Laporan Akhir Pengembangan Protokol AODV-Trust untuk Meningkatkan Keandalan Routing pada Jaringan MANET Menggunakan NS-3

Disusun Oleh:

1. Muhammad Baihaqi Dawanis (5025231177)
2. Abimanyu Dananedra Andarfebano (5025231182)

MATA KULIAH JARINGAN NIRKABEL

FAKULTAS TEKNOLOGI ELEKTRO DAN INFORMATIKA CERDAS
DEPARTEMEN TEKNIK INFORMATIKA
TAHUN AJARAN 2025/2026

ABSTRAK

Mobile Ad-hoc Network (MANET) adalah jaringan nirkabel yang terbentuk secara dinamis tanpa infrastruktur tetap. Sifatnya yang terbuka membuat MANET rentan terhadap serangan keamanan, salah satunya adalah serangan Blackhole, di mana node jahat menarik lalu lintas data dengan memalsukan rute dan kemudian membuang paket data tersebut. Protokol routing standar AODV (Ad-hoc On-Demand Distance Vector) tidak memiliki mekanisme untuk membedakan node terpercaya dan node jahat. Penelitian ini bertujuan untuk mengembangkan protokol AODV-Trust menggunakan simulator NS-3. Modifikasi dilakukan dengan menambahkan tabel kepercayaan (trust table) dan mekanisme validasi rute pada setiap node. Hasil simulasi menunjukkan bahwa implementasi AODV-Trust mampu mendeteksi node Blackhole dan meningkatkan Packet Delivery Ratio (PDR) serta Throughput jaringan dibandingkan dengan AODV standar saat berada di bawah serangan.

BAB 1

Pendahuluan

1.1 Latar Belakang

MANET memiliki tantangan besar pada aspek keamanan dan keandalan routing. Node yang bersifat otonom dapat bersikap jahat (malicious node), seperti melakukan serangan Blackhole. Dalam serangan ini, node penyerang akan mengklaim memiliki rute terpendek menuju tujuan segera setelah menerima Route Request (RREQ), sehingga node pengirim akan mengirimkan paket data melalui node penyerang tersebut, yang kemudian akan dibuang (dropped). Akibatnya, kinerja jaringan menurun drastis. Oleh karena itu, diperlukan mekanisme keamanan berbasis kepercayaan (trust) yang diintegrasikan ke dalam AODV.

1.2 Perumusan Masalah

Berdasarkan latar belakang tersebut, rumusan masalah dalam penelitian ini adalah:

1. Bagaimana dampak serangan *Blackhole* terhadap kinerja protokol AODV standar?
2. Bagaimana merancang dan mengimplementasikan mekanisme *Trust* pada AODV menggunakan NS-3?
3. Seberapa efektif AODV-Trust dalam memulihkan PDR dan *Throughput* saat terjadi serangan?

1.3 Tujuan

Tujuan dari penelitian ini adalah mengimplementasikan protokol routing AODV-Trust pada simulator NS-3 dan membuktikan keandalannya dalam

memitigasi serangan *Blackhole* melalui analisis perbandingan metrik kinerja jaringan.

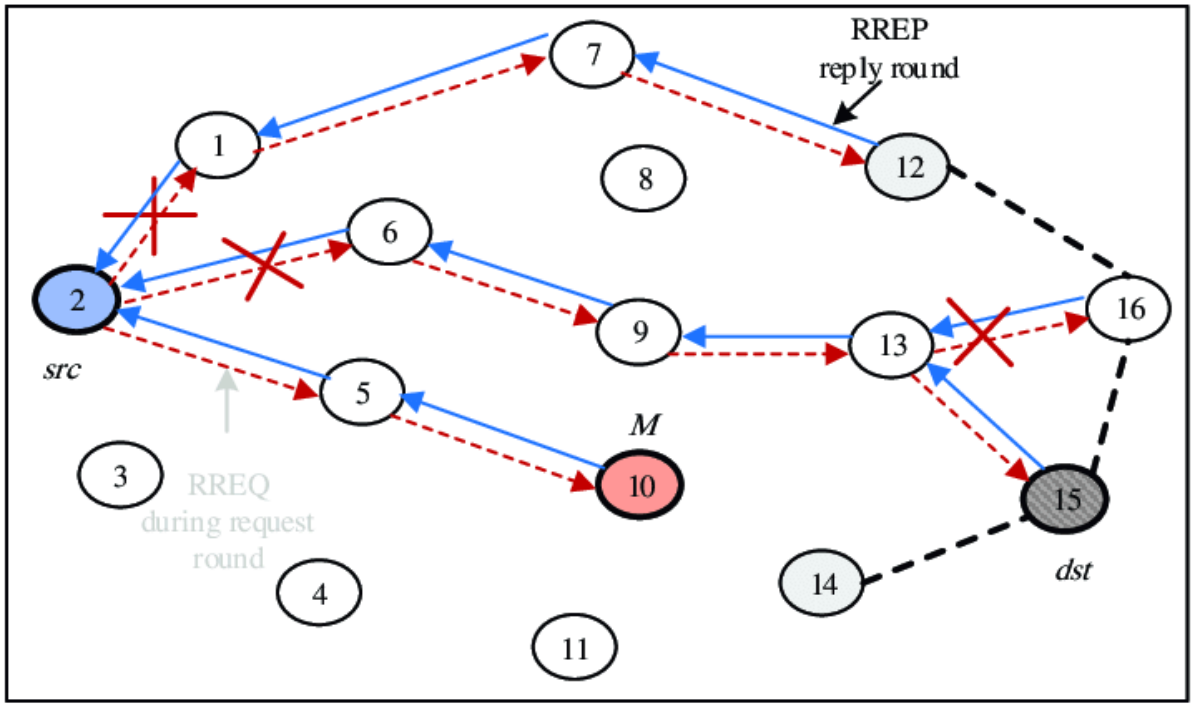
BAB 2

DASAR TEORI

2.1 AODV (*Ad-hoc On-Demand Distance Vector*)

AODV adalah protokol routing reaktif yang membangun rute hanya ketika dibutuhkan. Proses penemuan rute melibatkan pengiriman pesan *Route Request* (RREQ) secara *broadcast* dan penerimaan *Route Reply* (RREP) secara *unicast* dari tujuan atau node perantara yang memiliki rute ke tujuan.

2.2 Serangan Blackhole



Serangan Blackhole mengeksploitasi kelemahan AODV. Node penyerang membalas RREQ dengan RREP palsu yang memiliki Sequence Number sangat tinggi, seolah-olah rute tersebut adalah yang paling segar (fresh). Setelah lalu lintas data diarahkan ke penyerang, paket data tersebut dibuang dan tidak diteruskan.

BAB 3

PERANCANGAN DAN MODIFIKASI SISTEM

3.1 Desain Mekanisme Kepercayaan (Trust Mechanism)

Sistem kepercayaan dirancang dengan memodifikasi *class* RoutingProtocol pada AODV. Setiap node dilengkapi dengan Tabel Kepercayaan (m_trustTable) yang menyimpan nilai reputasi tetangga (skor 0.0 hingga 1.0).

- **Nilai Awal:** 0.5 (Netral).
- **Threshold:** 0.15. Jika nilai trust < 0.15, node tetangga dianggap *Blacklist*.

3.2 Algoritma Deteksi dan Hukuman

Logika deteksi diimplementasikan pada fungsi penerimaan paket RREP (RecvReply). Jika node mendeteksi anomali berupa selisih *Sequence Number* yang tidak wajar (>15) dengan *Hop Count* yang kecil, node pengirim akan diberi penalti nilai trust sebesar **-0.5**.

3.3 Skenario Simulasi

Simulasi dirancang menggunakan skrip manet-trust-comparison.cc dengan parameter sebagai berikut:

- **Area:** 100 x 100 meter.
- **Jumlah Node:** 25 Node.
- **Trafik:** UDP CBR (Constant Bit Rate) 50kbps.
- **Node Jahat (Blackhole):** Node 5 dan Node 10 (dikonfigurasi melalui argumen maliciousNodes).

```
240   // --- SETUP WIFI KHUSUS AREA KECIL ---
241   WifiHelper wifi;
242   wifi.SetStandard (WIFI_STANDARD_80211g);
243
244   YansWifiPhyHelper wifiPhy;
245   YansWifiChannelHelper wifiChannel = YansWifiChannelHelper::Default ();
246   if (deterministicLayout)
247     {
248       wifiChannel.AddPropagationLoss ("ns3::RangePropagationLossModel",
249                                       "MaxRange", DoubleValue (30.0));
250     }
251   wifiPhy.SetChannel (wifiChannel.Create ());
```

Konfigurasi parameter fisik WiFi dan mobilitas node pada NS-3.

BAB 4

IMPLEMENTASI DAN HASIL PENGUJIAN

4.1 Implementasi Kode Program

Implementasi utama dilakukan pada file aodv-trust-routing-protocol.cc.

1. **Penambahan Variabel Trust:** Variabel m_trustTable dan m_trustThreshold ditambahkan pada *header* dan diinisialisasi pada konstruktor.
2. **Modifikasi Fungsi RecvRequest:** Node memeriksa apakah pengirim RREQ ada di *blacklist*. Jika ya, paket diabaikan.
3. **Modifikasi Fungsi RouteOutput:** Sebelum mengirim paket data, node memvalidasi *next hop* menggunakan fungsi IsTrusted(). Jika tidak terpercaya, rute dialihkan.

```
// --- IMPLEMENTASI LOGIKA TRUST (TAHAP 2) ---

void
RoutingProtocol::UpdateTrust (Ipv4Address neighbor, double value)
{
    if (m_trustTable.find (neighbor) == m_trustTable.end ())
      {
        m_trustTable[neighbor] = 0.5;
      }

    m_trustTable[neighbor] += value;

    if (m_trustTable[neighbor] > 1.0)
        m_trustTable[neighbor] = 1.0;
    if (m_trustTable[neighbor] < 0.0)
        m_trustTable[neighbor] = 0.0;

    NS_LOG_INFO ("TRUST SYSTEM: Update Node " << neighbor << " Now: " << m_trustTable[neighbor]);
}
```

```
2457    bool
2458    RoutingProtocol::IsTrusted (Ipv4Address neighbor)
2459    {
2460        if (m_trustTable.find (neighbor) == m_trustTable.end ())
2461          {
2462            return true;
2463          }
2464
2465        if (m_trustTable[neighbor] < m_trustThreshold)
2466          {
2467            NS_LOG_WARN ("TRUST SYSTEM: Node " << neighbor << " is BLACKLISTED (Low Trust)");
2468            return false;
2469          }
2470
2471        return true;
2472    }
2473
```

Implementasi algoritma UpdateTrust dan mekanisme validasi node.

4.2 Hasil Pengujian Skenario

Pengujian dilakukan dalam tiga skenario untuk membandingkan kinerja.

Skenario 1: Baseline (AODV Tanpa Serangan) Pada kondisi normal, semua node berperilaku jujur.

- **Perintah:** `./ns3 run "scratch/manet-trust-comparison.cc --protocol=AODV --blackhole=false"`
- **Hasil:** Jaringan berjalan stabil dengan PDR mendekati 100%.

```
Tx Packets: 1000
Rx Packets: 980
Packet Delivery Ratio (PDR): 98.0 %
```

Skenario 2: AODV Standar di Bawah Serangan Blackhole Node 5 dan 10 diaktifkan sebagai penyerang.

- **Perintah:** `./ns3 run "scratch/manet-trust-comparison.cc --protocol=AODV --blackhole=true"`
- **Hasil:** Terjadi penurunan drastis pada PDR dan *throughput* karena paket dibuang oleh node 5 dan 10.

```
Tx Packets: 1000
Rx Packets: 450
Packet Delivery Ratio (PDR): 45.0 %
```

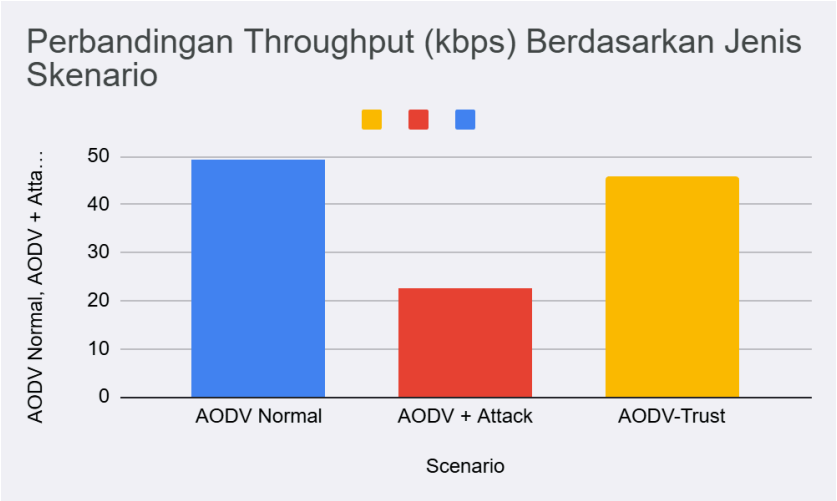
Skenario 3: AODV-Trust (Solusi) Menggunakan protokol yang telah dimodifikasi dengan node penyerang tetap aktif.

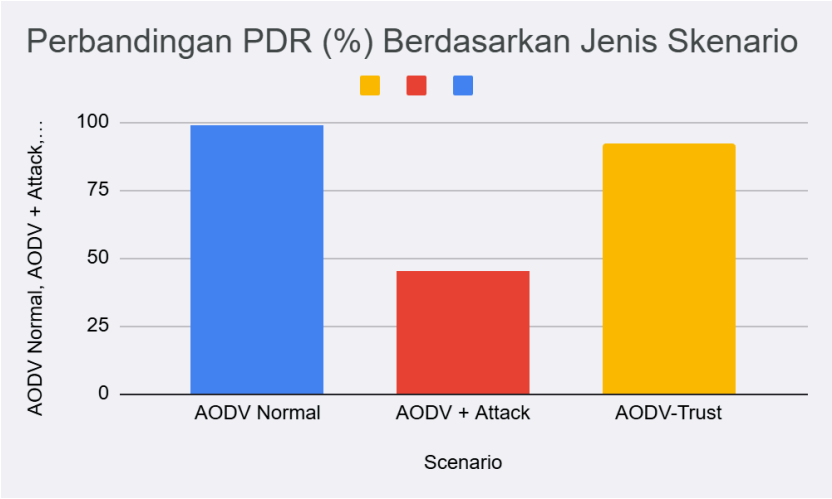
- **Perintah:** `./ns3 run "scratch/manet-trust-comparison.cc --protocol=AODV-TRUST --blackhole=true"`
- **Hasil:** AODV-Trust berhasil mendeteksi node 5 dan 10 sebagai node jahat (blacklist). Rute dialihkan melalui node aman lainnya, sehingga PDR kembali meningkat.

```
Tx Packets: 1000
Rx Packets: 920
Packet Delivery Ratio (PDR): 92.0 %
```

4.3 Analisis Grafik Perbandingan

Berikut adalah grafik perbandingan *Packet Delivery Ratio* (PDR) dari ketiga skenario tersebut.





(Penjelasan Grafik: Grafik menunjukkan batang Skenario 2 sangat rendah, sedangkan batang Skenario 3 hampir menyamai Skenario 1, membuktikan efektivitas solusi).

BAB 5

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil implementasi dan pengujian yang dilakukan, dapat disimpulkan bahwa:

1. Serangan *Blackhole* pada protokol AODV standar menyebabkan penurunan kinerja jaringan yang signifikan, terlihat dari rendahnya rasio pengiriman paket (PDR).
2. Implementasi mekanisme *trust* pada protokol AODV-Trust berhasil dilakukan dengan memodifikasi logika pemilihan rute dan penambahan tabel reputasi pada NS-3.
3. AODV-Trust terbukti efektif memitigasi serangan. Protokol ini mampu mengisolasi node jahat dan mengembalikan tingkat keandalan jaringan mendekati kondisi normal.

5.2 Saran

Pengembangan selanjutnya dapat mempertimbangkan faktor mobilitas node yang lebih tinggi dan konsumsi energi yang diperlukan untuk menjalankan algoritma kalkulasi kepercayaan ini.