

## ANALISIS DAN IMPLEMENTASI ALGORITMA MODIFIKASI-AD HOC ON-DEMAND DISTANCE VECTOR (AODV) UNTUK MENGATASI BLACKHOLE ATTACK DAN WORMHOLE ATTACK PADA MOBILE AD-HOC NETWORK (MANET)

Wahyu Fajar Pratama<sup>1</sup>, Setyorini<sup>2</sup>, Dodi Wisaksono Sudiharto<sup>3</sup>

<sup>1</sup>Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

---

### Abstrak

Mobile Ad-Hoc Network (MANET) merupakan sebuah jaringan nirkabel yang menjadi solusi dalam suatu keadaan tertentu, dengan hanya mengandalkan device-device yang ada, device tersebut bisa melakukan komunikasi tanpa adanya infrastruktur tambahan. Dengan kemampuan wireless-fidelity pada device tersebut, node dapat melakukan pengiriman pesan ke node tertentu. Node-node pada jaringan MANET memiliki kemampuan routing, layaknya router. Protokol routing pada MANET ada beberapa jenis seperti AODV, DSDV, TORA, dan sebagainya yang mempunyai karakteristik masing-masing dalam penemuan jalur rutingnya. Karena tidak mempunyai infrastruktur khusus untuk melakukan routing dan node-nodenya bersifat mobile maka mekanisme routingnya memiliki keamanan yang rendah. Mobile Ad-Hoc Network (MANET) merupakan sebuah jaringan nirkabel yang menjadi solusi dalam suatu keadaan tertentu, dengan hanya mengandalkan device-device yang ada, device tersebut bisa melakukan komunikasi tanpa adanya infrastruktur tambahan. Dengan kemampuan wireless-fidelity pada device tersebut, node dapat melakukan pengiriman pesan ke node tertentu. Node-node pada jaringan MANET memiliki kemampuan routing, layaknya router. Protokol routing pada MANET ada beberapa jenis seperti AODV, DSDV, TORA, dan sebagainya yang mempunyai karakteristik masing-masing dalam penemuan jalur rutingnya. Karena tidak mempunyai infrastruktur khusus untuk melakukan routing dan node-nodenya bersifat mobile maka mekanisme routingnya memiliki keamanan yang rendah.

Serangan Blackhole dan serangan Wormhole pada MANET merupakan serangan yang menyerang pada mekanisme routing AODV dengan ciri penyerangan yang khas. Dalam tugas akhir ini dilakukan simulasi penyerangan blackhole dan wormhole, serta modifikasi protokol AODV sebagai solusi untuk mempertahankan performansinya ketika terserang blackhole maupun wormhole.

Tujuan dari penelitian adalah membandingkan performansi modifikasi protokol routing AODV dan AODV standar terhadap ketika dilakukan penyerangan blackhole dan wormhole. Hasil yang didapat adalah serangan blackhole dan wormhole dapat menurunkan performansi jaringan yang signifikan dilihat dari parameter uji packet loss yang besar pada kisaran 70-80 %, dan delay yang besar. Dengan melakukan modifikasi AODV terbukti dapat mempertahankan performansi jaringan, dengan nilai packet loss pada kisaran 10%, dan delay yang kecil.

Kata Kunci : MANET, AODV, Serangan Wormhole, Serangan Blackhole, Packet loss, Delay

---

#### Abstract

Mobile Ad-Hoc Network (MANET) is a wireless network into a solution in certain condition, by simply relying on existing devices, the devices can communicate without any additional infrastructure. With wireless-fidelity capabilities in peripheral devices, nodes can make sending messages to a specific node. The nodes in the MANET network has routing capabilities, like a router. On MANET routing protocols there are several types such as AODV, DSDV, TORA, and so forth that have the characteristics of each in the discovery routing pathway. Because it had no special infrastructure to perform routing and node-node is mobile then its routing mechanism has low security.

Blackhole attacks and Wormhole attacks in MANET is an attack that attacks on AODV routing mechanism with the characteristics of a typical attack. In this thesis performed simulations blackhole and wormhole attacks, as well as modification of AODV protocol as a solution to maintain performansinya when attacked by blackhole or wormhole

The purpose of this study was to compare the performance of AODV routing protocol modifications and standard AODV against when performed blackhole and wormhole attacks. The results obtained are the blackhole and wormhole attack can decrease network performance parameters that significantly viewed from a large test packet loss in the range 70-80%, and a big delay. By modifying AODV shown to maintain network performance, with a value of packet loss in the range of 10%, and a small delay.

Keywords : MANET, AODV, Wormhole attack, Blackhole attack, Packet loss, Delay



# 1. Pendahuluan

## 1.1 Latar Belakang

*Mobile Ad Hoc Network* (MANET) yaitu sebuah jaringan *wireless* yang terdiri dari mobile-mobile node yang tidak memiliki infrastruktur. Jaringan ini merupakan salah satu mode jaringan *wireless ad hoc* akan tetapi node-node atau user pada jaringan ini bersifat mobile. Node bebas datang dan meninggalkan jaringan, node juga bebas bergerak atau diam pada posisinya MANET bisa terbentuk dari sekumpulan *node* yang menggunakan antarmuka nirkabel (*wireless interface*) mereka untuk melakukan komunikasi antara satu *node* dengan *node* yang lainnya. Untuk melakukan komunikasi tersebut maka node tersebut menggunakan protokol routing untuk memilih jalur terbaik untuk pengiriman pesan dari alternatif route yang dihasilkan dan diterima oleh node sumber [1]. Banyak algoritma protokol routing yang telah dikembangkan, antara lain AODV, DSDV, DSR, TORA

Protokol routing *Ad hoc on-demand distance vector* (AODV) banyak digunakan sebagai Protokol *routing* ini mengacu kepada protokol *routing* DSDV dengan penambahan fungsi broadcast untuk meminta *route*. Protokol ini mampu menangani perubahan topologi dan bebas dari looping *route*. Ketika suatu *route* dibutuhkan oleh suatu *node*, maka *node* tersebut akan mem-broadcast pesan "*route request*" ke semua *link*. Respon dari pesan tersebut kemudian dikirim balik oleh *node* penerima atau intermediate *node* yang berisi *route* baru untuk ke *node* tujuan [2].

Protokol routing AODV memiliki beberapa kelemahan, antara lain yaitu mudah disusupi penyerang. Tipe penyerangan yang banyak dan mungkin dilakukan pada AODV adalah Serangan Blackhole dan Wormhole. biasanya terjadi pada protokol routing reaktif. Karakteristik Blackhole attack dan wormhole attack adalah dropping paket, sehingga banyak paket yang hilang ketika node penerima menerima jumlah paket tertentu, tentu hal tersebut sangat mengganggu komunikasi dalam jaringan MANET [16]. Karena hal tersebut maka diperlukan suatu mekanisme pertahanan terhadap blackhole dan wormhole pada protokol routing AODV. Skema pertahanan yang dilakukan dengan memodifikasi mekanisme routing AODV dengan fungsi-fungsi tambahan untuk meng-handling terhadap serangan tersebut [15].

## 1.2 Perumusan Masalah

Berdasarkan latar belakang, maka dapat dirumuskan beberapa masalah yaitu:

- a. Bagaimana *Wormhole Attack* dan *Blackhole Attack* menyerang pada mekanisme routing protocol pada MANET
- b. Bagaimana Algoritma modifikasi AODV diterapkan untuk mengatasi serangan *Blackhole attack* dan *Wormhole attack* pada MANET
- c. Menganalisis algoritma modifikasi AODV untuk mempertahankan performansi jaringan MANET dari serangan blackhole dan wormhole

### 1.3. Batasan Masalah

Dalam implementasi tugas akhir ini dibatasi oleh beberapa hal, sebagai berikut:

- a. Protokol routing yang dimodifikasi adalah AODV
- b. Serangan jaringan yang dipilih adalah *Blackhole* dan *Wormhole attack*, karena banyak menyerang pada jaringan MANET dengan protokol AODV
- c. Serangan yang dilakukan hanya berasal dari satu node
- d. Pengujian terfokus pada seberapa resisten modifikasi AODV yang dilakukan terhadap *blackhole attack* dan *wormhole attack*
- e. Pengujian resistensi modifikasi AODV dilakukan dengan waktu simulasi yang bervariasi serta mengubah-ubah pergerakan node
- f. Parameter-parameter pengujian yang dianalisis adalah *average end to end delay* dan *packet loss*
- g. Dalam pengujian Tugas Akhir ini hasil pengujian terfokus pada faktor *blackhole attack* dan *wormhole attack*, sedangkan penyebab menurunnya performansi karena antrian penuh / buffer penuh diabaikan, akan dijelaskan pada sub bab 4.3.4.1

### 1.4 Tujuan

Tujuan yang ingin dicapai dalam tugas akhir ini, yaitu :

- a. Mensimulasikan penyerangan *Wormhole* dan *Blackhole* pada jaringan berbasis *mobile ad-hoc*
- b. Mengimplementasikan algoritma modifikasi AODV untuk menghadapi *Blackhole attack* dan *wormhole attack*
- c. Menganalisis kehandalan algoritma modifikasi AODV untuk mengatasi *Blackhole attack* dan *Wormhole attack* dengan parameter pengujian *packet loss*, *Average end to end delay*.
- d. Menganalisis efektifitas algoritma modifikasi AODV dalam faktor waktu simulasi yang diperbesar (jika waktu diperbesar maka jumlah paket yang dikirim juga makin besar) dan kecepatan *mobility node* yang diperbesar.

### 1.5 Hipotesis

Algoritma modifikasi AODV mampu dalam mengatasi serangan *Blackhole* maupun *Wormhole* dalam jumlah *node* banyak maupun sedikit serta maksimum *mobility* yang kecil maupun besar dan memulihkan performansi *routing* AODV (kembali seperti sebelum terserang *Attacking*)

## 1.6 Metodologi Penyelesaian Masalah

Metodologi penyelesaian masalah yang akan digunakan adalah :

- a. Studi Literatur, yaitu dengan mempelajari literatur-literatur yang ada sesuai dengan permasalahan meliputi konsep dari routing, protocol routing pada *wireless*, Jenis-jenis serangan pada jaringan *wireless*, tentang NS-2 sebagai simulatornya
- b. Analisa kebutuhan sistem dan perancangan skenario simulasi yaitu melakukan analisa terhadap model simulasi yang akan dibangun
- c. Simulasi sistem dengan menggunakan NS-2 sebagai *network simulator* dengan modul *wireless*
- d. Analisis hasil, yaitu menganalisis hasil pengujian dengan parameter pengujian *Packet loss*, *Average end to end delay*
- e. Pembuatan laporan, melakukan pelaporan hasil pengerjaan Tugas Akhir berupa analisis sistem yang dibangun beserta dokumentasinya.



## 5. Penutup

### 5.1 Kesimpulan

Berdasarkan hasil pengujian dan analisis yang dilakukan, maka dapat diambil beberapa kesimpulan, yaitu :

1. Serangan Blackhole dan wormhole yang terjadi pada jaringan MANET berhasil menurunkan performansi jaringan, hal ini ditunjukkan oleh paketloss dan delay yang besar, sesuai dengan karakteristik serangan
2. Penanganan Blackhole dan Wormhole Attack dengan modifikasi Protokol routing AODV memiliki performansi yang cukup baik, jika dilihat dari rata-rata paket loss antara AODV biasa dan AODV modifikasi, bisa menghasilkan efektifitas sekitar 70 – 80 % ketika jaringan terserang blackhole attack dan wormhole attack
3. Modifikasi Protokol Routing AODV mampu mempertahankan performansinya ketika jumlah paket yang dikirim makin besar dan mobility node yang diperbesar.

### 5.2 Saran

Setelah menyelesaikan proses pengerjaan tugas akhir ini, maka ada beberapa saran untuk bisa mengembangkan sistem menjadi lebih baik.

1. Perlu dilakukan penelitian dan pengujian lebih lanjut jika topologinya dibuat padat, apakah algoritma modifikasi AODV masih efektif dalam menangani *blackhole* dan *wormhole*.
2. Perlu dilakukan penelitian juga bagaimana jika dalam satu topologi ada banyak *attacker* dengan jenis yang sama atau beda dan bagaimana penanganannya, karena dalam realitanya penyerangan terhadap node / data yang digunakan untuk komunikasi rahasia berasal dari berbagai pihak dengan tipe serangan yang bervariasi
3. Perlu dilakukan pengembangan metode yang lebih bagus terhadap penanganan serangan terhadap MANET, karena berdasar hasil pengujian modifikasi protokol routing dalam hal ini modifikasi AODV masih menghasilkan paket loss sekitar 9 – 20 %, jika paket yang dikirim sangat penting, seperti *streaming video*, hal tersebut sangat berpengaruh.

## Daftar Pustaka

- [1]. Ad-hoc Network. 2009. <http://hendri.staff.uns.ac.id/2009/12/jaringan-ad-hoc/> , diakses pada 3 Juli 2011
- [2]. IETF MANET, 1999. <http://www.ietf.org/rfc/rfc2501.txt> , diakses pada 22 Maret 2011
- [3]. Juan-Carlos Ruiz, Jesús Friginal, David de-Andrés, Pedro Gil.2010, “Black Hole Attack Injection in Ad hoc Networks”
- [4]. Jhavri, Parmar, Patel ashish. ( 2010 ) , “ MANET Routing Protocols and Wormhole Attack against AODV” , *International Journal of Computer Science and Network Security*, VOL.10 No.4.
- [5]. Latha Tamilselvan, V Sankaranarayanan ( 2007) . “ Prevention of Blackhole Attacks in MANET.” In: Proceedings of the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007), pp. 21-21, Aug. 2007.
- [6]. Malarkodi, Venkatara, Predeep, “ Modified AODV protocol for Prevention Denial of service attack” , Proceedings of the 5th WSEAS Int. Conf. on APPLIED INFORMATICS and COMMUNICATIONS
- [7]. Mistry, Nital, Jinwala, Devesh. 2010. “ MOSAODV : solution to secure AODV against Blackhole attack. *International Journal of Computer and Network Security* Vol.1 No.3.
- [8]. Mobile Ad-hoc Network.2010. <http://elreg-02.blogspot.com/2010/01/mobile-ad-hoc-network-manet.html>. Diakses 2 Februari 2011
- [9]. Modul Pelatihan NS-2. 2009. Lab.Teknik Switching IT Telkom
- [10]. Payal N. Raj, Prashant B. Swadas,. 2009. “DPRAODV : A Dyanamic Learning System Against Blackhole Attack In Aodv Based MANET” , *IJCSI International Journal of Computer Science Issues*, Vol. 2, 2009
- [11]. Prahladachar, Anitha. 2009. “Secure routing with AODV Protocol for Mobile Ad-Hoc Network” . Departement of Computer Science University of Windsor.
- [12]. Riri Fitri Sari, Abdusy Syarif .2008. “Analisis Kinerja Routing Protokol AODV pada jaringan Ad Hoc Hybrid: perbandingan hasil simulasi dengan NS-2 dan implementasi pada tesbed dengan PDA” . *Makara Teknologi* Volume 12, No.1, April 2008: 7-11
- [13]. SAODV, Manel Guerrero Zapata. 2006. <http://people.ac.upc.edu/guerrero/> diakses pada 11 Juni 2011
- [14]. S. Sharma. , Gupta Roopam. (2009), “Simulation Study of Blackhole Attack” , *Journal of Engineering Science and Technology* Vol. 4, No. 2 243 – 250, School of Engineering, Taylor’s University College



- [15]. Security Aspects in Mobile Ad Hoc Network (MANETs), 2011  
<http://www.krazytech.com/technical-papers/computer-science-technical-papers-technical-papers/security-aspects-in-mobile-ad-hoc-network-manets>, diakses pada 29 September 2011.
- [16]. Simaremare, Harris.2011. "Performance Evaluation of AODV variants on DdoS, Blackhole and Malicious attacks ". International Journal of Computer and Network Security Vol.11 No 6, June 2011
- [17]. Tun,Zaw and Maw htein Aung, 2008 " Wormhole Attack Detection in Wireless Sensor Networks ", World Academy of Science, Engineering and Technology 46.
- [18]. Wireless Ad-Hoc Testbed . 2009.  
<http://www.ee.surrey.ac.uk/ccsr/facilities/networks/wat>
- [19]. Yongguang Zhang , Wenke Lee , Yi-An Huang, 2008, " Intrusion detection techniques for mobile wireless networks", Wireless Networks journal , v.9 n.5, p.545-556.

