Universitas Indonesia Library >> UI - Disertasi Membership

Pengembangan dan evaluasi kinerja protokol routing aodv yang aman dan optimal berbasis mekanisme kepercayaan dan algoritma semut = A development of secure and optimized aodv routing protocol using ant algorithm

Simaremare, Harris, author

Deskripsi Lengkap: https://lib.ui.ac.id/detail?id=20364584&lokasi=lokal

---

Abstrak

Saat ini jaringan nirkabel telah berkembang dengan pesat pada bidang teknologi telekomunikasi. Jaringan nirkabel memiliki sifat utama yaitu menyediakan akses informasi tanpa memperhatikan posisi geografi dan jenis topologi jaringan. Salah satu teknologi komunikasi nirkabel yang populer saat ini adalah Mobile Adhoc Network (MANET). MANET memiliki sifat terdesentralisasi, mampu mengorganisasi diri sendiri dan tidak memiliki infrastruktur tetap. Node meneruskan paket komunikasi antara satu dengan lainnya untuk menemukan dan membentuk jalur komunikasi. Dikarenakan tidak adanya node yang berfungsi sebagai pengatur, setiap node di dalam jaringan bertanggung jawab atas keberlangsungan komunikasi. Seperti tipe jaringan lainnya, MANET berjalan menggunakan protokol routing. Beberapa protokol routing yang berjalan di MANET antara lain Ad Hoc on Demand Distance Vector (AODV), Optimized Link State Routing (OLSR), dan Dynamic Source Routing (DSR).

Disebabkan oleh karakteristik jaringan yang unik, terdapat dua isu penting dalam pengembangan protokol komunikasi pada MANET yaitu isu kinerja dan isu keamanan. Dibandingkan dengan protokol routing MANET lainnya, protokol routing AODV memiliki kinerja yang lebih baik. Aspek keamanan protokol routing AODV ditingkatkan dengan menggunakan dua mekanisme yaitu mekanisme kriptografi dan mekanisme kepercayaan. Mekanisme kepercayaan memiliki kinerja yang lebih baik dibandingkan dengan mekanisme kriptografi. Pada penelitian ini, mekanisme kepercayaan dipilih untuk meningkatkan keamanan dari protokol routing AODV.

Pada bagian pertama, dikombinasikan fasilitas gateway pada AODV+ dan reverse route pada protokol R-AODV untuk mendapatkan protokol optimal yang bisa berjalan pada jaringan hibrid. Protokol yang diusulkan dinamakan AODV-UI. Untuk dapat berkomunikasi dengan jaringan infrastruktur, digunakan mode gateway dari protokol AODV+. Sedangkan reverse route pada protokol R-AODV digunakan untuk meningkatkan kinerja protokol AODV. Kinerja dari protokol AODV-UI dievaluasii menggunakan NS-2 dengan parameter packet delivery rate, end to end delay dan routing overhead.

Hasil simulasi menunjukkan bahwa protokol AODV-UI memiliki kinerja yang lebih baik dibandingkan dengan protokol AODV+. Konsumsi energi dan kinerja protokol AODV-UI dievaluasi dengan jenis mobilitas yang berbeda. Jenis mobilitas yang digunakan adalah random waypoint (RWP) dan Reference Point Group Mobility (RPGM). Hasil simulasi menunjukkan bahwa protokol AODV-UI memiliki kinerja lebih baik dan konsumsi energi lebih kecil apabila menggunakan jenis mobilitas RWP. Protokol AODV-UI lebih sesuai menggunakan mobilitas RWP. Kontribusi kedua pada penelitian ini adalah diusulkan mekanisme kepercayaan baru untuk meningkatkan keamanan dari protokol AODV. Protokol yang diusulkan dinamakan Trust AODV. Paket komunikasi hanya dikirimkan ke node tetangga yang terpercaya. Perhitungan tingkat kepercayaan berdasarkan pada perilaku dan informasi aktifitas setiap node. Perhitungan tingkat kepercayaan dibagi menjadi dua yaitu Trust Global (TG) dan Trust Local (TL). TG adalah tingkat

kepercayaan yang dihitung berdasarkan perbandingan antara seluruh paket yang diterima dengan seluruh paket yang diteruskan oleh setiap node. Sedangkan TL adalah perbandingan antara seluruh paket yang diterima dengan seluruh paket yang diteruskan oleh node tetangga yang berasal dari node tertentu. Node menyimpulkan total tingkat kepercayaan dengan menggabungkan nilai perhitungan TL dan TG. Sebuah node dianggap terpercaya apabila nilai TG dan TL adalah terpercaya. Apabila node dicurigai sebagai node penyerang, maka mekanisme keamanan akan mengisolasinya dari jaringan sebelum komunikasi dijalankan. Kinerja Protokol Trust AODV dievaluasi dengan serangan DOS/DDOS dan blackhole, kemudian dibandingkan dengan protokol sejenis dalam hal ini protokol TCLS. Hasil simulasi menunjukkan bahwa Protokol Trust AODV memiliki kinerja yang lebih baik dalam hal end to end delay, packet delivery rate dan routing overhead. Pada skenario jumlah serangan tetap dan kecepatan mobilitas divariasikan, nilai rata-rata end to end delay turun sebesar 44.37%, ratarata packet delivery rate naik sebesar 29.65% dan rata-rata routing overhead turun sebesar 64.2%. Pada skenario jumlah serangan dinaikkan, rata-rata penurunan end to end delay sebesar 70.1%, peningkatan packet delivery rate sebesar 30.5% dan rata-rata penurunan overhead sebesar 82.7%.

Kontribusi terakhir adalah optimalisasi kinerja protokol Trust AODV menggunakan algoritma semut. Protokol yang diusulkan dinamakan Trust AODV+Ant. Implementasi algoritma semut pada protokol Trust AODV adalah dengan menambahkan paket agen. Agen berfungsi mencari jalur komunikasi dan meletakkan feromon positif pada setiap node yang dianggap terpercaya disepanjang jalur komunikasi. Nilai feromon positif disimpan di tabel routing pada setiap node. Tabel routing node dimodifikasi dengan menambahkan field nilai feromon. Jalur komunikasi dipilih berdasarkan nilai konsentrat feromon dan jalur terpendek. Untuk meningkatkan kinerja protokol, jumlah paket agen dikontrol menggunakan mekanisme Controlled Neighbor Broadcast (CNB) yang diadopsi dari protokol SARA. Pada mekanisme CNB, hanya satu node yang memiliki otoritas untuk meneruskan agen ke lingkungan tetangga berikutnya. Kinerja protokol Trust AODV+Ant diuji menggunakan NS-2. Kinerja protokol yang diusulkan dibandingkan dengan protokol AODV, SARA dan protokol Trust AODV ketika serangan DOS/DDOS dilakukan.

Hasil simulasi menunjukkan bahwa nilai packet delivery rate dan throughput dari protokol Trust AODV meningkat setelah menggunakan algoritma semut. Akan tetapi dalam hal end to end delay peningkatan kinerja tidak signifikan. Nilai rata-rata packet delivery rate meningkat sebesar 4.58%, dan nilai rata-rata throughput meningkat sebesar 4.81%. Sedangkan penurunan end to end delay sebesar 1.08%.

.....

Currently wireless networks have grown significantly in the field of telecommunication networks. Wireless networks have the main characteristic of providing access of information without considering the geographical and the topological attributes of a user. One of the most popular wireless network technologies is mobile ad hoc networks (MANET). A MANET is a decentralized, self-organizing and infrastructure-less network. Every node acts as a router for establishing the communication between nodes over wireless links. Since there is no administrative node to control the network, every node participating in the network is responsible for the reliable operation of the whole network. Nodes forward the communication packets between each other to find or establish the communication route. As in all networks, MANET is managed and become functional with the use of routing protocols. Some of MANET routing protocol are Ad Hoc on Demand Distance Vector (AODV), Optimized Link State Routing (OLSR), Topology Dissemination Based on Reverse-Path Forwarding (TBRPF), and Dynamic Source Routing (DSR).

Due to the unique characteristics of mobile ad hoc networks, the major issues to design the routing protocol

are a security aspect and network performance. In term of performance, AODV has better performance than other MANET routing protocols. In term of security, secure routing protocol is divided in two categories based on the security method, i.e. cryptographic mechanism and trust based mechanism. We choose trust mechanism to secure the protocol because it has a better performance rather than cryptography method.

In the first part, we combine the gateway feature of AODV+ and reverse method from R-AODV to get the optimized protocol in hybrid network. The proposed protocol called AODV-UI. Reverse request mechanism in R-AODV is employed to optimize the performance of AODV routing protocol and gateway module from AODV+ is added to communicate with infrastructure node. We perform the simulation using NS-2 to evaluate the performance of AODV-UI. Performance evaluation parameters are packet delivery rate, end to end delay and routing overhead. Simulation results show that AODV-UI outperformed AODV+ in term of performance. The energy consumption and performance are evaluated in simulation scenarios with different number of source nodes, different maximum speed, and also different mobility models. We compare these scenarios under Random Waypoint (RWP) and Reference Point Group Mobility (RPGM) models.

The simulation result shows that under RWP mobility model, AODV-UI consume small energy when the speed and number of nodes access the gateway are increased. The performance comparison when using different mobility models shows that AODV-UI has a better performance when using RWP mobility model. Overall the AODV-UI is more suitable when using RWP mobility model. In the second part, we propose a new secure AODV protocol called Trust AODV using trust mechanism. Communications packets are only sent to the trusted neighbor nodes. Trust calculation is based on the behaviors and activity information of each node. It is divided in to Trust Global and Trust Local. Trust global (TG) is a trust calculation based on the total of received routing packets and the total of sending routing packets. Trust local (TL) is a comparison between total received packets and total forwarded packets by neighbor node from specific nodes. Nodes conclude the total trust level of its neighbors by accumulating the TL and TG values. When a node is suspected as an attacker, the security mechanism will isolate it from the network before communication is established.

The performance of Trust AODV is evaluated under DOS/DDOS attack and blackhole attack using network simulator NS-2. It compares with the similar type of secure AODV protocol, in this case TCLS protocol. Performance parameters are packet delivery rate, end to end delay and routing overhead. Simulation results show that the Trust AODV has a better performance than TCLS protocol in term of end to end delay, packet delivery rate and overhead. When the speed is varied, the average end-to-end delay value decreases 44.37%, the average packet delivery rate increase 29.65% and the average routing overhead decrease 64.2%. When the number of attack is varied, the average end-to-end delay value decreases 70.1%, the average packet delivery rate increase 30.5% and the average routing overhead decrease 82.7%.

In the last part of this thesis, we improve the performance of Trust AODV using ant algorithm. The protocol called Trust AODV+Ant. The implementation of ant algorithm in the proposed secure protocol is by adding ant agent to put the positive pheromone in the node if the node is trusted. Ant agent is represented as a routing packet. The pheromone value is saved in the routing table of the node. We modified the original routing table by adding the pheromone value field. The path communication is selected based on the pheromone concentrations and the shortest path. To control the number of packet agents in the network, we use Controlled Neighbor Broadcast (CNB) mechanism that is adopted from SARA protocol. In this mechanism, only one node has the authority to rebroadcast the packet agents to its own neighborhood. Trust AODV+Ant is evaluated using NS-2 in term of performance. Our proposed protocol is compared with

SARA, AODV and trust AODV under DOS/DDOS attacks.

Simulation results show that the packet delivery rate and throughput of the Trust AODV increases when using ant algorithm. However, in term of end-to-end delay there is no significant improvement. The packet delivery rate increases 4.58%, and the throughput increases 4.81%. However the end-toend delay value decreases 1.08%.