhabra, 2014).

2.7.3 *Logistic*

Logictic Regression adalah model prediktif yang digunakan ketika variabel target juga digunakan sebagai variabel kategori (Meenakshi & Geetika, 2014). *Logistic Regression* menggunakan dua jenis variabel target (Meenakshi & Geetika, 2014):

a. Variabel target kategori terdiri dari dua kategori variabel, yaitu variabel biner dan dikotomi.
b. Variabel target kontinyu terdiri dari nilai yang berkisar dari 0,0 hingga 1,0 yang digunakan untuk merepresentasikan nilai probabilitas atau proporsi.

Hal ini merupakan solusi untuk masalah klasifikasi yang mengasumsikan bahwa kombinasi linier fitur yang diamati dapat digunakan untuk menentukan

probabilitas masing-masing hasil spesifik dari variabel independen (Miguel-Hurtado *et al.*, 2016).

2.7.4 *Multilayer Perceptron* (MLP)

Bentuk arsitektur dari jaringan syaraf yang terkenal adalah *multilayer perceptron* (MLP) (Sebastian, 2015). Jaringan MLP memiliki *input* yang disebut *neuron*, yang diatur dalam lapisan dengan satu lapisan yang terhubung ke lapisan terakhir atau lapisan keluaran (Jamil, 2016). MLP cocok untuk mendekati fungsi klasifikasi yang menentukan *instance* yang ditentukan oleh nilai atribut vektor menjadi satu atau lebih kelas (Sebastian, 2015).

2.7.5 *Sequential Minimal Optimization* (SMO)

Algoritma pembelajaran *Support Vector Machin*e (SVM) yang baru disebut *Sequential Minimal Optimization* (SMO) (Abbas Hassan *et al.*, 2015). SMO adalah algoritma optimasi yang digunakan untuk melatih SVM dalam klasifikasi *dataset* (S. Singaravelan, D. Murugan, 2015; Velinov, A., 2018). Dibuat oleh John Platt pada tahun 1998 di *Microsoft Research* (S. Singaravelan, D. Murugan, 2015). *Kernel polinomial* atau RBF digunakan oleh SMO untuk melatih *classifier* pendukung, dapat menggantikan nilai yang hilang dan mengubah atribut nominal menjadi biner (Abbas Hassan *et al.*, 2015). Biasanya digunakan untuk memecahkan masalah tentang *Quadratic Programming* (QP), diimplementasikan oleh *LibSVM* yang merupakan alat untuk pelatihan SVM (Rani & Purwar, 2017).

2.7.6 *Naïve Bayes*

Dalam metode *Naive Bayes* ini, ada perbedaan dalam data *numerik kontinu*. Perbedaan ini dapat dilihat ketika menentukan nilai probabilitas setiap kriteria, apakah kriteria menggunakan nilai data *string* atau nilai data *numerik* (Saleh & Nasari, 2018). *Naïve Bayes* adalah algoritma pembelajaran statistik yang menerapkan aturan *Bayes* yang disederhanakan, untuk menghitung probabilitas kategori *posterior* mengingat nilai atribut *input* dari sebuah *example situation* (Jamil, 2016). Metode *Naïve Bayes* dalam *Weka* adalah *weka.classifiers.bayes.NaiveBayes* (Tribhuvan *et al.*, 2015).

2.8 *Feature Selection Algorithm*

Feature selection (seleksi fitur) adalah langkah *preprocessing* untuk *machine learning* yang efektif dalam mengurangi dimensi, menghapus data yang tidak relevan, meningkatkan akurasi pembelajaran dan meningkatkan hasil komprehensibilitas (Doshi, 2014). *Feature selection* melakukan pencarian melalui ruang *feature subset* (Hall, 1999).

Salah satu pencarian sederhana yang disebut *greedy hill climbing*, menganggap perubahan lokal ke *feature subset*. Perubahan lokal hanya menambah dan menghapus *feature* tunggal *subset*. Penambahan *feature* pada *subset* disebut *forward selection*, sedangkan penghapusan *feature* pada *subset* disebut *backward elimination*. Selain *greedy hill climbing*, terdapat algoritma lain yang disebut *best first search*. *Best first search* merupakan strategi pencarian AI yang memungkinkan pelacakan kembali *(back tracking)* sepanjang jarur pencarian. Tidak seperti *hill*

climbing, jika jalur yang dijelajahi mulai terlihat kurang baik, *best first* dapat kembali melacak ke *subset* sebelumnya yang lebih baik dan melanjutkan penelusuran dari subset *tersebut* (Hall, 1999).

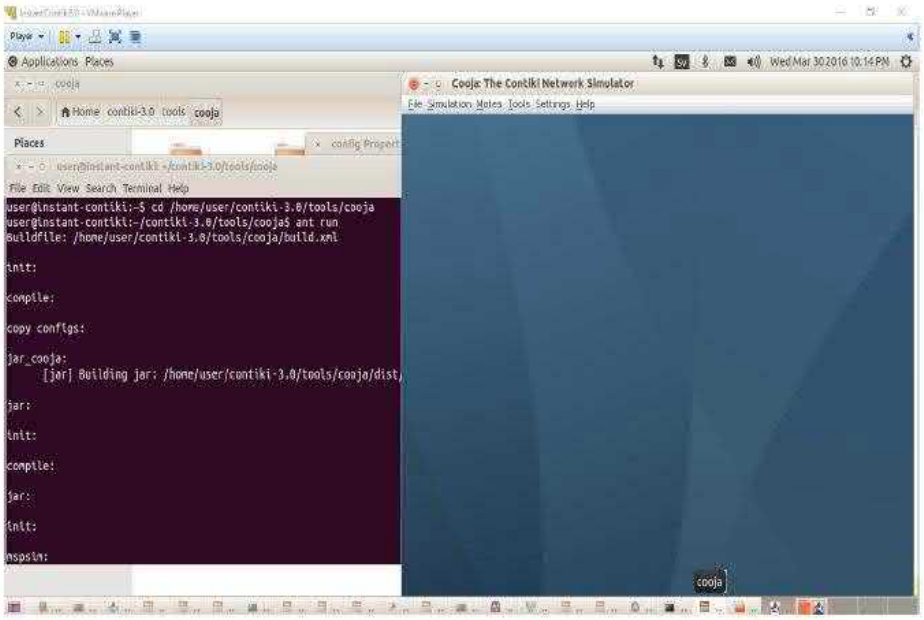
2.9 *Routing Attacks* dalam Protokol 6LoWPAN

Napiah *et al* (2018) menjelaskan bahwa serangan pada 6LoWPAN dibagi menjadi dua, yaitu serangan eksternal dan serangan internal. Serangan eksternal berasal dari internet, misal brute force attack, malware attack, SSL attack, DNS attack. Serangan internal berasal dari *wireless sensor network* (WSN), misal serangan routing yaitu *hello flood, sinkhole, selective forwarding, spofing, wormhole,* dan sebagainya. Tujuan serangan *routing* adalah mengganggu lapisan jaringan ketika *routing* pesan dari satu *node* ke *node* lain dalam jaringan.

2.10 *Contiki OS*

Contiki OS adalah sistem operasi *open source* untuk IoT (Contiki-os.org, 2018). *Contiki* merupakan OS yang sangat portabel dan telah diporting ke beberapa platform yang berjalan pada berbagai jenis prosesor. *Contiki* mendukung baik pada penerapan IPv6 dan IPv4, serta standar nirkabel berdaya rendah terbaru: *6lowpan, RPL, CoAP*. *Contiki* digunakan dalam berbagai sistem, seperti meter listrik, pemantauan industri, sistem alarm, pemantauan rumah jarak jauh, pemantauan radiasi, lampu jalan, dan sebagainya. Versi terbaru *Contiki OS* adalah *Contiki 3.0* (Velinov & Mileva, 2016).

Cooja adalah simulator jaringan *Contiki*. *Cooja* termasuk aplikasi berbasis *Java* dengan GUI *(Graphical User Interface)* (Roussel *et al.*, 2016). Dapat digunakan untuk mensimulasikan jaringan besar dan kecil dari *Contiki Motes* (modul sensor simulasi). Cooja dapat meniru beberapa platform, seperti *TelosB/SkyMote, Zolertia Z1 mote, Wismote, ESB, MicaZ mote*.



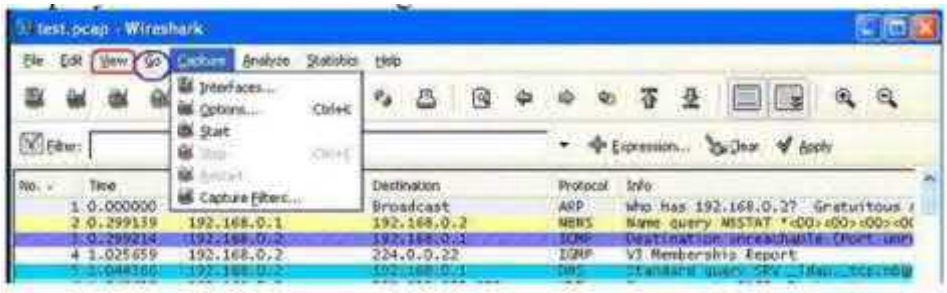
Gambar 2.5 *Cooja Simulator* pada *Contiki OS*

(Velinov & Mileva, 2016)

Gambar 2.5 merupakan tampilan *Cooja Simulator* pada *Contiki OS*. *Cooja* merupakan alat yang berguna untuk pengembangan aplikasi dan *debugging Contiki OS*. Hal ini memungkinkan pengembang untuk menguji kode dan sistem mereka, sebelum menjalankannya pada perangkat keras nyata, untuk memperkirakan konsumsi daya *node* dalam simulasi atau untuk menunjukkan transmisi radio (Velinov & Mileva, 2016).

2.11 *Wireshark*

Wireshark merupakan alat penangkap dan penganalisa jaringan berbasis GUI. *Wireshark* mampu mencegat paket yang dikirimkan melalui jaringan dan menyusun statistik tentang penggunaan jaringan, memungkinkan pengguna untuk melihat konten yang sedang diakses oleh pengguna jaringan lain, dan menyimpan informasi penggunaan untuk akses *offline* (Kumar & Yadav, 2016).



Gambar 2.6 *Capture* Jaringan pada *Wireshark*

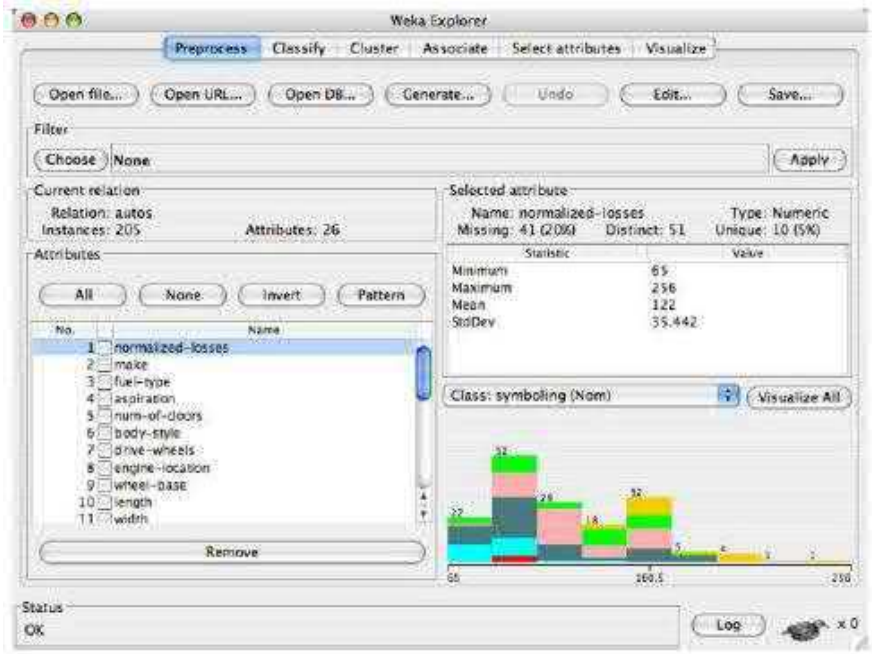
(Banerjee *et al.*, 2010)

Gambar 2.6 menunjukkan proses *capture* jaringan di *Wireshark*. Ada versi baris perintah dari utilitas paket *capture*, yang disebut *Tshark*. *Tshark* menyediakan banyak fitur yang sama seperti sebelumnya, tetapi berbasis konsol. Hal ini dapat menjadi alternatif yang baik jika hanya akses baris perintah yang tersedia, dan juga menggunakan lebih sedikit sumber daya karena tidak memiliki GUI untuk dihasilkan (Kumar & Yadav, 2015).

2.12 *Weka*

Weka (Waikato Environment for Knowledge Analysist) merupakan perangkat lunak *machine learning* yang ditulis di *Java*, dikembangkan oleh

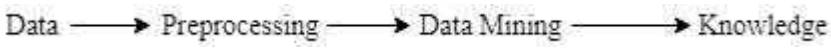
Universitas Waikato, Selandia Baru. Dapat dijalankan di *Windows, Linux, Mac*, serta dapat digunakan untuk penelitian, pendidikan dan proyek. GUI digunakan untuk alat *preprocessing*, metode evaluasi, dan memiliki lingkungan untuk membandingkan teknik pembelajaran (Sharma & Jain, 2013).



Gambar 2.7 *Weka Explorer*

(Sharma & Jain, 2013)

Gambar 2.7 menunjukkan tampilan *Weka Explore*. Aplikasi *Weka* memungkinkan pengguna untuk mengidentifikasi informasi tersembunyi dari *database* dan sistem file dengan opsi yang mudah digunakan dan antarmuka visual. *Weka workbench* berisi kumpulan alat visualisasi dan algoritma *(C4.5, ID3, K-means, Apriori)* untuk memecahkan masalah *data mining* pada dunia nyata (Kulkarni G. & Kulkarni B., 2016). Alur kerja Weka adalah sebagai berikut:



Empat antarmuka grafis pada *Weka* (Kulkarni G. & Kulkarni B., 2016) antara lain:

1. *Explore* : lingkungan untuk menjelajahi data.
2. *Experiments* : melakukan tes statistik antara skema pembelajaran.
3. *Knowledge Flow* : *Java-Beans* untuk menyiapkan dan menjalankan percobaan *machine learning*.
4. *Simple CLI* : memungkinkan eksekusi langsung.

BAB V

PENUTUP

Bab ini berisi tentang beberapa simpulan yang dihasilkan berdasarkan penelitian yang telah dilakukan. Selain itu, dalam bab ini juga memuat beberapa saran yang dapat digunakan untuk mengembangkan penelitian pada *Intrusion Detection System* (IDS).

5.1 Simpulan

Berdasarkan pembahasan dari hasil pengujian simulasi *routing attacks* menggunakan *Smart Intrusion Detection System* berbasis *Compression Header Analyzer* pada *software Cooja Simulator* di dalam *Contiki OS* diperoleh kesimpulan bahwa penelitian ini merupakan kelanjutan dari CHA-IDS. Dalam hal ini, simulasi diuji dengan varian baru model *routing attacks*, berupa *selective forwarding attack* dan *sinkhole attacks*. BFS dan GS dengan CFS yang merupakan *feature selection algorithm* digunakan untuk memilih fitur terbaik yang dapat dipelajari lebih lanjut oleh *machine learning algorithm*. *Random Forest, J48, Logistik, MLP, SMO*, dan *Naïve Bayes* merupakan *machine learning algorithm* yang digunakan dalam mengklasifikasikan antara serangan dan *non*-serangan. Dari enam *machine learning algorithm* tersebut, kinerja terbaik dalam mendeteksi *routing attacks* ditunjukkan oleh *Random Forest* dengan tingkat akurasi sebesar 99,4721%. Selain itu, *Random Forest* juga mencapai nilai TP tertinggi sebesar 0,995 dan nilai MAE terendah sebesar 0,0008.

5.2 Saran

Penelitian tentang *Intrusion Detection System* (IDS) pada jaringan IoT masih perlu ditindak lanjuti agar diperoleh efektifitas dan hasil yang lebih baik. Dari penelitian ini diperoleh beberapa saran yang dapat digunakan untuk penelitian selanjutnya sebagai berikut:

1. *Smart Intrusion Detection System* dapat ditingkatkan untuk mendeteksi model *routing attacks* lainnya yang terdapat pada jaringan IoT.
2. Tingkat akurasi *routing attacks* dapat dihitung dengan menggunakan model *Artifical Inteligence* (AI) lainnya.

DAFTAR PUSTAKA

Abbas Hassan, A., Sheta, A.F. & Wahbi, T.M. 2015. Intrusion Detection System Using Weka Data Mining Tool. *International Journal of Science and Research (IJSR) ISSN*, 6(9): 337–342.

Al-sarawi, S., Anbar, M., Alieyan, K. & Alzubaidi, M. 2017. Internet of Things (IoT) Communication Protocols : Review. *8th International Conference on Information Technology (ICIT)*, 685–690.

Alrajeh, N.A., Khan, S. & Shams, B. 2013. Intrusion detection systems in wireless sensor networks: A review. *International Journal of Distributed Sensor Networks*, 2013.

Ambhore, M.P.B. & Meshram, D.B.B. 2014. Intrusion Detection System for Intranet Security. 4(5): 626–631.

Amish, P. & Vaghela, V.B. 2016. Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV Protocol. *Procedia Computer Science*, 79: 700–707.

Aydin, M.A., Zaim, A.H. & Ceylan, K.G. 2009. A hybrid intrusion detection system design for computer network security. *Computers and Electrical Engineering*, 35(3): 517–526.

Banerjee, U., Vashishtha, A. & Saxena, M. 2010. Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection. *International Journal of Computer Applications*, 6(7): 1–5.

Bauer, H., Burkacky, O. & Knochenhauer, C. 2017. Security in the Internet of Things. (Itt): 25–26.

CHELLI, K. 2015. Security Issues in Wireless Sensor Networks: Attacks and Countermeasures. I.

Contiki-os.org 2018. *Contiki: The Open Source OS for the Internet of Things*.

Cruz, M.A.A., Rodrigues, J.J.P.C., Member, S., Al-muhtadi, J., Korotaev, V. V & Albuquerque, V.H.C. De 2018. A Reference Model for Internet of Things Middleware. 5(2): 871–883.

Desale, Ketan Sanjay and Ade, R. 2015. Genetic Algorithm based Feature Selection Approach for Effective Intrusion Detection System. *2015 International Conference on Computer Communication and Informatics*.

Doshi, M. 2014. Correlation Based Feature Selection (Cfs) Technique To Predict Student Perfromance. *International Journal of Computer Networks & Communications*, 6(3): 197.

Ee, G.K., Ng, C.K., Noordin, N.K. & Ali, B.M. 2010. A Review of 6LoWPAN Routing Protocols. *Proceedings of the Asia-Pacific Advanced Network*, 30(0): 71.

Hall, M. 1999. Correlation-based Feature Selection for Machine Learning. *Methodology*, 21i195-i20(April): 1–5.

Heer, T., René, O.G., Loong, S., Sandeep, K. & Klaus, S.K. 2011. Security Challenges in the IP-based Internet of Things. 527–542.

Ieee, G. & Transceiver, Z.R.F. n.d. CC2420 CC2420.

Jabez, J. & Muthukumar, B. 2015. Intrusion detection system (ids): Anomaly detection using outlier detection approach. *Procedia Computer Science*,

48(C): 338–346.
Jamil, L.S. 2016. Data Analysis Based on Data Mining Algorithms Using Weka Workbench. *International Journal of Engineering Sciences & Research Technology*, 5(8): 262–267.
Kamesh & Sakthi Priya, N. 2014. Security enhancement of authenticated RFID generation. *International Journal of Applied Engineering Research*, 9(22): 5968–5974.
Kang, S. 2015. A Feature Selection Algorithm to Find Optimal Feature Subsets for Detecting DoS Attacks. 1–3.
Kaur, G. & Chhabra, A. 2014. Improved J48 Classification Algorithm for the Prediction of Diabetes. *International Journal of Computer Applications*, 98(22): 13–17.
Kaur, M. & Singh, A. 2017. Detection and mitigation of sinkhole attack in wireless sensor network. *Proceedings - 2016 International Conference on Micro-Electronics and Telecommunication Engineering, ICMETE 2016*, 217–221.
Kim, S. & Lee, I. 2017. IoT device security based on proxy re-encryption. *Journal of Ambient Intelligence and Humanized Computing*, 0(0): 0.
Kolias, C., Kambourakis, G., Stavrou, A. & Gritzalis, S. 2016. Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset. *IEEE Communications Surveys and Tutorials*, 18(1): 184–208.
Kothmayr, T. 2011. A Security Architecture for Wireless Sensor Networks based on DTLS. (December).
Kulkarni G., E. & Kulkarni B., R. 2016. WEKA Powerful Tool in Data Mining. *International Journal of Computer Applications National Seminar on Recent Trends in Data Mining*, 5(Rtdm): 975–8887.
Kumar, A. & Yadav, J.B. 2016. Comparison : Wireshark on different parameters. 5(16041): 16041–16046.
Kumar, M. & Yadav, R. 2015. Tcp & Udp Packets Analysis Using Wireshark. *International Journal of Science, Engineering and Technology Research (IJSETR)*, 4(7): 2470–2474.
Livingston, F. 2005. Implementing Breiman ' s Random Forest Algorithm into Weka. *Machine Learning*, 1–5.
Meenakshi, M. & Geetika, G. 2014. Survey on Classification Methods using WEKA. *India International Journal of Computer Applications*, 86(18): 16–19.
Miguel-Hurtado, O., Guest, R., Stevenage, S. V., Neil, G.J. & Black, S. 2016. Comparing machine learning classifiers and linear/logistic regression to explore the relationship between hand dimensions and demographic characteristics. *PLoS ONE*, 11(11): 1–25.
Moteiv Corporation 2006. Moteiv: tmote sky low power wireless sensor module. *Product Data Sheet*, 1–28.
Mulligan, G. 2007. The 6LoWPAN architecture. *Proceedings of the 4th workshop on Embedded networked sensors - EmNets '07*, 78.
Napiah, M.N., Idris, M.Y.I., Ramli, R. & Ahmedy, I. 2018. Compression Header Analyzer Intrusion Detection System (CHA -IDS) for 6LoWPAN Communication Protocol. *IEEE Access*, 3536(c).

Nath, A. 2016. Classification of Machine Learning Algorithms. *International Journal of Innovatice Research in Advanced Engineering*, 3(April): 6–11.

Ngu, A.H.H., Gutierrez, M., Metsis, V. & Sheng, Q.Z. 2016. IoT Middleware : A Survey on Issues and Enabling Technologies. X(X): 1–20.

PalSingh, V., S. Anand Ukey, A. & Jain, S. 2013. Signal Strength based Hello Flood Attack Detection and Prevention in Wireless Sensor Networks. *International Journal of Computer Applications*, 62(15): 1–6.

Pavan Pongle, G.C. 2015. A Survey : Attacks on RPL and 6LoWPAN in IoT. 0(c): 0–5.

Pedro, Mugdhe, S. 2016. *http://anrg.usc.edu/contiki/index.php/Cooja_Simulator*.

Pongle, P. & Chavan, G. 2015. Real Time Intrusion and Wormhole Attack Detection in Internet of Things. *International Journal of Computer Applications*, 121(9): 975–8887.

Rameshpant, S., Associate, K., Ladtree, K. & Randomforest, R. 2008. Comparative Analysis of WEKA Data Mining Algorithm RandomForest, RandomTree and LADTree for Classification of Indigenous News Data. *International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com ISO Certified Journal*, 9001(1): 507–517.

Rani, N. & Purwar, R. 2017. Performance Analysis of various classifiers using Benchmark Datasets in Weka tools. *Ijettjournal.Org*, 47(May): 290–294.

Raza, S., Duquennoy, S. 2011. Securing communication in 6LoWPAN with compressed IPsec. In Distributed Computing in Sensor Systems and. *IEEE Workshops (DCOSS)*, 1–8.

Raza, S., Wallgren, L. & Voigt, T. 2013. SVELTE : Real-time intrusion detection in the Internet of Things. *AD HOC NETWORKS*. Tersedia di http://dx.doi.org/10.1016/j.adhoc.2013.04.014.

Roussel, K., Song, Y., Zendra, O., Roussel, K., Song, Y., Zendra, O., Cooja, U., Some, S., Uses, N. & Zendra, O. 2016. Using Cooja for WSN Simulations : Some New Uses and Limits To cite this version : HAL Id : hal-01240986 Using Cooja for WSN Simulations : Some New Uses and Limits.

S. Singaravelan, D. Murugan, R.M. 2015. Analysis of Classification Algorithms J48 and Smo on Different Datasets. *World Engineering & Applied Sciences Journal 6*, 6(2): 1–5.

Sahu, S. & Mehtre, B.M. 2015. Network Intrusion Detection System Using J48 Decision Tree. *Advances in Computing, Communications and Informatics (ICACCI), 2015 International Conference on*, 2023–2026.

Saini, P.K.K. 2013. Denial of Service Attacks in Wireless Networks. 13(4): 1–11.

Saleh, A. & Nasari, F. 2018. Implementation of Equal-Width Interval Discretization in Naive Bayes Method for Increasing Accuracy of Students â€™ Majors Prediction. *Lontar Komputer : Jurnal Ilmiah Teknologi Informasi*, 9(2): 104–113.

Sarica, A., Cerasa, A. & Quattrone, A. 2017. Random forest algorithm for the classification of neuroimaging data in Alzheimer's disease: A systematic review. *Frontiers in Aging Neuroscience*, 9(OCT): 1–12.

Sebastian, S. 2015. Evaluating Students Performance by Artificial Neural Network using WEKA. *International Journal of Computer Applications*, 119(23): 975–

8887.

Shah, H., Shrimali, R. & Parikh, V. 2016. Header Compression and Neighbor Discovery in 6LoWPAN based IoT - A survey. *Proceedings of the 2016 IEEE International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2016*, 306–311.

Sharma, T.C. & Jain, M. 2013. WEKA Approach for Comparative Study of Classification Algorithm. *India WEKA*, 2(4): 1925–1931.

Shelby, Z. & Bormann, C. 2009. *6LoWPAN : The Wireless Embedded Internet*.

Sonar, K. & Upadhyay, H. 2016. An Approach to Secure Internet of Things Against DDoS.

Soofi, A.A. & Awan, A. 2017. Classification Techniques in Machine Learning: Applications and Issues. *Journal of Basic & Applied Sciences*, 13: 459–465.

Suresh, M. & Anitha, R. 2011. Evaluating Machine Learning Algorithms for Detecting DDoS Attacks *. 441–452.

TARIQAHMAD SHERASIYA, H.U.& H.B.P. 2016. a Survey: Intrusion Detection System for Internet of Things. *International Journal of Computer Science and Engineering (IJCSE)* , 5(2): 91–98.

Tribhuvan, A.P., Tribhuvan, P.P. & Gade, J.G. 2015. Applying Naive Bayesian Classifier for Predicting Performance of a Student Using WEKA. *Advances in Computational Research*, 7(1): 239.

Velinov, A., C.M.B. 2018. Classification with ID3 and SMO Using Weka. *International Conference on Information Technology and Development of Education – ITRO*.

Velinov, A. & Mileva, A. 2016. Running and Testing Applications for Contiki OS Using Cooja Simulator. *International Conference on Information Technology and Development of Education*, 279–285.

Wallgren, L., Raza, S. & Voigt, T. 2013. Routing Attacks and Countermeasures in the RPL-Based Internet of Things. 2013.

Witten, I.H., Frank, E. & Hall, M. a 2011. *Data Mining: Practical Machine Learning Tools and Techniques (Google eBook)*. *Complementary literature None*.