**PROPOSAL PROYEK AKHIR**

HALAMAN SAMPUL  
**PERBANDINGAN PERFORMA PENGGUNAAN PROTOKOL COAP SERTA MQTT PADA SISTEM RUMAH PINTAR**

***COMPARISON OF THE PERFORMANCE IN IMPLEMENTATION OF COAP AND MQTT PROTOCOL AT SMART HOME SYSTEM***

****

**Diajukan oleh :**  
**MUHAMMAD RUSMINTO HADIYONO**  
**15/386767/SV/10153**

**PROGRAM SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET**  
**SEKOLAH VOKASI**  
**UNIVERSITAS GADJAH MADA**  
**YOGYAKARTA**  
**2019**



**USULAN TUGAS AKHIR YANG DIAJUKAN KEPADA**

**PROGRAM SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET SEKOLAH VOKASI UNIVERSITAS GADJAH MADA**

1. JUDUL TUGAS AKHIR : Perbandingan Performa Penggunaan Protokol CoAP serta MQTT pada Sistem Rumah Pintar.

*Comparison of The Performance in Implementation of CoAP and MQTT Protocol at Smart Home.*

1. PENYUSUN : Muhammad Rusminto Hadiyono
2. DOSEN PEMBIMBING I
3. Nama Lengkap : Muhammad Arrofiq, S.T., M.T., Ph.D.
4. NIP : 197311271999031001
5. TEMPAT PENELITIAN : Ruang Layanan Internet Teknologi Rekayasa Internet UGM.

Yogyakarta, 10 April 2018

# HALAMAN PENGESAHAN

Disetujui Oleh :

|  |  |
| --- | --- |
| Dosen Pembimbing  Muhammad Arrofiq, S.T., M.T., Ph.D.  NIP. 197311271999031001 | Penyusun  Muhammad Rusminto Hadiyono  NIM. 15/386767/SV/10153 |
| Mengetahui,  Ketua Program Studi Teknologi Jaringan  Muhammad Arrofiq, S.T., M.T., Ph.D.  NIP. 197311271999031001 | |

# INTISARI

**USULAN TUGAS AKHIR**

**PERBANDINGAN PERFORMA PENGGUNAAN PROTOKOL COAP SERTA MQTT PADA SISTEM RUMAH PINTAR**

Jaringan *wireless ad hoc* dengan tidak adanya dukungan infrastruktur yang tetap, mengharuskan jaringan ini saling bergantung antar *node-node* yang saling terhubung dalam jaringan tersebut. Jaringan *mobile ad hoc* adalah jaringan yang termasuk kedalam jaringan *wireless ad hoc* dengan karakteristik yang sedikit berbeda, yaitu *node* yang sering berpindah-pindah tempat sehingga mengakibatkan topologi jaringan menjadi sangat dinamis dan susah untuk diprediksi sehingga mengharuskan proses pertukaran informasi pada jaringan *mobile ad hoc* memerlukan sebuah protokol *routing* khusus. XBee melalui protokol ZigBee dapat mengimplmentasikan *Ad hoc On-demand Distance Vector* (AODV) sebagai cara untuk menemukan rute dari sumber ke tujuan dimana protokol tersebut termasuk kedalam kategori reaktif *routing* yang bekerja hanya berdasarkan jika terdapat permintaan dari sebuah *node*. Pada proses penerapan *mobile ad hoc network* itu sendiri masih beberapa celah, salah satunya adalah pada keamanan jaringan *mobile ad hoc* belum sepenuhnya terjamin karena banyak sekali pengaruh yang bisa dilakukan untuk merusak jaringan *mobile ad hoc* tersebut. Maka dari itu pada tugas akhir ini dilakukan implementasi dan analisis kinerja dari protokol *routing* AODV pada protokol ZigBee *mesh networ*k dengan pangaruh *Data* *Flooding Attack*. Parameter yang digunakan untuk mengukur *availability* dan kinerja dari protokol antara lain: *packet delivery ratio* (pdr), *delay*, *throughput*, dan *packet loss*.

Kata Kunci : *Wireless, Ad hoc*, *Mobile Ad hoc Network* (MANET), AODV, Data *Flooding.*

# DAFTAR ISI

[HALAMAN SAMPUL i](#_Toc503989741)

[HALAMAN PENGESAHAN ii](#_Toc503989742)

[INTISARI iii](#_Toc503989743)

[DAFTAR ISI iv](#_Toc503989744)

[DAFTAR GAMBAR v](#_Toc503989745)

[DAFTAR TABEL vi](#_Toc503989746)

[BAB I PENDAHULUAN 1](#_Toc503989747)

[1.1 Latar Belakang 1](#_Toc503989748)

[1.2 Rumusan Masalah 2](#_Toc503989749)

[1.3 Batasan Masalah 2](#_Toc503989750)

[BAB II TUJUAN PROYEK AKHIR 4](#_Toc503989751)

[BAB III TINJAUAN PUSTAKA 5](#_Toc503989752)

[BAB IV LANDASAN TEORI DAN HIPOTESIS 13](#_Toc503989753)

[4.1 Landasan Teori 13](#_Toc503989754)

[4.1.1 Jaringan Nirkabel atau *Wireless Network* 13](#_Toc503989755)

[4.1.2 Jaringan *Mobile Ad hoc Network* (MANET) 17](#_Toc503989756)

[4.1.3 *Routing* pada jaringan *Mobile Ad hoc Network* (MANET) 21](#_Toc503989757)

[4.1.4 Mikrokontroler dan Arduino 31](#_Toc503989758)

[4.1.5 Modul XBee 34](#_Toc503989759)

[4.1.6 Kalilinux 38](#_Toc503989760)

[4.1.7 Parameter Kinerja 38](#_Toc503989761)

[4.2 Hipotesis 41](#_Toc503989762)

[BAB V METODE PENELITIAN 42](#_Toc503989763)

[5.1 Alat dan Bahan 42](#_Toc503989764)

[5.2 Prosedur Penelitian 43](#_Toc503989765)

[5.3 Analisis Hasil 47](#_Toc503989766)

[5.4 Jadwal Penelitian 47](#_Toc503989767)

[DAFTAR PUSTAKA 48](#_Toc503989768)

# DAFTAR GAMBAR

[Gambar 4.1 *Mobile Ad hoc Network* (MANETs) 17](#_Toc511035013)

[Gambar 4.2 Tantangan pada Jaringan MANETs berdasarkan layer 21](#_Toc511035014)

[Gambar 4.3 Format Pesan *Route Request* 25](#_Toc511035015)

[Gambar 4.4 Format Pesan *Route Reply* 25](#_Toc511035016)

[Gambar 4.5 Format Pesan *Route Error* 26](#_Toc511035017)

[Gambar 4.6 Format Pesan *Route Reply Acknowledgement* 26](#_Toc511035018)

[Gambar 4.7 Ilustrasi *Route Discovery* 31](#_Toc511035019)

[Gambar 4.8 Ilustrasi *Route Maintence* 31](#_Toc511035020)

[Gambar 4.9 Arduino Uno R3 32](#_Toc511035021)

[Gambar 4.10 Tampilan Arduino IDE 33](#_Toc511035022)

[Gambar 4.11 Topologi Jaringan XBee 37](#_Toc511035023)

[Gambar 5.1 Rancangan Topologi Jaringan MANET Skenario 1 43](#_Toc511035024)

[Gambar 5.2 Rancangan Topologi Jaringan MANET Skenario 2 43](#_Toc511035025)

[Gambar 5.3 Rancangan Topologi Jaringan MANET Skenario 3 44](#_Toc511035026)

[Gambar 5.4 Gambaran *Node* 45](#_Toc511035027)

[Gambar 5.5 *Flowchart* Penelitian 46](#_Toc511035028)

DAFTAR TABE

[Tabel 3.1 Ringkasan Sumber Jurnal Penelitian12](#_Toc511035085)

[Tabel 4.1 Standarisasi Delay versi *TIPHON*Error: Reference source not found](#_Toc511035086)

[Tabel 4.2 Data *Througput* XBeeError: Reference source not found](#_Toc511035087)

[Tabel 4.3 Standarisasi *Packet Loss* versi *TIPHON*Error: Reference source not found](#_Toc511035088)

[Tabel 5.1 Ringkasan data dan waktu penyeranganError: Reference source not found](#_Toc511035089)

[Tabel 5.2 Jadwal Penelitian21](#_Toc511035090)

# BAB I

**PENDAHULUAN**

## Latar Belakang

Teknologi jaringan w*ireless* terus berkembang setiap harinya yang diakibatkan oleh aktivitas seseorang dengan kebutuhan mobilitas yang tinggi. Jaringan *wireless* dapat dijumpai dimana saja seperti telepon yang biasa digunakan untuk berkomunikasi dan *Access Point*. Pada dasarnya jaringan *wireless* terbagi menjadi 2 yaitu jaringan *wireless* dengan insfrastruktur dan jaringan *wireless* tanpa infrastruktur yang kemudian dikenal dengan istilah *wireless* *ad hoc*. Dalam perkembangan jaringan *wireless ad hoc* itu sendiri kemudian memunculkan berbagai macam bentuk model jaringan baru seperti *Mobile Ad hoc Networks* (MANET) dan *Vehicular Ad hoc Networks* (VANETs).

Jaringan *Mobile Ad hoc* adalah jaringan yang tidak memiliki *gateway* atau jalur keluar yang tetap dengan demikian setiap perangkat yang saling terhubung akan saling bertukar informasi satu sama lain menggunakan bantuan protokol *routing* khusus untuk jaringan MANETs seperti *Ad hoc On Demand Distance Vector Routing* (AODV), *Dynamic Source Routing Protokol* (DSR), *Destination Sequence Distance Vector Routing* (DSDV), *Optimized Link State Routing* (OLSR) dan protokol *routing* yang lain. Ketika berbagi informasi antar perangkat pada *Mobile Ad hoc Network* terdapat beberapa hal yang harus diperhatikan terkait dengan keamanan *Mobile Ad hoc Network*. Hal-hal yang harus diperhatikan adalah *Authenticity* yaitu keaslian dari sebuah pesan yang dikirimkan, *Integrity* yaitu pesan yang dikirim atau diinformasikan kepada perangkat lain tidak dimodifikasi ketika dijalan atau dalam proses pengiriman, *Confidentiality* yaitu pesan harus bersifat rahasia karena tidak boleh ada orang yang tahu selain pengirim dan penerima pesan tersebut, *Availability* berhubungan dengan ketersediaan jaringan apakah jaringan tersebut dapat mengirimkan pesan atau tidak, dan *Non-Repudiation* (Thilak 2016).

Dari lima (5) bagian yang perlu diamankan yang paling penting dan sangat mendasar adalah tingkat ketersediaan jaringan itu sendiri atau *availability*, karena adanya ketersediaan jaringan dapat memfasilitasi aktivitas pada bagian lain seperti *Integrity* dan *Authenticity.* Maka dari itu pada tugas akhir ini akan dilakukan implementasi dan analisis kinerja protokol *routing Ad hoc On-demand Distance Vector* (AODV) yang dipengaruhi oleh serangan *data flooding attack* untuk menguji tingkat ketersediaan pada protokol *routing* yang digunakan tersebut.

## Rumusan Masalah

Beberapa rumusan masalah yang mengacu pada tujuan penulisan tugas akhir ini adalah sebagai berikut :

1. Bagaimana cara menerapkan protokol MQTT dan CoAP di Sistem Rumah Cerdas ?
2. Apakah level QoS yang akan digunakan pada protokol MQTT ?
3. Bagaimana arsitektur sederhana dari penerapan *smart device* di Sistem Rumah Cerdas ?
4. Bagaimana hasil perbandingan throughput dan latency dalam penggunaan protokol MQTT dan CoAP ?
5. Berdasarkan hasil perbandingan, bagaimanakah kondisi yang tepat untuk menggunakan MQTT atau CoAP ?

## Batasan Masalah

1. Lampu pada maket rumah pintar masih menggunakan LED, tidak menggunakan lampu dan relay.
2. *Smart device* yang digunakan hanyalah Google Home dan Alexa.

### 1

# BAB II

**TUJUAN PROYEK AKHIR**

### **3**

Bagi Mahasiswa D4 Teknologi Rekayasa Internet :

1. Menambah wawasan mahasiswa mengenai penerapan protokol MQTT dan CoAP dalam jaringan IoT.
2. Mampu mengetahui protokol mana yang lebih dibutuhkan dalam kondisi jaringan tertentu.
3. Mampu merancang *smart device* yang terhubung dengan sensor atau komponen elektronik lainnya.

Bagi Program Studi D4 Teknologi Jaringan :

1. Penelitian ini dapat digunakan sebagai bahan ajar tambahan dalam mata kuliah Praktikum Rancangan dan Aplikasi IoT.

# BAB III

**TINJAUAN PUSTAKA**

Paradigma *wireless networking* atau jaringan nirkabel dapat dikategorikan menjadi dua golongan yaitu *wireless Ad hoc* dan *cellular networking* atau jaringan yang terinfrastruktur. Adanya infrastruktur menjadi perbedaan utama antara dua golongan jaringan *wireless* tersebut. Pada *Ad hoc networking paradigm* atau paradigma jaringan *Ad hoc* tidak ada infastruktur yang tetap dan paket data terkirim ke tujuan melewati jaringan *wireless* dengan beberapa lompatan (*multihop*), dan juga *node* seringkali tidak hanya berfungsi sebagai host melainkan juga berfungsi sebagai *router* dengan memberikan informasi keadaan lalu lintas pada *node* yang lain (*neighboor node*). Topologi pada jaringan *Ad hoc* dapat berubah setiap saat karena *node* selalu bergerak (*mobile*) atau keadaan lain yang mungkin terjadi adalah *node*-*node* tersebut gagal untuk membangun sebuah topologinya. Pada jaringan yang terinsfrastruktur atau *cellular networking* *node* dapat mencapai *access point* atau *gatewaynya* hanya dalam satu lompatan jaringan *wireless*, gambar jaringan wireless *Ad hoc* dan *cellular networking* (Çayırcı and Rong 2009).

Fungsi *node* pada jaringan *Ad hoc* tidak hanya sebagai host, fungsi yang lain adalah sebagai *router*, ketika berfungsi sebagai *router* maka *node* tersebut harus mencari dan memelihara informasi dari jalur yang digunakan untuk sampai pada *node* yang lain. Dalam melakukan tugas tersebut *node* tidak bisa menjalankan pekerjaannya seorang diri melainkan dibutuhkan sebuah protokol *routing* pada jaringan *Ad hoc*. Secara garis besar protokol *routing* pada *Mobile Ad hoc Network* (MANET) dapat dikategorikan menjadi 2 yaitu *Table-driven* atau *Proactive* dan *On-demand* atau *Reactive*. Protokol *routing* yang bersifat proaktif bekerja dengan cara memelihara informasi rute setiap saat kepada *node* tetangganya. Contoh yang termasuk dalam golongan *routing* proaktif ini adalah *Destination Sequence Distance Vector* (DSDV). Kemudian protokol *routing* yang bersifat reaktif, *node* hanya melakukan pencarian rute ketika ada *node* sumber akan melakukan pengiriman paket data ke *node* tujuan, maka kemudian *node* mencari jalur menuju *node* tujuan tersebut dan pembaruan informasi dilakukan secara berkala tidak setiap saat. Contoh protokol *routing* yang termasuk dalam kategori ini adalah *Ad hoc On-demand Distance Vector* (AODV) dan *Dynamic Source Routing* (DSR) (Deng, Li and Agrawal 2002).

Dalam penelitian ini, ada beberapa hal penting yang dapat dikaji dalam manet maupun protokol Zigbee pada jaringan nirkabel yaitu dengan cara mengukur *throughput*, *delay* *packet delivery ratio* (pdr) dan *packet loss* sebagai parameter tolak ukur performa jaringan manet tersebut. Penelitian pertama yang digunakan sebagai acuan penelitian yang berkaitan dengan protokol *routing Ad hoc On-demand Distance Vector* (AODV) adalah pada penelitian simulasi menggunakan perangkat lunak NS-3 tentang kinerja protokol *routing* AODV yang ditimpa dengan *flooding attack* (Bandyopadhyay and Vuppala 2011)*.* Penelitian tersebut membagi *flooding attack* kedalam dua tipe serangan yaitu *Route Request* (RREQs) *Flooding Attack* dan *Data Flooding Attack*. *Flooding Attack* sendiri merupakan jenis serangan dari *Denial of Service Attack* dimana *node* jahat melakukan serangan dengan cara membanjiri *node* yang lain dengan paket data dalam jumlah yang sangat banyak. Dua jenis serangan *flooding attack* yang akan digunakan juga memiliki mekanisme yang berbeda saat melakukan serangan, RREQs *Flooding Attack* melakukan serangan dengan cara mengambil keuntungan ketika proses pencarian rute pada protokol *routing* yang bersifat reaktif seperti DSR dan AODV. Dalam serangan ini *node* jahat melakukan pesan siaran dijaringan dimana tidak terdapat alamat valid yang dituju, sehingga ketika tidak ada tujuan yang valid jaringan menjadi penuh dengan paket RREQs dari *node* jahat, sedangkan untuk serangan *Data Flooding Attack* pembajiran data dilakukan ketika rute antar *node* sudah terbangun dan siap digunakan. *node* jahat mengalirkan data dalam jumlah yang besar dan tidak berguna sama sekali didalam jaringan sehingga membuat jalur menjadi tersumbat dan mengurangi *bandwidth* jaringan yang ada. Pada simulasi ini digunakan 15 *node* yang ditempatkan secara acak dalam area berukuran (500x500)m dengan waktu simulasi untuk melakukan serangan adalah selama 60 detik. Parameter yang digunakan untuk pengukuran antara lain : *routing overhead,* presentase dari *data packet loss*, serta *bandwidth usagenya.* Simulasi yang dilakukan menghasilkan data seperti penjelasan berikut, ketika dilakukan RREQs *flooding attack* terdapat dua parameter yang digunakan yaitu *routing overhead* dan *data packet loss* yang sama-sama mengalami peningkatan dan membuat jaringan menjadi lemah, hal yang sama ditunjukkan pada jaringan *Ad hoc* yang dilakukan serangan dengan *data flooding attack,* dilihat dari parameter *routing overhead, bandwidth usage* dan *data packet loss* mengalami peningkatan yang signifikan.

Simulasi terhadap *Mobile Ad hoc Network* (MANET) yang ditimpa dengan berbagai macam serangan juga dilakukan peneltian dengan beberapa variabel yang dianalisis seperti dampak dari ukuran jaringan, dampak dari mobilitas *node*, dampak *traffic load* (HoudaMoudni, et al. 2016)*.* Pada penelitian tersebut dititik beratkan pada kinerja protokol *routing* AODV pada jaringan MANET dan menggunakan perangkat lunak NS-2. Simulasi sendiri menggunakan beberapa parameter untuk menentukan batasan masalah terhadap penelitian tersebut, parameter-parameter yang digunakan untuk simulasi antara lain luas area berukuran (500 x 500)m, ukuran paket sebesar 512 bytes dan durasi atau lama waktu melakukan simulasi terhadap sebuah skenario adalah 200 detik. Kinerja protokol *routing* AODV ketika ditimpa oleh serangan *balckhole attack*, *flooding attack*, dan *rushing attack* diamati melalui parameter pada jaringan seperti *packet delivery ratio* (pdr), *end-to-end delay*, *throughpu*t, dan *packet loss* dengan hasil simulasi yang menunjukkan hampir sebagian variabel yang diamati mengalami penurunan kinerja ketika ditimpa oleh serangan-serangan tersebut.

Variabel yang pertama yaitu pengaruh ukuran jaringan yang ditandai dengan banyaknya *node* yang berhubungan satu sama lain ketika ditimpa. *Packet delivery ratio* menunjukkan penurunan yang signifikan saat ditimpa oleh *black hole attack* sampai dibawah 25%, berbeda halnya saat diserang oleh *flooding attack* dan *rushing attack* yang masih memiliki packet delivery ratio diatas 75 %, selanjutnya pada pengamatan dengan parameter *end-to-end delay* menunjukkan penurunan kinerja ketika ditimpa oleh tiga serangan tersebut, sedangkan *throughput* mengalami penurunan secara signifikan dialami oleh jaringan ketika ditimpa dengan *black hole attack*. Variabel yang kedua pada pengamatan yaitu pengaruh mobilitas atau pergerakan *node* terhadap kinerja protokol. Pada pengamatan ini *node* yang digunakan sebanyak 5, dengan kecepatan diatur sampai dengan 30 m/s dan hasil menunjukkan ketika ditimpa oleh *black hole attack*, kinerja protokol *routing* mengalami penurunan yang sangat signifikan yaitu dibawah angka 20% pada parameter pdr dan *throughput*. Berbeda dengan *flooding attack* dan *rushing attack* yang tidak terlalu menurunkan kinerja protokol *routing* AODV tersebut. Sedangkan pada parameter *end-to-end delay* serangan *black hole* juga meningkatkan waktu secara signifikan dibandingan kedua serangan lainnya.

Sebuah penelitian juga dilakukan pada jaringan *Ad hoc* yang ditimpa dengan DoS *attack*. Penelitian dilakukan dengan cara simulasi menggunakan perangkat lunak *open source* NS-3 dengan *platform* sistem operasi Ubuntu. Pada simulasi tersebut digunakan 10 *node* dengan protokol *routing* AODV, pada area (500x500)m, dan waktu simulasi dalam satu kali tempaan adalah 10 detik. Selanjutnya serangan yang dilakukan dalam jaringan pada penelitian ini adalah dua jenis serangan yang termasuk dalam kategori serangan DoS yaitu *hello floods attack* dan *flooding attack.* Serangan *flooding attack* dilakukan dengan cara mengirim paket *route request* (rreq) secara terus menerus dalam jaringan yang mengakibatkan kemacetan sementara untuk *hello floods attack* dilakukan dengan cara pembanjiran paket data pesan hello kepada para tetangganya untuk membuat *node* tetangga menjadi kehilangan daya sehingga tidak memberikan pesan balasan terhadap pesan rreq yang asli. Dalam pengambilan data penelitian ini menggunakan lima skenario yaitu tiga skenario untuk *node* dengan pergerakan (*mobile nodes*) dan dua skenario untuk *node* tanpa pergerakan tetap (*fixed nodes*). Hasil dari penelitian terhadap lima skenario tersebut adalah seperti berikut : simulasi yang pertama yaitu *node* bergerak dengan tidak ditimpa oleh serangan apapun didalamnya yang menunjukkan presentasi plr 0% dan rtt sebesar 4ms, akan tetapi ketika *node-node* dilakukan perubahan posisi atau digerakkan (*mobile),* parameter plr berubah menjadi 65% dan rtt mendekati 1000ms. Skenario yang kedua dilakukan penyerangan pada *node* tanpa pergerakan dengan *hello floods attack*, hasilnya adalah kehadiran satu *node* jahat dengan serangan tersebut membuat *round trip time* (rtt) dari sebuah *node* normal menjadi 120ms. Skenario yang ketiga yaitu dilakukan penyerangan *flooding attack* pada *node* tanpa pergerakan dengan hasil kehadiran satu atau dua *node* dengan serangan tersebut membuat *node* normal memiliki rtt 10 kali lipat lebih besar dari pada tidak dilakukan serangan, sedangkan untuk plrnya naik menjadi 40%. Kemudian untuk skenario yang keempat dilakukan serangan *hello flood attack* pada jaringan dengan *node* dilakukan pergerakan (*mobile nodes*) yang menunjukkan hasil satu *node* jahat yang melakukan serangan mengakibatkan seluruh *node* kehilangan paketnya, dan untuk skenario yang terakhir adalah penyerangan pada *node* dengan pergerakan oleh serangan *flooding attack*. Dampak dari serangan tersebut membuat plr menjadi 80% (Lotfy and Azer 2013).

Beberapa penelitian diatas baru dilakukan secara simulasi artinya belum sepenuhnya yang ada pada simulasi tersebut bisa dilakukan secara nyata dengan menggunakan sebuah alat tertentu. Penelitian secara nyata kini mulai dilakukan, salah satunya adalah pada jurnal yang melakukan penelitian tentang perbandingan *Quality of Service* (QoS) dijaringan *Wireless Sensor Network* (WSN) menggunakan XBee pada topologi *star* dan topologi *multihop* (Pramono, et al. 2017)*.* *Quality of Service* (QoS yang digunakan untuk menjadi acuan dalam penelitian tersebut berupa *delay*, *throughput* dan *packet loss*. Peneltian dilakukan menggunakan sebuah modul komunikasi nirkabel berupa XBee dengan tipe S2C dengan setiap pengambilan data QoSnya, perangkat Xbee tersebut ditempatkan pada jarak yang berbeda-beda. Sehingga selain membandingkan topologi *star* dan *Multihop* penelitian tersebut juga membandingkan dari faktor jarak dan jarak yang digunakan adalah 10m, 20m, dan 30m. Dari penelitian tersebut didapatkan kesimpulan bahwa 2 topologi yang dibandingkan didapatkan nilai *throughput* tertinggi pada topologi *star* dengan nilai 4109 bps dan 3019 untuk topologi multihop. Pada parameter *packet loss* didapatkan paket yang hilang sebesar 4% pada topologi *star* dan 5,5% pada topologi *multihop*, sedangkan untuk parameter *delay* didapatkan nilai 296 ms pada topologi *star* dan 554 ms pada topologi *multihop* serta jarak terjauh yang dapat tercapai pada penelitian tersebut adalah 660 m dengan penerapan *Line-of-Sight* (LOS). Penelitian yang hamper sama juga dilakukan yaitu tantang analisis performa jaringan ZigBee pada *Wireless Sensor Network* (WSN) dengan parameter *Quality of Service* (Qos) (Fitriawan, et al. 2017). Dalam penelitian ini dilakukan uji performa QoS berupa *throughput*, *delay* dan *packet loss* dengan model topologi menerapkan *Line-of-Sight* (LOS) dan *Non Line-of Sight* (NLOS) dan percobaan dilakukan dengan kecepatan *baudrate* yang berbeda-beda. Modul komunikasi yang digunakan pada penelitian ini adalah modul RF XBee S2 dan menggunakan perangkat lunak docklight v 2.0 untuk menganalisan *Quality of Service* (Qos) tersebut. Hasil pada penelitian tersebut membuktikan bahwa setiap kecepatan *baudrate* yang diterapkan mempengaruhi terhadap parameter uji *Quality Os Service.* Pada *throughput* semakin bertambahnya kecepetan *baudrate* maka akan meningkatkan nilai *throughput*, dan pada *delay* semakin rendah kecepatan *baudrate* akan membuat nilai *delay* semakin besar.

Berdasarkan penelitian pada uraian sebelumnya dapat diketahui bahwa pada jaringan *Ad hoc* yang ditimpa berbagai macam jenis serangan dari *Denial of Service* (DoS) Attack pada protokol *routing* yang tidak diberikan protokol keamanan seperti ARAN atau SAODV akan mengkibatkan kemacetan pada jalur, yang jika dibiarkan terus menerus akan membuat jaringan akan mati total dan tidak bisa digunakan untuk komunikasi antar *node*. pendekatan yang mungkin bisa dilakukan untuk melakukan implentasi jaringan *ad hoc* network kedalam dunia nyata adalah menggunakan modul komunikasi nirkabel XBee seperti pada 2 paparan jurnal terkahir. Dalam penelitian yang diuraikan tersebut jaringan *Ad hoc* diimplementasikan hanya dalam sebatas simulasi dan baru beberapa penelitian yang melakukan implementasi menggunakan alat yang sesungguhnya dan sedikit penelitian yang berusaha untuk merealisasikan *mobile ad hoc network* (manet) secara langsung, oleh karena itu berdasar pada penelitian yang sudah ada, penelitian ini akan mengimplementasikan jaringan *Ad hoc* menggunakan alat berupa modul komunikasi nirkabel XBee dengan protokol ZigBee dimana didalam protokol ZigBee sudah menerapkan proses *routing* *Ad hoc On demand Distance Vector* (AODV). Setelah topologi terbangun akan dilakukan ujicoba ketersediaan jaringan dengan pengaruh serangan *data* *flooding attack* menggunakan salah satu *tools* pada Kali Linux yaitu hping3. Adapun ringkasan berdasarkan uraian penelitian diatas dapat dilihat pada Tabel 3.1 dibawah ini :

Tabel 3.1 Ringkasan Sumber Jurnal Penelitian

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **No** | **Judul Penelitian** | **Pokok Bahasan** | **Tipe Penelitian** | **Skenario** | **Penulis** |
| 1 | *A Simulation Analysis of Flooding Attack in MANET using NS-3* | Melakukan serangan pada jaringan *Adhoc* dengan jenis serangan *RREQ Flooding Attack* dan *Data Flooding Attack* | Simulasi | NS-3, AODV tanpa keamanan, 15 *node* | Alokparna Bandyopadhyay, Satyanarayana Vuppala |
| 2 | *Performance Analysis of AODV Routing Protocol in MANET* *under the influence of Routing Attack* | Melakukan serangan pada jaringan *Mobile Adhoc Network* (MANET) dengan jenis serangan *black hole, flooding* dan *rushing attack* | Simulasi | NS-2, AODV, tanpa keamanan, 20 s/d 80 *node* | HoudaMoudni, Mohamed Er-rouidi, HichamMouncif, Benachir El Hadadi |
| 3 | *Performance Evaluation of AODV Under Dos Attack* | Melakukan serangan pada jaringan *Adhoc* dengan jenis serangan *Hello Floods Attack* dan *Flooding Attack* | Simulasi | NS-3, AODV tanpa keamanan, 10 *node* | Poussy A. Lotfy, Marianne A. Azer |
| 4 | *Comparative Analysis of Star Topology and Multihop Outdoor Propagation Basen on Quality of Service (*QoS*) of Wireless Sensor Network (*WSN*)* | Melakukan analisis terhadap nilai QoS berupa *delay*, *throughput* dan *packet* *loss* pada jaringan WSN dengan topologi Star dan *Multihop* | Implementasi | XBee S2C, Sensor MQ-9, Star dan Multihop (Mesh) | Subuh Pramono, Arisa Olivia Putri, Endro Warsito, Budi Basuki |
| 5 | ZigBee *Based Wireless Sensor Network and Performance Analysis in Various Environment* | Melakukan uji performa jaringan Zigbee dengan dua keadaan yaitu LOS dan NLOS | Implementasi | XBee S2, ZigBee Protocol, AODV, *Line-of-Sight* (LOS), *Non Line-of-Sight* (NLOS) | Helmy Fitriawan, Misfa Susanto, Ahmad Surya Arifin, Danny Mausa, Agus Trisanto |

# BAB IV

**LANDASAN TEORI DAN HIPOTESIS**

### 3

Pada bab landasan teori dijelaskan berbagai macam teori mengenai *Internet of Things* secara umum beserta penerapannya, khususnya untuk teori yang mendalam tentang penerapannya dengan *smart device*. Selain itu juga dijelaskan teori pendukung mengenai komponen-komponen yang digunakan dalam proses implementasi jaringan *Ad hoc* menggunakan XBee ini. Penjelasan teori dimulai dari tinjauan singkat mengenai bagian-bagian penting dan mendasar dari sistem jaringan *wireless* yang merupakan dasar dalam pembuatan jaringan *Mobile Ad hoc Network* (MANET) itu sendiri. Pustaka yang dipilih disesuaikan berdasarkan keterkaitan isu dari pustaka dengan ruang lingkup topik yang dibahas secara lengkap dan menyeluruh sehingga dapat mendukung pemecahan masalah dalam penelitian ini.

Pada sub bab berikutnya dijelaskan hipotesisyang merupakan jawaban sementara terhadap permasalahan yang sedang diteliti dimana kebenarannya harus diuji secara empiris. Hipotesis dikatakan sementara karena jawaban yang diberikan baru didasarkan pada teori yang relevan dan belum didasarkan pada fakta-fakta yang empiris yang diperoleh melalui pengumpulan data (Hasibuan 2007).

#### Landasan Teori

##### J

#### Hipotesis

Berdasarkan sumber-sumber yang telah dirangkum di Tinjauan Pustaka, terdapat beberapa kesimpulan sementara :

1. MQTT menggunakan sistem publish-subscribe dimana server sebagai broker, dengan sistem ini cocok digunakan untuk memantau sensor dari platform lain.
2. CoAP menggunakan sistem client-server dimana untuk pengolahan datanya menggunakan metode CRUD (Create, Read, Update, dan Delete), sehingga kurang cocok untuk sistem yang terhubung dengan platform lain dan yang membutuhkan transportasi data secara real-time. Protokol ini lebih cocok digunakan dalam penyimpanan data.
3. MQTT melalui jalur transport TCP sedangkan CoAP melalui UDP dimana UDP memiliki sifat lebih ringan namun mempunyai resiko kehilangan data lebih tinggi, sehingga throughput CoAP lebih ringan daripada MQTT.

# BAB V

**METODE PENELITIAN**

### 3

###### Alat dan Bahan

Dalam penelitian ini, dibutuhkan beberapa perangkat dan bantuan pihak ketiga yang meliputi :

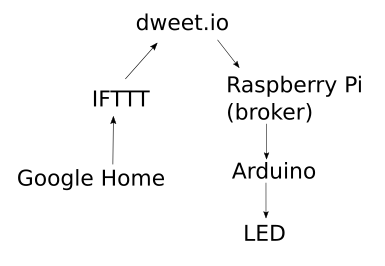
1. 1 buah nodemcu mega yang telah ditanamkan ESP8266
2. 1 buah nodemcu nano yang telah ditanamkan ESP8266
3. 1 buah breadboard ukuran *large*
4. 1 buah raspberry pi
5. 15 buah LED
6. 1 buah LED RGB
7. 5 buah motor DC
8. 1 buah sensor suhu
9. 1 buah router
10. 2 buah Google Home
11. 1 buah Alexa
12. 1 buah maket smart home

###### Prosedur Penelitian

1. **Perancangan Topologi**

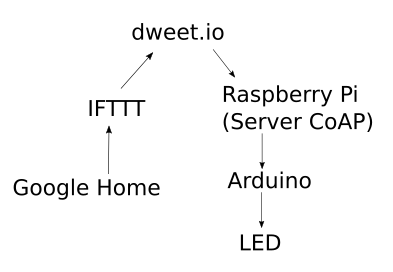
Dalam proses memperoleh data throughput dan latensi dari protokol CoAP dan MQTT, maka dibuatlah 2 skenario pengambilan data sebagai berikut :

* Skenario 1 – Rancangan protokol MQTT



Gambar 5.1 Rancangan Topologi protokol MQTT

* Skenario 2 – Rancangan protokol CoAP

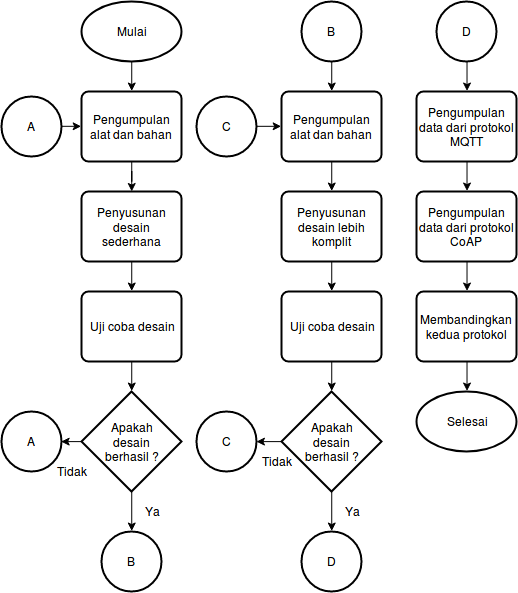


Gambar 5.2 Rancangan Topologi protokol CoAP

Perbedaan dari kedua skenario tersebut adalah topologi yang digunakan oleh kedua protokol. Proses pengambilan data dilakukan diantara dari Raspberry Pi dengan Arduino.

1. **Diagram Alir Metode Penelitian**

Metode penelitian yang dilakukan penulis dalam penelitian ini dapat dilihat pada *flow chart* berikut :



Gambar 5.3 *Flowchart* Penelitian

###### Analisis Hasil

Hasil dari penelitian ini berupa data perbandingan protokol CoAP dan MQTT menggunakan parameter throughput serta latensi. Angka-angka tersebut diambil dari software yang telah diletakkan diantara perangkat Arduino dengan Raspberry Pi. Data tersebut kemudian diolah dalam bentuk grafik beserta penjelasannya. Hasil lain dari penelitian ini berupa maket smart home yang telah diintegrasikan dengan *smart device.*

###### Jadwal Penelitian

Penelitian ini dirancang untuk dilaksanakan dalam kurun waktu 4 bulan, atau sesuai dengan tabel dibawah ini.

Tabel 5.2 Jadwal Penelitian

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Tahap Kegiatan | Bulan Ke : | | | | | | | | | | | | | | | | | | |
| 1 | | | | 2 | | | | | 3 | | | | | 4 | | | | |
| 1 | 2 | 3 | 4 | | 1 | 2 | 3 | 4 | | 1 | 2 | 3 | 4 | | 1 | 2 | 3 | 4 |
| Tahap Awal |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  |
| Identifikasi Masalah |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  |
| Perancangan Topologi |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  |
| Tahap Pelaksanaan |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  |
| Pengumpulan Alat dan Bahan |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  |
| Pengerjakan Perangkat Keras |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  |
| Pengerjakan Perangkat Lunak |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  |
| Percobaan dan Perbaikan |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  |
| Tahap Akhir |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  |
| Pengambilan Data |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  |
| Analisis Hasil |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  |
| Penyusunan Laporan |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  |

# DAFTAR PUSTAKA

Abdelshafy, Mohamed A., and Peter J. B. King. 2015. “Dynamic Source Routing under Attacks.” *IEEE* 7.

Asriyadi, and Rahmadi Kurnia. 2016. “Unjuk Kerja Protokol ZIGBEE pada Jaringan WSN.” *Jurnal Teknik Elektro ITP* 3.

Ayrton P, Muhammad Rihga. 2016. “Implementasi dan Analisis Kinerja Protokol Routing Ad hoc On-demand Distance Vector (AODV) pada Pemantauan Suhu dan Kelembaban Ruang Berbasis XBEE.”

Bandyopadhyay, Alokparna , and Satyanarayana Vuppala. 2011. “A Simulation Analysis of Flooding Attack in MANET using NS-3.” *IEEE.*

Basagni, Stefani , Marco Conti, Silvia Giordano, and Ivan Stojmenovic. 2004. *Mobile Ad hoc Networking.* New Jersey: IEEE Press.

Bundela, Avinash S., Prashant Panse, Gaurav Sharma, and Sachin Solanki. 2016. “A Secure Routing in Ad-Hoc Network.” *IEEE.*

Çayırcı, Erdal , and Chunming Rong. 2009. *Security in Wireless Ad Hoc and Sensor Networks.* United Kingdom.

Chlamtac, I. , and M. El-Zarki. 1994. *"Introduction to Computer Networks" in Encyclopedia of Telecommunications.*

Deng, Hongmei , Wei Li, and Dharma P. Agrawal. 2002. “Routing Security in Wireless Ad Hoc Networks.” *IEEE.*

Digi. n.d. *XCTU Configuration and Test Utility Software.*

Faludi, Robert. 2011. *Building Wireless Sensor Network.* 1st. California: O’Reilly Media, Inc.

Fitriawan, Helmy, Misfa Susanto, Ahmad Surya Arifin, Danny Mausa, and Agus Trisanto. 2017. “ZigBee Based Wireless Sensor Networks and Performance Analysis in various Environments.” Bali: IEEE.

Hasibuan, Zainal A. 2007. *Metode Penelitian Pada Bidang Ilmu Komputer dan Teknologi Informasi.*

Hebel, Martin, George Bricker, and Daniel Harris. 2010. *Getting Started with XBee RF Modules : A Tutorial for BASIC Stamp and Propeller Microcontrollers.* California: Parallax.

HoudaMoudni, Mohamed Er-rouidi, HichamMounci, and Benachir El Hadadi. 2016. “Performance Analysis of AODV Routing Protocol in MANET under the Influence of Routing Attacks.” *International Conference on Electrical and Information Technologies ICEIT.* Morroco: IEEE.

Ilyas, Mohammad . 2003. *THE HANDBOOK OF ADHOC WIRELESS NETWORK.* Florida: CRC Press LLC.

Leon-Garcia, Alberto , and Indra Widjaja. 2003. *Communication Networks Fundamental Concepts and Key Architectures.* The McGraw Companies.

Lin, Y. Bing , and I. Chlamtac. 2000. *Wireless and Mobile Network Architectures.* Wiley, .

Lotfy, Poussy A., and Marianne A. Azer. 2013. “Performance Evaluation of AODV Under DoS Attack.” *IEEE.*

Murthy, C. Siva Ram , and B. S. Manoj. 2004. *Ad Hoc Wireless Networks Architectures and Protocols.* New Jersey: Prentice Hall Professional Technical Reference.

Pramono, Subuh , Arisa Olivia, Endro Warsito, and Budi Basuki. 2017. “Comparative Analysis of Star Topology and Multihop Outdoor Propagation Based on Quality of Service (QoS) of Wireless Sensor Network (WSN).” Semarang: IEEE.

Thilak, K.Deepa. 2016. “DoS Attack on VANET Routing and possible defending solutions-A Survey.” Puducher