ISSN: 2302 -2805

EVALUASI KINERJA CLUSTER-BASED KEY MANAGEMENT PADA MANET UNTUK KOMUNIKASI TAKTIS KAPAL PERANG

Dinar HS Wahyuni, Gamantyo Hendrantoro
Jurusan Teknik Elektro,Fakultas Teknik Industri, ITS Surabaya
Sukolilo, Surabaya, Jawa Timur
email : sadriyantien@yahoo.com

Abstrak

The role of communication networsk in millitary operation continues to grow in importance, with mission areas such as covert special operations, time critical, targeting, command and control all relying heavily on networks and network application. Mobile Ad Hoc Network (MANET), which is self-organizing, infrastructureless, multihop networks, is especially suitable for communication in millitary. The wireless and distributed nature of MANET and very bad security environment in battlefield bring a great challenge to securing tactical MANET. MANET is requires less or no fixed infrastructure support communication among nodes that can be quickly and adaptively constructed. Indeed, a fully realized MANET would be powerful in enabling highly mobile, highly responsive, and quickly deployable tactical forces. Security is one of the major issues in MANET. Due to the inherent nature of MANET, a security key management procces is always required. Key management plays an important role in the security of today's information especially in MANET in which key management has received more and more attention for the dificulty to be implemented in such dynamic network. Desirable features of MANET for key management becomes our evaluation parameters. In this paper we compare the evaluation parameters among the existing methods using NS2 (Network Simulator 2).

Kata kunci :
Security, Key Management. Cluster-Based

1. Pendahuluan

Ketangguhan komunikasi taktis sangat dibutuhkan dalam dunia militer. Masalah yang sering sekali muncul adalah topologi medan pertempuran yang ekstrim disertai dengan mobilitas yang tinggi. Kondisi alam yang sangat tidak menentu menuntut sebuah sistem komunikasi yang mudah beradaptasi. MANET (Mobile Ad Hoc Network) adalah sebuah sistem komunikasi yang tidak mempunyai infrastruktur, *self-organizing* dan sangat mudah beradaptasi. MANET adalah sebuah jarigan yang terhubung dengan wireless. Karakteristik MANET ini sesuai dengan kebutuhan komunikasi taktis. Jaringan ini beroperasi dan mengatur diri sendiri tanpa adanya sentralisasi sehingga sering disebut jaringan yang mandiri dan mempunyai kemampuan kooperatif antar *node*. Hal ini yang membuat MANET tidak membutuh infrastruktur sesuai dengan sifat alaminya [1].

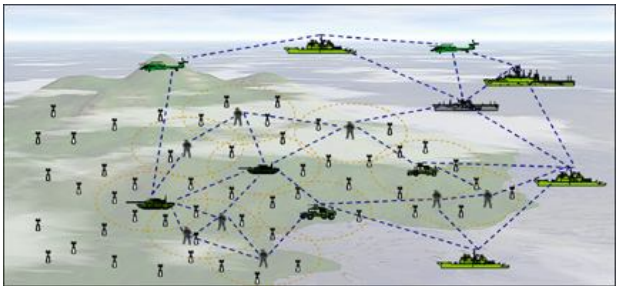
Karakterisktik MANET membawa pada permasalahan baru yaitu keamanan informasi yang sangat penting pada komunikasi taktis. Terdapat beberapa jenis serangan pada sistem MANET dari yang paling sederhana sampai yang paling rumit. Misalnya, penyerang dengan tidak meneruskan pesan ke *node* lainnya, menghapus data yang diterimanya dan mengirimkan informasi routing palsu. Manajemen Kunci mempunyai peranan yang sangat penting pada keamanan informasi jaringan MANET.

Manajemen kunci dapat didefinisikan sebagai sebuah teknik dan prosedur yang berfungsi untuk sarana dan mendukung kelangsungan kelacaran pada sistem ini [2]. Manajemen kunci pada MANET harus sesuai dengan topologi yang dinamik yaitu kemampuan untuk mengatur diri sendiri dan sistem organisasi yang tidak terpusat [2]. Beberapa fitur yang diingikan dalam manajemen kunci adalah *availability, robustness, efficiency, scalability, survivability dan resistance to known key attacks* yang juga akan menjadi indikator perbandingan pada penelitian ini [2].

Seiring perkembangan teknologi manajemen kunci pada manet, banyak peneliti yang membahas dan berusaha menemukan solusi terbaik. Beberapa skema sudah diterapkan pada penelitian sebelumnya adalah *Partially Distributed Certificate Athority, Fully Distributed Certificate Athority, Isdentity-Based Key Manangement, Certificate Chainning Based Key Management, Cluster-Based Key Management, Mobility-Based Key Management* dan *Parallel Key Management.* Skema yang akan dibahas pada makalah ini adalah Cluster-Based Key Management.

Cluster-Based Key Management menerapkan model simulasi menggunakan *node* yang dibedakan berdasarkan *cluster*. Setiap *cluster* mempunyai *cluster head* dan *recommended node* yang telah ditentukan juga.

ISSN: 2302 -2805



Gambar 1. Sistem Komunikasi Taktis

Cluster head bertugas untuk menyampaikan informasi kepada beberapa *recommended node* pada *cluster* yang sama.

Penelitian ini bertujuan untuk membuktikan dan mengimplementasikan simulasi skema manajemen kunci kemanan *Cluster-Based Key Management* sesuai dengan indikator perbandingan *robustness*, *efficiency*, *scalability survivability*, *availability* dan *resistant to known key attacks* yang paling sesuai digunakan dalam MANET pada komunikasi kapal perang [3].

2. Tinjauan Pustaka

A. MANET (Mobile Ad Hoc Network)

Komunikasi dengan secara ad hoc umumnya disebut sebagai Mobile Ad Hoc Network (MANET). Mobile ad hoc Network (MANET) yaitu sebuah jaringan wireless yang terdiri dari 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. Setiap mobile node memiliki wireless network interface dan saling berkomunikasi dengan memanfaatkan media transmisi. Karena media transmisi mempunyai daya pancar yang terbatas, maka komunikasi antar node tersebut dilakukan dengan melewati satu dari beberapa node lainnya (node berfungsi sebagai router atau host) sehingga MANET juga bisa disebut multi-hop network [2].

Pada jaringan MANET setiap mobile node dalam jaringan memiliki kedudukan yang sama dan tidak ada administrator pusat seperti pada jaringan celluler atau pada jaringan wireless local area network (WLAN) mode infrastruktur. Setiap node dibatasi oleh cakupan daerah komunikasi tergantung dari kartu jaringan masing-masing. Sehingga perlu adanya beberapa node lain untuk dapat saling menghubungkan. Beberapa karakteristik jaringan MANET diantaranya adalah topologi yang dinamis yang diakibatkan karena seringnya perubahan posisi node. Selain itu jaringan ini juga memiliki keterbatasan storage, keterbatasan bandwidth, keterbatasan power baterai dalam pentransmisian data, dan juga keterbatasan resource CPU dan memori. Jaringan MANET dapat dibangun pada tempat yang tidak terdapat infrastruktur jaringan sebelumnya.

Node yang selalu bergerak membuat topologi jaringan yang dinamis. Komunikasi pada topologi dinamis tidak semudah komunikasi pada topologi statis. Selain itu kecepatan data (bitrate) pada kanal VHF hanya 1200 bps. Oleh karena itu kanal harus digunakan se-efektif mungkin .

Pada dasarnya jaringan ad hoc membutuhkan protokol untuk route discovery dan route maintenance. Saat dua node tidak dapat berkomunikasi secara langsung, protokol routing memegang peranan penting. Pada sistem komunikasi laut, protokol routing ad hoc harus disesuaikan dengan karakterisitik laut. Ada banyak hal yang harus diperhatikan dalam komunikasi ad hoc di laut diantaranya adalah kecepatan kapal laut (node), ketersediaan trafik pada kanal yang dipakai dan kondisi geografis laut.

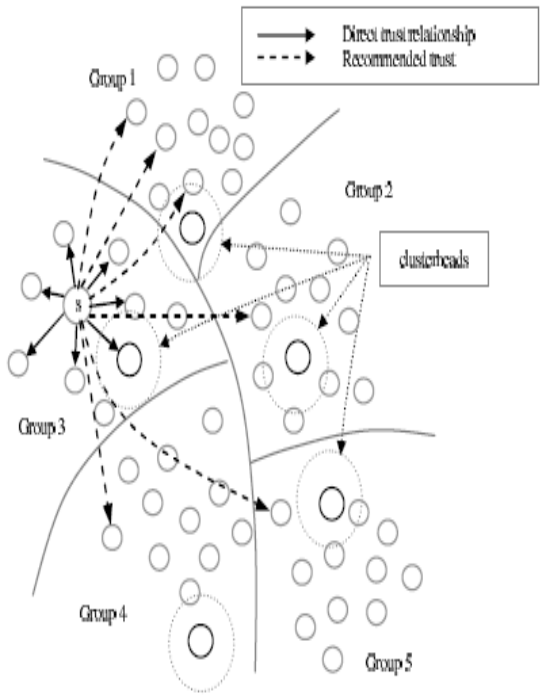
B. Key Management

Key management adalah faktor utama pada keamanan MANET. Key management sangat penting untuk menyediakan keamanan komunikasi pada jaringan yang besar maupun dengan topologi yang selalu berubah. Dalam Key Management terdapat beberapa skema yang digunakan yaitu Partially Distributed Certificate Authority, Fully Distributed Certificate Authority, Identity-Based Key Management, Certificate Chainning Based Key Management, Cluster-Based Key Management, Mobility-Based Key Managemenr\t, Parallel Key Management. Setiap skema mempunyai keunggulan masing-masing. Pada penelitian dipilih skema Cluster-Based Key Management karena sesuai untuk sistem komunikasi taktis kapal perang [6].

C. Cluster-Based Key Management [5]

Setiap node pada skema ini bertanggung jawab untuk membuat dan memperbarui public key maupun private key oleh dirinya sendiri. Setiap node dapat mengenali public key dari node lain pada klompok yang sama. Node dapat berasumsi untuk melakukan pengawasan terhadap setiap karakterisik node lain. Node yang menadi acuan adalah node yang dapat memberitahukan node mana saja yang dapat dapat memberika public key yang benar. Kepercayaan antar node dalam satu cluster berdasarkan direct trust. Sedangkan hubungan kepercayaan antar node dalam cluster yang berbeda berdasarkan recommended trust. Setiap node harus mempunyai tabl hubungan kepercayaan yang dikirimkan kepada node lain. Bentuk dari hubungan kepercayaan ini ditunjukkan dalam gambar di bawah ini.

ISSN: 2302 -2805



Gambar 2. Cluster Based Key Management

Pada MANET akan terjadi kalkulasi rute apabila terjadi perubahan lokasi maupun luasan daerah jangkuan. Dengan adanya skema berdasarkan cluster ini pesan pada jaringan lokal dapat di transmisikan pada jarak terdekat dalam cluster yang sama, sedangkan pengiriman pesan untuk jarak yang jauh dilakukan pada cluster yang berbeda. Setiap cluster ditandai dengan adanya cluster head yang menunjukkan wilayah sebuah cluster.

Sebuah clusterhead bertugas untuk kalkulasi rute dalam cluster dan pengiriman pesan long-distance. Pengriman pesan long-distance mengharuskan clusterhead menggunakan tenaga lebih untuk transmisi.

Kondisi komunikasi dalam MANET yang dinamik merupakan masalah dalam skema cluster. Konsentrasi utama dalam skema ini adalah pemilihan, konfigurasi dan peletakan clusterhead. Setiap node harus mampu untuk menjadi clusterhead dalam sebuah jaringan. Node yang menjadi clusterhead tidak berbeda dengan node lainnya dalam jaringan tersebut dan mempunyai karakteristik yang hamper sama. Dengan adanya kegagalan konektivitas maka dari itu dibutuhkan pembagian wilayah. Adanya perubahan yang berkala pada clusterhead maupun anggota cluster menyebabkan perhitungan dan komunikasi yang rumit.

Tugas dari clusterhead sangat sulit karena tidak semua node bias menjadi clusterhead. Node yang terpilih adalah node yang mempunyai kemampuan untuk mengendali cluster secara keseluruhan. Pendekatan mengunakan skema ini mempunya tingkat efektif yang lebih tinggi.

D. Cluster Based Routing Protocol (CBRP)

Cluster Based Routing protokol adalah routing yang berfungsi untuk menangani packet loss dan efisiensi penggunaan energy. Pada protokol ini setiap node bisa menjadi cluster head. Node yang menjadi cluster head adalah node yang mempunyai kemampuan tertinggi dari node lainnya. Node ini harus menjalankan tugas sebagai cluster head dalam jaringan untuk proses pengiriman pesan. Ketika node tidak menerima request message dari cluster head maka node akan mengirimkan pesan ke cluster head lain untuk menghindari pesan yang hilang. Node ini akan mengirimkan registration message ke cluster head baru terdekat lainnya.

Ketika cluster head baru telah menerima pesan data dari semua node maka akan dilakukan pemeriksaan ulang. Pemeriksaan ini untuk untuk mendata kembali node-node yang mengirimkan pesan balik. Cluster head akan membuang node yang tidak mengirim pesan kembali ke cluster head. Jika ada Node baru yang akan bergabung, node harus mengirim pesan pemberitahuan untuk bergabung dalam cluster. Cluster head akan menambahkan node baru ini ke dalam daftar rute pengiriman pesan.

3. Metode Penelitian

Simulasi pada penelitian ini menggunakan NS2 (Network Simulator 2). Simulasi ini dijalankan pada system operasi Linux. Tujuan simulasi ini untuk mengetahui kemampuan kerja MANET pada skema Cluster Based Key Management. Karakteristik node dan topologi yang digunakan pada simulasi ini sesuai dengan Tabel 1. Hasil simulasi berupa animasi ditunjukkan pada Gambar 4.

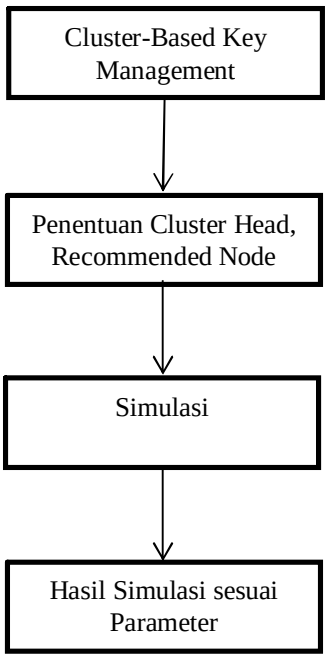
Pada Gambar 3 dijelaskan metoe peracnangan simulasi. Setelah memilih skema cluster based key management kita tentukan cluster head tiap cluster. Selain cluster head tentukan juga koordinat node lain yang merupakan bagian dari cluster. Kita buat beberapa node yang bergerak menjauh maupun mendekati tiap cluster. Perubahan topologi yang akan kita lihat hasilnya.

Node yang berfungsi sebagai clusterhead adalah node 0, 1 dan 10. Dalam simulasi ini menggunakan routing AODV. Untuk simulasi cluster based key management ini lebih baik jika menggunakan routing CBR (Cluster Based Routing). CBR dapat secara otomatis mengatur routing untuk jenis cluster.

Tabel 1. Karakteristik Node

Parameter	Nilai
Kecepatan *Node*/Kapal Perang	Bervariasi
Frekuensi	VHF
Antena	Omni Directional
Model Propagasi	TwoRay

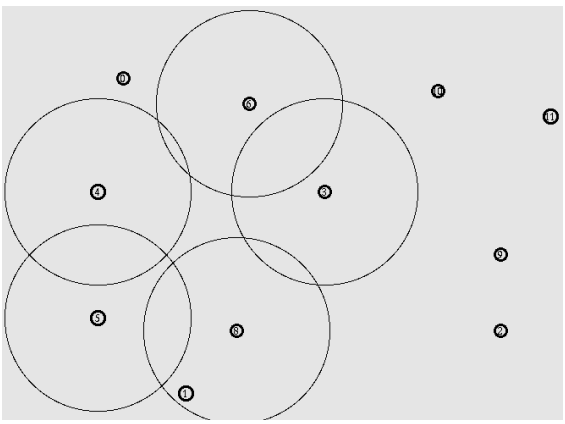
Jumlah *node*	11 *node*
Jangkauan / radius	<250 m
Routing	AODV



Gambar 3. Skema simulasi Cluster-Based Key Management

Pada rancangan model ini akan dibuat 11 node yang akan digunakan dalam pembuatan scenario tiap skema. Node-node ini akan dibuat sedemikian hingga sesuai dengan sifat setiap skema yang akan disimulasikan dalam Network Simulator 2

Setiap node yang dibuat akan ditentukan posisi dan fungsinya masing-masing sesuai kebutuhan. Penentuan ini disesuaikan dengan algoritma yang dimiliki setiap skema yang akan diteliti.



Gambar. 4. Hasil simulasi menggunakan NS2

4. Hasil dan Pembahasan

Hasil keluaran dari simulastor NS2 adalah Network Animator (NAM) dan Trace graph. NAM ditunjukkan pada Gambar 4. Perubahan topologi dan perpindahan node dapat menunjukkan kinerja skema ini. Lingkaran berwarna hitam menunjukkan perubahan routing pengiriman data yang harus berubah sesuai dengan perubahan topologi.

Keluaran dalam bentuk trace menunjukkan setiap proses perubahan gerakan maupun routing. Pada penelitian ini masi terkendala dalam pembaccan trace untuk mempermudah mengetahui grafik dan kinerja dari simulasi yang dilakukan. Usaha dalam pembacaan trace masi dilakukan sampai saat ini. Dari pembacaan trace sceara manual diperoleh hasil yaitu menggunakan metode cluster-based key management dapat meningkatkan keamanan jaringan dari serangan yang ditunjukkan dengan kceepatan jaringan dalam menerima perubahan topologi.

5. Kesimpulan dan Saran

Pendekatan mengunakan skema ini mempunya tingkat efektif yang lebih tinggi. Sistem keamanan yang terbangun dalam skema ini dapat menjamin kelangsungan pertukaran informasi dalam sistem komunikasi taktis kapal perang.

Daftar Pustaka

[1] E. C. H. Ngai, M. R. Lyu, and R. T. Chin, "An Authentication Service Against Dishonest Users in Mobile Ad Hoc Networks," in proc. IEEE Aerospace Conf., March, 6-13 2004.

[2] Wieland, A., Wallenburg, C.M., 2012. Dealing with supply chain risks: Linking risk management practices and strategies to performance. International Journal of Physical Distribution & Logistics Management, 42(10)

[2] C.-K. Toh, 2001, Ad *Hoc Mobile Wireless Networks:Protocols and Systems*. Prentice Hall PTR

[3] J. Sharony, June 1996, "*A Mobile Radio Network Architecture with Dynamically Changing Topo- logy using Virtual Subnets*," in proc. IEEE International Conf. o Communications (ICC/SUPERCOMM'96)

[4] L. Zhou and Z. J. Haas, 1999, "*Securing Ad Hoc Networks*," IEEE Network: special issue on network security, vol. 13, no. 6, pp. 24–30

[5] S. Capkun, L. Buttyan, and J.-P. Hubaux, 2003, "*Self-Organized Public-Key Management for Mobile Ad Hoc Networks*," IEEE Transactions on Mobile Computing, vol. 2, no. 1, pp. 52–64

[6] S. Yi and R. Kravets, 2004, "*Composite Key Management for Ad Hoc Networks*," in proc. First Annual International Conf. on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous'04), August, 22 - 26

[7] F. Richard Y., H. Tang, F. Wang,"A Hierarchical Identity Based Key Management Scheme in Tactical Mobile Ad Hoc Networks," IEEE Transaction On Network And Service Management, Vol. 7, NO. 4, December 2010

ISSN: 2302 -2805

Biodata Penulis

Dinar Hana Sadriyantien Wahyuni, memperoleh gelar Sarjana Teknik (ST), Jurusan Teknik, Fakultas Teknik Universitas Brawijaya Malang, lulus tahun 2010. Saat ini sedang menempuh program Magister Teknik program studi Telekomunikasi dan Multimedia di ITS Surabaya.

ISSN: 2302 -2805