*Jurnal Sosial dan Teknologi (SOSTECH)*
Volume 1, Number 8, August 2021
p-ISSN **2774-5147** ; e-ISSN **2774-5155**

# ANALISIS ANCAMAN DAN SOLUSI KEAMANAN PADA *MOBILE AD-HOC NETWORK* (MANET): SEBUAH KAJIAN LITERATUR

**Haris Muhammad[1] dan Niken Febrina Ernungtyas[2]**
Universitas Indonesia[1 dan 2]
haris.muhammad01@ui.ac.id[1] dan niken.febrina@ui.ac.id[2]

Diterima:
**27 Juni 2021**
Direvisi:
**12 Juli 2021**
Disetujui:
**14 Agustus 2021**

**Abstrak**

*Mobile Ad Hoc Network* (Manet) adalah kumpulan dari dua atau lebih perangkat/*node* dengan komunikasi nirkabel dan kemampuan *network* yang berkomunikasi satu sama lain tanpa bantuan administrator terpusat. Penelitian ini bertujuan untuk mengetahui ancaman apa saja yang dapat terjadi pada *Mobile Ad-Hoc Network* (Manet) dan untuk mengetahui solusi keamanan yang tepat dan dapat diterapkan pada *Mobile Ad-Hoc Network* (Manet). Metode penelitian ini, peneliti menggunakan studi literatur dibandingkan dengan *network* yang bergantung pada infrastruktur kabel, *Mobile Ad Hoc Network* (Manet) lebih rentan terhadap serangan karena topologinya yang dinamis dan tidak adanya administrasi *network* terpusat. Manet menghadapi lebih banyak ancaman keamanan daripada *network* terpusat. Tinjauan literatur awal tentang masalah keamanan Manet menunjukkan bahwa meskipun ada upaya penelitian untuk mengidentifikasi ancaman keamanan dan solusi pada Manet, tinjauan komprehensifnya sedikit atau kurang. Berdasarkan upaya untuk mengatasi kekurangan itu, studi ini menawarkan literatur terkini tentang masalah keamanan dan solusi di Manet. Berdasarkan hasil telaah tinjauan pada penelitian-penelitan terdahulu tentang topik Manet, artikel jurnal ini dapat menawarkan penyajian yang komprehensif tentang masalah keamanan di Manet.

**Kata kunci** : **Mobile Ad Hoc *Network* (Manet), Ancaman, Keamanan, Solusi**

***Abstract***

*The Mobile Ad Hoc Network (Manet) is a collection of two or more devices/nodes with wireless communication and network capabilities that communicate with each other without the help of a centralized administrator. This study aims to find out what threats can occur to the Mobile Ad-Hoc Network (Manet) and to find out the right security solutions that can be applied to the Mobile Ad-Hoc Network (Manet). In this research method, researchers used literature studies compared to networks that rely on cable infrastructure, Mobile Ad Hoc Network (Manet) is more vulnerable to attacks due to its dynamic topology and the absence of centralized network administration. Manet faces more security threats than centralized networks. An initial literature review of Manets security concerns shows that despite research efforts to identify security threats and solutions to Manet, its comprehensive review is little or less. Based on efforts to address these shortcomings, this study offers the latest literature on security issues and solutions at Manet. By studying reviews of previous studies on the topic of Manet, this journal article can offer a comprehensive presentation of security issues at Manet.*

***Keywords :* *Mobile Ad Hoc Network (Manet), Threats, Security, Solutions***

**How to cite:** Haris Muhammad[1] dan Niken Febrina Ernungtyas[2]. (2021). Analisis Ancaman dan Solusi Keamanan pada *Mobile Ad-Hoc Network* (Manet): Sebuah Kajian Literatur. *Jurnal Sosial dan Teknologi (SOSTECH), 1*(8): 768-777
**E-ISSN:** 2774-5155
**Published by:** https://greenvest.co.id/

e-ISSN 2774-5155
p-ISSN 2774-5147

## PENDAHULUAN

Berdasarkan masyarakat saat ini, perangkat *mobile* (misalnya laptop dan ponsel) semakin terintegrasi ke dalam aktivitas sehari-hari (Handayaningsih & Nugroho, 2013). Hal ini membuat perangkat tersebut menjadi bagian integral (Mufid, 2018), tidak terpisahkan dari kehidupan dalam masyarakat kontemporer. Secara harfiah, perangkat seluler ditemukan hampir dimanapun tempat manusia berada (Bagenda & Ajianto, 2014). Menurut alasan ini, perangkat seluler diperlukan guna saling terhubung, menyampaikan pesan antara individu dan kelompok, sehingga memungkinkan komunikasi yang efektif (Derveloy, 2012).

Biasanya perangkat ini saling terhubung untuk memungkinkan respon terhadap tuntutan skema tertentu. Tuntutan khusus skema tersebut mencakup situasi darurat, misalnya operasi penyelamatan dan di zona pertempuran militer. "Dengan berbagai protokol perutean, keterbatasan sumber daya dan media komunikasi berbeda yang digunakan oleh *network* ini, keamanan biasanya tidak menjadi yang terdepan dalam desainnya". Memahami ancaman laten terhadap keamanan *ad hoc network* (Febriane & Mariamah, 2013), sangat penting untuk memahami arti dari istilah "*ad hoc*". "*Ad hoc*" adalah kata latin untuk "tujuan khusus". Seperti yang ditunjukkan oleh istilah, sifat inti dari tujuan *ad hoc network* adalah gagasan bahwa mereka dibentuk berdasarkan permintaan. Artinya, *ad hoc network* dibentuk untuk menanggapi skema dimana jaringan tradisional tidak tersedia (Hardiono & Harsasto, 2018), rusak atau tidak dapat diterapkan. Selain itu, kualitas utama dari *ad hoc network* adalah bahwa mereka dapat impulsif, tidak permanen, dibangun dengan tujuan, terdistribusi dan otonom.

Selain itu, *ad hoc network* secara khusus dirancang berdasarkan kebutuhan situasi (Hariyadi, 2016). Setiap skema membutuhkan *ad hoc network* yang disesuaikan secara unik. Diharapkan, *ad hoc network* mengikuti proses administrasi dan keamanan yang ditemukan di jaringan kabel konvensional (Alamsyah, 2012). Namun, sementara penyebaran diskret *ad hoc network* dapat berbeda secara signifikan (Azra, 2019), mereka memiliki karakteristik umum tertentu. Menurut (Derveloy, 2012), sifat-sifat tersebut termasuk kurangnya kontrol pusat, sumber daya terbatas (Hakim, 2013), mobilitas, topologi dinamis, konektivitas nirkabel dan protokol perutean khusus (Hamim, 2019). Tidak mengherankan, masing-masing karakteristik ini membawa masalah keamanan yang unik (Lucy et al., 2012). Contoh kasus desentralisasi dalam *ad hoc network* berarti tidak adanya administrasi terpusat (Nuradhawati, 2019) sehingga tidak memiliki titik dan mekanisme pengaturan keamanan yang terpadu. Akibatnya, jaringan nirkabel pada umumnya dan *mobile ad hoc network* pada khususnya rentan terhadap ancaman eksternal seperti gangguan sinyal. Selain itu, karena *mobile ad hoc network* mengalami sumber daya yang terbatas, mereka mungkin tidak mengakomodasi protokol perutean konvensional yang tidak disesuaikan. Kustomisasi terkadang dapat merusak efektivitas peringatan keamanan yang ada.

*Mobile Ad hoc Network* (Manet) terdiri dari *node* seluler yang dapat dikonfigurasi sendiri, terhubung melalui koneksi nirkabel (Rai et al., 2012). *Node* Manet yang berdekatan satu sama lain dapat mengirimkan informasi di antara mereka dan bergantung pada *node* langsung untuk meneruskan informasi ke *node* lain dalam *network*. Sebuah *mobile node* dapat berfungsi sebagai pengirim, penerima atau *router*. *Mobile Ad hoc Network* (Manet) dijelaskan oleh kemampuannya untuk *multi-hop*, mengkonfigurasi sendiri dan fluiditasnya saat *node* bergabung dan meninggalkan *network*. Manet terdiri dari klaster perangkat *mobile* yang terminalnya terhubung secara nirkabel. Terminal *mobile* berfungsi sebagai penerima dan pemancar informasi *router* dan *host*. Manet tidak

memerlukan infrastruktur, sementara pada saat yang sama menjadi sangat dinamis karena sifat Manet yang berbasis kebutuhan ini, mereka sangat dapat diterapkan di area atau situasi yang membutuhkan respon sesaat. *Node* di Manet tidak bergantung pada infrastruktur tetap, pendekatan untuk masalah keamanan mereka selalu berbeda dari rekan-rekan kabel mereka.

Tantangan keamanan yang disediakan oleh *node* di Manet sangat berbeda dari masalah keamanan yang dihadapi *node* yang bergantung pada infrastruktur. Selain itu, karena Manet bersifat *case-specific*, dirancang untuk menanggapi tuntutan skema unik tertentu, solusi untuk keamanannya berbeda dari jaringan yang bergantung pada infrastruktur. Hal ini dikarenakan otonomi *node* untuk bergabung atau meninggalkan jaringan, solusi keamanan jaringan tradisional mungkin tidak dapat diterapkan. Oleh sebab itu, adalah bijaksana untuk menggunakan respons keamanan berbasis konsep saat menggunakan Manet. Transmisi nirkabel paket data di Manet memaparkan sinyal kemungkinan intrusi dari penyerang berbahaya. Tidak seperti di jaringan kabel, lebih mudah untuk memanfaatkan sinyal Manet. Propagasi nirkabel paket data memperkenalkan kerentanan dalam jaringan karena umumnya pelindung data dan keamanannya relatif buruk. Akibatnya sangat sering Manet rentan terhadap sinyal interferensi, kemacetan, menguping dan distorsi.

Oleh karena itu, protokol perutean di Manet, dalam banyak kasus, dirancang untuk menangani kerentanan seperti itu. Mobilitas *node* yang tinggi dalam Manet mempersulit upaya keamanan dibandingkan dengan jaringan kabel. Jika memanfaatkan celah keamanan yang dibuat oleh *node* yang bergerak, peretas dapat membobol seluruh *network* atau membuat serangan parsial karena begitu banyak karakteristik Manet yang mobilitas tinggi, dinamis dan otonomi, ada banyak masalah dan ancaman keamanan yang memerlukan perhatian. *Mobile ad hoc network* menggunakan *node* mereka sebagai *router*/pemancar dan penerima karena status *node* tujuan ganda ini, setiap perangkat *mobile* dalam jaringan sangat penting untuk keamanan transmisi data. Akibatnya, *node* yang dikonvensikan dapat menular ke perangkat lainnya. Saat merancang *mobile ad hoc network*, penting untuk selalu mempertimbangkan ketergantungan timbal balik antara *node* tetangga. Hal ini terjadi karena semua *node* dalam *ad hoc network* memelihara informasi topologi dari *node* tetangga. Infeksi atau serangan pada satu *node* dapat menyebar dengan cepat jika tidak ditangani dengan baik. Konektivitas pada Manet, biasanya terjadi pada protokol *link-layer* dan protokol *network-layer*. Koneksi *single-hop* terjadi pada protokol *link-layer*, sedangkan koneksi *multiple-hop* terjadi pada *network-layer*. Akibatnya, untuk mencapai keamanan maksimum dalam transmisi paket data, sangat penting untuk menerapkan langkah-langkah keamanan di kedua lapisan *link-layer dan network-layer*. Pada instalasi keamanan *link-layer*, konektivitas satu *hop* di antara dua *node* ujung ke ujung yang berada dalam jangkauan komunikasi satu sama lain melalui protokol aman, seperti protokol IEEE 802.11 WEP atau tambahan 802.11i/. Protokol WPA dilindungi. Propagasi *multi-hop* yang aman dan pengiriman paket data dijalankan oleh lapisan *network*.

Lapisan *network* menjamin transmisi sinyal data yang efektif dan handal sesuai dengan ketentuan keamanan yang tertanam dalam protokol perutean. Oleh karena itu, masalah keamanan ditentukan oleh titik serangan mereka. Artinya, masalah keamanan di Manet dapat diberi label sebagai pertanyaan protokol perutean atau ancaman jaringan umum. Tautan *node* nirkabel di *mobile ad hoc network* tidak dapat diandalkan untuk konektivitas yang aman dan stabil. Saat *node* keluar dan bergabung dengan *network*, informasi topologi berubah. Perubahan informasi topologi dalam tabel *node* dapat memanfaatkan titik lemah untuk serangan oleh penyusup jahat. Selain itu, tidak dapat diandalkannya *mobile node ad hoc* dapat dihasilkan dari pasokan energi yang tidak

e-ISSN 2774-5155
p-ISSN 2774-5147

memadai ke perangkat. Oleh karena itu, pasokan daya yang terbatas ke perangkat dan pergerakan *node* yang konsisten di sekitar *network*, secara negatif memengaruhi keamanan dan komunikasi secara keseluruhan.

Beberapa kasus, *mobile ad hoc node* memiliki integrasi yang tidak memadai dan implementasi struktur keamanan. Serangan dan ancaman Manet dapat berasal dari luar maupun dari dalam. Serangan internal adalah ancaman keamanan yang berasal dari pengguna dan *node*/perangkat dalam *network*. Keakraban dengan *network* sangat berguna dalam perumusan serangan internal. Pengguna *network* terkadang memiliki informasi penting yang diperlukan dalam gangguan pesan, penghapusan catatan atau bahkan penolakan layanan *network*. Biasanya, serangan internal diarahkan ke tautan *network* dan antarmuka keamanan. Serangan eksternal, di sisi lain, melibatkan ancaman eksekusi dari luar *network*. Serangan ini dibagi menjadi dua, yaitu serangan aktif dan pasif. Kedua hal ini bisa menjadi relatif, serangan aktif biasanya menyebabkan lebih banyak kerusakan daripada serangan pasif. Tujuan penelitian ini untuk mengetahui ancaman apa saja yang dapat terjadi pada *mobile ad-hoc network* (Manet), untuk mengetahui solusi keamanan yang tepat dan dapat diterapkan pada *mobile ad-hoc network* (Manet). Manfaat penelitian ini yaitu untuk menambah data dan informasi yang ditunjukkan kepada peneliti lain yang ingin mengembangkan serta memperbaiki sistem jaringan Manet terhadap serangan keamanan, memberikan informasi tentang ancaman-ancaman pada Manet dan solusi apa yang tepat untuk mengatasinya dan mengetahui kinerja Manet apabila terkena serangan ancaman keamanan.

## METODE PENELITIAN

Menurut upaya untuk menghasilkan literatur terbaru tentang ancaman, masalah dan solusi keamanan Manet, mesin pencari *Google* digunakan untuk mengakses artikel dari berbagai situs *web* dan jurnal. Pertama, artikel penelitian yang dihasilkan oleh pencarian umum di *Google* ditinjau berdasarkan istilah kunci seperti *mobile ad hoc*, Manet, keamanan, ancaman dan solusi. Selain itu, artikel penelitian selanjutnya dipilih berdasarkan penampilannya di situs *web* seperti *Remote Lib UI*, *ResearchGate*, *Mendeley* atau *Google Scholar*.

Representasi studi yang seimbang dipastikan dengan menggunakan kriteria berikut:

1. Setiap ancaman keamanan diambil dari satu studi
2. Setiap solusi untuk ancaman keamanan Manet dipilih dari satu studi
3. Protokol perutean dan karakteristik Manet dipilih secara acak dari berbagai penelitian.

Artikel jurnal ini dibagi menjadi lima bagian, yaitu pendahuluan, metode penelitian, hasil dan pembahasan (terdiri dari penelitian terdahulu, jenis ancaman keamanan pada Manet, solusi untuk ancaman keamanan Manet, aspek keamanan pada manet) dan terakhir kesimpulan yang di dalamnya disertakan rekomendasi penelitian lebih lanjut.

## HASIL DAN PEMBAHASAN

Sejumlah penelitian telah dilakukan tentang tantangan dan solusi keamanan di *Mobile Ad Hoc Network* (Manet). Serangan peretas terhadap Manet dapat terjadi dalam dua cara utama, yakni secara pasif maupun aktif. Menurut serangan pasif, data yang ditransmisikan tidak terpengaruh. Sebaliknya, serangan pasif berpura-pura menjadi bagian dari data, tetapi dengan satu-satunya motif mengumpulkan informasi penting

(Kaur, 2016) serangan pasif dapat dilihat sebagai menanam mata-mata jahat dalam sekelompok orang baik dengan tujuan mencuri informasi. Tidak ada gangguan perutean saat serangan pasif terjadi. Namun, dalam serangan aktif, transmisi data terputus. Dibandingkan dengan serangan pasif, serangan aktif lebih parah karena transmisi normal data antar *node* terpengaruh secara negatif, tulis (Kaur, 2016). Salah satu dari jenis serangan dapat berasal dari dalam atau luar karena Manet bergantung pada *node* untuk reorganisasi diri, sistem *network* mereka lebih rentan terhadap serangan daripada *network* kabel. Untuk alasan ini, mengamankan Manet bisa menjadi tugas yang menakutkan. Tetapi ada tujuan keamanan yang harus dicapai Manet untuk menjamin keamanan bagi pengguna. Kerahasiaan harus selalu diperhatikan. Hanya perangkat dan pengguna yang berwenang yang diizinkan mengakses *network* untuk melindungi privasi dan kerahasiaan (Yadav & Uparosiya, 2014). Setiap *node* membutuhkan kemampuan untuk memvalidasi kecerdikan *node* peer dan pengguna. Pengguna dan *node network* yang valid memerlukan kredensial validasi untuk mengakses *network*. Otentikasi mencegah peniru mengakses *network* secara tidak sah.

Penyebaran kriptografi tepi untuk menjamin keamanan dan keselamatan *network*. Prosedur untuk mengaktifkan *node* individu dalam *network* untuk mengotentikasi keamanan *node* sesama sehingga mengeluarkan sertifikat keamanan. Protokol perutean Manet yang mendasarkan keamanannya pada berbagi informasi secara diam-diam di bawah transmisi dalam *network* dan kemungkinan melindungi ancaman keamanan menawarkan model umum untuk mengamankan transmisi data dan konektivitas di Manet.

Kemungkinan respon terhadap ancaman yang ditimbulkan oleh serangan lubang hitam. Protokol perutean Manet yang aman dan itu dijuluki ARAN. Protokol ini menggunakan sertifikasi *node* untuk menjamin keamanan dalam *network*. Sertifikasi, memiliki potensi untuk membanjiri setiap ancaman keamanan yang diarahkan ke *network* Manet. Presentasi dan diskusi yang komprehensif tentang masalah keamanan dan ancaman yang memengaruhi *multi hopping* di Manet. Menurut studi itu, isu-isu yang berkaitan dengan desain keamanan dan status keamanan kontemporer dalam transmisi paket data disorot. Oleh karena kerentanannya, para peneliti telah mengembangkan banyak cara untuk memerangi ketidakamanan di Manet. Misalnya, deteksi intrusi adalah skema respons untuk mendeteksi ancaman sebelumnya. Deteksi intrusi mengajukan model terdistribusi dan kooperatif, yang dirancang untuk merasakan dan mengidentifikasi serangan.

Deteksi intrusi semua *node* dalam *network* dipanggil untuk bertindak. Setelah sebuah *node* mengidentifikasi ancaman secara independen, ia menyiarkan peringatan ke seluruh *node* lainnya. Tetapi kadang-kadang, sebagai akibat dari keterbatasan daya *node*, penyebaran peringatan mungkin tidak berhasil. Insiden tersebut memerlukan deteksi instrusi berbasis *cluster*. Deteksi Intrusi Berbasis *cluster* dirancang sedemikian rupa sehingga *network* dibagi menjadi sub kelompok (*cluster*). *Cluster* memungkinkan *node* anggota untuk menyebarkan peringatan serangan ke *node* pendamping. Peran deteksi intruksi ditugaskan ke satu *node* yang berfungsi sebagai penjaga untuk yang lain. Setiap kali serangan terdeteksi, *node* yang bertanggung jawab diharapkan untuk memperingatkan *node* lainnya dalam *cluster*. Semua *node* yang ditugaskan ke sebuah *cluster* dilayani oleh satu jangkauan radio, termasuk beberapa serangan Manet lainnya seperti *Wormhole*. Tali paket adalah respon serangan terhadap *Wormhole*. *Wormhole* ini memotong informasi yang sedang ditransmisikan dengan berpura-pura menjadi penerima asli. Informasi yang dicegat disalurkan ke penyerang *wormhole* lainnya. Informasi yang dicegat dirusak oleh *wormhole* dan dikirim kembali ke penerima asli. Meskipun pesan disamarkan sebagai valid, ia membawa skrip tersembunyi yang dirancang untuk mencuri informasi atau menonaktifkan jalur transmisi. Respon terhadap serangan *wormhole*

e-ISSN 2774-5155
p-ISSN 2774-5147

termasuk menambahkan informasi tambahan ke paket untuk mengatur jarak maksimum transmisi, ini disebut paket *leashing*. Paket *leashing* dapat terikat secara geografis atau terikat temporal. Paket *leashing* yang terikat secara geografis menggunakan jarak untuk mengatur transmisi paket, sementara paket *leashing* terikat temporal menyebarkan waktu maksimum transmisi paket.

**A. Jenis Ancaman Keamanan pada Manet**

Oleh karena koneksi Manet dan *transfer* paket data bergantung pada kelompok *node* atau perangkat *mobile* yang terbentuk, dalam banyak kasus, *network* sementara yang berumur pendek, kebutuhan akan administrasi pusat dihilangkan. Untuk alasan ini, kurangnya administrasi pusat, interkoneksi *mobile node* harus didasarkan pada kepercayaan mutlak. Selain itu, karena sifat dinamis dari Manet dan perubahan informasi topologi yang cepat, secara komparatif, mereka rentan terhadap serangan internal. Serangan di Manet dapat dikategorikan berdasarkan lapisan *network*. *Flooding* adalah serangan di Manet yang mengganggu fungsi normal *network* dengan membajak sumber dayanya. Misalnya *node* jahat yang dirancang untuk menyerang dapat menggunakan *bandwidth* dan daya secara berlebihan untuk mengganggu dan menimbulkan gangguan dalam kinerja *network*. Serangan lubang hitam terjadi ketika *node* jahat mendistribusikan sinyal yang salah ke seluruh *node network*. Pesan sinyal seperti itu dapat menunjukkan kepada *node* lainnya bahwa *node* yang terinfeksi adalah yang terbaik dari rute yang tersedia di sekitar *network*. *Link Spoofing* adalah serangan lapisan *network* yang terjadi ketika *node* jahat menyiarkan informasi link palsu ke *node* lainnya karena pesan tautan palsu yang dikirimkan salah, seluruh operasi *network* terganggu (Gagandeep & Kumar, 2012). Serangan *Network Partitioning* membagi *network* menjadi *sub-network* untuk memperkenalkan heterogenitas yang tidak perlu dalam paket data dan transmisi informasi topologi. Heterogenitas yang tidak perlu dalam *network* Manetmemastikan tidak adanya *rute* yang dapat diandalkan, sehingga menonaktifkan transmisi yang efektif dalam *network*.

Serangan lapisan *network* lainnya di Manet termasuk keegoisan. Menurut serangan ini, *node* yang terinfeksi bertindak jahat dan tidak kooperatif karena *node* Manet seharusnya bertindak baik sebagai *router*/*receiver* dan *transmitter*, *node* yang egois dapat memutuskan untuk tidak menjalankan salah satu dari peran tersebut. Apabila mengasumsikan dormansi, sebuah *node* dengan demikian memperkenalkan kerusakan tautan dalam *network*. Berdasarkan serangan *Sleep Deprivation*, sebuah *node* dalam *network* Manet dipaksa untuk menggunakan catu dayanya secara berlebihan. Penggunaan catu daya yang berlebihan, seperti baterai menghasilkan korsletingnya kegunaan *node* secara keseluruhan dan terkadang mengurangi masa pakai. *Denial of Service* (DoS) terjadi ketika *node* yang terinfeksi memblokir penerimaan dan transmisi paket data dan informasi topologi *network* lainnya di antara *node* lainnya.

Serangan *gray hole* memperkenalkan *red herrings* dalam transmisi paket data. Serangan *gray hole* muncul ketika penyerang menyetujui *rute* berbahaya sebagai valid. Setelah mendukung *rute* yang tidak aman, data dialihkan ke penyerang, sehingga menimbulkan kesulitan dalam kerja umum *network*. Ketika penyerang menerima paket data, mereka segera dijatuhkan, rusak atau dihancurkan. Serangan *jelly fish* menciptakan ketidaknyamanan dan gangguan yang tidak perlu dalam *network* Manet. Misalnya, serangan *jelly fish* dapat mencemari satu *node* atau beberapa *node* untuk membuat penundaan waktu transmisi paket. Waktu transmisi yang tertunda menyebabkan penurunan kinerja *network* secara keseluruhan. Serangan konsumsi sumber daya terjadi sebagai akibat dari *node* yang terinfeksi dengan sengaja menyusup ke sumber daya *node* lain seperti baterai dan *bandwidth*. Serangan *network* Manet lainnya adalah *detour*.

Berdasarkan serangan *detour*, *node* jahat memastikan pengalihan *rute* transmisi paket data. Serangan *detour* merusak informasi *rute* asli yang disimpan di masing-masing *node network*, sehingga menimbulkan kebingungan dalam siaran di dalam *network*. Selain mengkategorikan serangan Manet berdasarkan lapisan *network*, ancaman keamanan dapat dikelompokkan berdasarkan sumber, perilaku dan *node*.

Serangan pasif dirancang untuk memotong informasi di bawah transmisi dalam *network*. Menurut kategori serangan ini, intruksi tidak menyebabkan gangguan yang terdeteksi dalam *network*. Saat mengendus informasi berlangsung, aktivitas nyata seperti menjatuhkan paket data atau pengenalan paket palsu dihindari. Secara harfiah, serangan pasif mengambil bagian dari *network* sambil tetap mengawasi informasi dalam transmisi. Oleh karena partisipasi *inert* berbahaya dalam *network*, serangan ini dengan mudah mengganggu batasan kerahasiaan data. Serangan pasif sangat sulit dideteksi karena menghindari hasutan dari operasi jahat yang dapat mengganggu jalannya *network*. Kasus jenis serangan tersebut meliputi analisis lalu lintas, pemantauan lalu lintas dan penyadapan. Di sisi lain, serangan aktif relatif mengganggu. *Node* berbahaya aktif mengubah lalu lintas *network* dan transmisi keseluruhan dengan menyebabkan kemacetan, penyebaran informasi perutean yang salah dan rusak. Sebagai hasil dari sifat aktif serangan mereka, deteksi dan pencegahannya dapat dilakukan dengan relatif mudah. Contoh serangan pasif terdiri dari serangan modifikasi, peniruan identitas, fabrikasi dan *replay* pesan (Kumar, 2011).

Serangan Manet juga dapat dikelompokkan berdasarkan lokasinya terhadap *network* yang diserang. Kriteria ini mengklasifikasikan serangan sebagai internal atau eksternal. Serangan eksternal diprakarsai oleh *node* berbahaya tanpa izin yang bukan bagian dari *network*. Penyerang eksternal dapat membanjiri paket palsu dalam *network* dan terkadang meniru *node* asli. *Node* jahat eksternal terutama, bermaksud untuk menjejalkan atau mengganggu kerja *network* biasa. Sebaliknya, serangan internal dipicu oleh *node* otentik dalam *network*. Serangan internal bertujuan untuk membajak *node* resmi dan pada gilirannya menggunakannya sebagai penyerang *proxy* atau sewenang-wenang merebut sumber daya dari *node network* lain-daya baterai, kekuatan pemrosesan, dan *bandwidth*. Terlalu berlebihan merebut sumber daya *network* dapat mengakibatkan eksploitasi yang dirancang dan disengaja dari *node* anggota (Gupta & Mittal, 2017).

## B. Solusi untuk Ancaman Keamanan Manet

Ada beberapa teknik yang disarankan untuk menggagalkan ancaman keamanan di Manet. Misalnya penelitian dari (Kaur, 2016) mengamati bahwa pada dasarnya ada dua metode untuk mengamankan Manet, yakni pendekatan proaktif dan reaktif. Menurut pendekatan proaktif, kriptografi adalah metode utama yang diterapkan-mengubah sinyal yang sedang ditransmisikan sehingga tidak mudah dideskripsi. Metode proaktif secara aktif beraksi selama operasi *network*. Sebaliknya, teknik reaktif dirancang untuk merespons saat mendeteksi ancaman keamanan. Sampai ancaman terdeteksi, tindakan keamanan reaktif tetap tidak aktif dalam *network*. Masing-masing taktik ini memiliki kualitas, kekuatan dan kelemahannya. Akibatnya setiap tindakan keamanan cocok dan tepat dalam menanggapi berbagai ancaman keamanan. Sebagian besar protokol *routing* aman mengasumsikan dan menerapkan metode proaktif untuk melindungi sinyal pesan di bawah transmisi.

Di sisi lain, beberapa protokol perutean menggunakan metode keamanan reaktif saat melakukan penerusan paket data. Studi lain seperti (Biswas & Ali, 2007) mengidentifikasi ancaman keamanan di setiap lapisan *network* dan penanggulangan yang setara. Oleh karena keamanan dan ancaman di Manet tidak didefinisikan dengan baik seperti di *network* yang bergantung pada infrastruktur, sangat penting bahwa garis

e-ISSN 2774-5155
p-ISSN 2774-5147

pertahanan yang diusulkan harus selengkap mungkin. Oleh karena itu, setiap solusi keamanan untuk Manet harus menggabungkan tindakan proaktif dan reaktif sementara dan menggabungkan pencegahan, deteksi dan reaksi. Elemen pencegahan mencegah serangan dengan secara ekspresif menambah tantangan yang mengganggu *network*.

Akibatnya mekanisme deteksi dan reaksi menentukan gangguan berbahaya dan meresponnya. Mekanisme ini sangat penting karena memungkinkan *network* menghindari serangan musuh yang mendesak, mekanisme ini penting untuk langkah-langkah keamanan lain yang sedang beroperasi dalam ancaman keamanan yang berkurang. Konstituen pendeteksian merasakan serangan dengan mengidentifikasi aktivitas tidak teratur seperti yang diungkapkan oleh *node* jahat. Aktivitas abnormal tersebut dirasakan baik secara *end-to-end* atau oleh *node* tetangga melalui mendengar saluran dan mencapai konsensus kolaboratif. Setelah mengidentifikasi *node* ancaman, elemen reaksi mengoreksi prosedur perutean dan penerusan, aktivitas semacam itu mungkin melibatkan penghindaran *rute* yang melewati *node* ancaman yang diidentifikasi atau saling mengecualikan *node* dari *network*. Studi (Koul & Sharma, 2015) mencoba untuk menyoroti berbagai masalah keamanan secara komprehensif.

**C. Aspek Keamanan pada Manet**

Aspek *network* dipengaruhi oleh serangan berbahaya termasuk penolakan ketersediaan *network*. Ketersediaan dalam *mobile ad hoc network* berkonotasi kemampuan *node network* untuk terus menjalankan tugas mereka tanpa gangguan yang tidak direncanakan atau tidak perlu. *Denial of Service* (DoS) adalah salah satu serangan yang mengganggu dan merusak aksesibilitas *network*. Integritas *network* adalah aspek lain yang dapat diserang dalam *mobile ad hoc network*. Integritas *network* memastikan bahwa identitas paket data di bawah propagasi dipertahankan. Keamanan integritas data dapat dikompromikan dengan dua cara utama, yaitu melalui perubahan yang jahat dan perubahan yang tidak disengaja. Berdasarkan serangan berbahaya terhadap integritas data, paket data yang sedang ditransmisikan dapat dihapus, diganti atau rusak. Namun, jika paket data atau isinya hilang atau diubah sebagai akibat dari kerusakan *network* alami, kejadian tersebut disebut perubahan yang tidak disengaja. Kerahasiaan pesan adalah bagian lain yang dapat dikompromikan oleh penyusup jahat. Serangan terhadap kerahasiaan data terjadi ketika orang atau agen yang tidak berwenang mengakses pesan yang tidak boleh mereka lakukan. Serangan berbahaya juga dapat membahayakan keaslian data. Keaslian data dilanggar ketika peniru mendapatkan akses ke data. Jika menghindari ancaman dan serangan ini, sangat penting bahwa prosedur otentikasi yang sesuai disematkan dalam protokol perutean *mobile ad hoc network*. Orang atau agen yang mengakses *network* harus selalu membuktikan identitas mereka untuk otorisasi. Entitas pengguna potensial untuk *network* memerlukan kredensial standar dan aman. Demikian pula enkripsi kredensial akses sangat penting dalam menjaga anonimitas dan privasi.

## KESIMPULAN

Menurut ulasan artikel jurnal ini, jelas bahwa ada banyak penelitian yang mencoba menyoroti masalah keamanan dan solusinya di Manet. Namun, hampir semuanya belum memberikan tinjauan komprehensif terkait masalah keamanan dan solusi mereka di Manet, mereka kekurangan fitur seperti kategorisasi ancaman keamanan yang lengkap. Menanggapi kekurangan literatur ini, artikel ini mencoba menyajikan tinjauan literatur komprehensif tentang masalah keamanan Manet, terutama ancaman dan solusi. Perlu dicatat, bagaimanapun masyarakat telah menghadapi kemajuan teknologi yang konstan,

sehingga menambah inovasi baru. Oleh karena itu, sangat penting bagi para peneliti untuk terus meninjau tambahan baru pada studi yang ada. Area Manet hanya akan terus bertumbuh. Menurut alasan ini, kompilasi berkelanjutan dari perkembangan ini sangat penting untuk kemajuan pengetahuan. Penelitian masa depan disarankan dapat mencakup pemeriksaan dan eksplorasi bidang-bidang seperti masa depan Manet dan dampak Manet terhadap sektor pendidikan dan pertanian.

## BIBLIOGRAFI


Alamsyah, D. (2012). *LKP: Instalasi dan Troubleshooting di Warnet Aundrey (Client) Sidoarjo*. Institut Bisnis dan Informatika Stikom.

Azra, A. (2019). *Pendidikan Islam: tradisi dan modernisasi di tengah tantangan milenium III*. Prenada Media.

Bagenda, D. N., & Ajianto, G. (2014). Prototipe Sistem Keamanan Rumah Menggunakan GSM Sebagai Pengirim Informasi Berbasis Mikrokontroler. *Jurnal Komputer Bisnis*, *5*(1).

Biswas, K., & Ali, M. (2007). *Security threats in mobile ad hoc network*.

Derveloy, R. (2012). Security Issues of Ad Hoc *Network*s. *CPSC-5620 SPRING 2012*.

Febriane, S., & Mariamah, M. (2013). Keberhasilan Semu Deradikalisasi di Indonesia. *Global: Jurnal Politik Internasional*, *15*(2).

Gagandeep, A., & Kumar, P. (2012). Analysis of different security attacks in MANETs on protocol stack A-review. *International Journal of Engineering and Advanced Technology (IJEAT)*, *1*(5), 269–275.

Gupta, K., & Mittal, P. K. (2017). An overview of security in MANET. *Int J Adv Res Comput Sci Softw Eng ISSN*, *7*(6), 151–156.

Hakim, L. (2013). Proteksi Anarkisisme. *Kafaah: Journal of Gender Studies*, *3*(2), 223–238.

Hamim, S. (2019). *Efisiensi Rute pada Routing Aodv Menggunakan Algoritma Path Aware Short*. Universitas Muhammadiyah Gresik.

Handayaningsih, S., & Nugroho, H. (2013). MODEL SISTEM M-GOVERNMENT (Studi Kasus: Pemerintah Kota Yogyakarta). *Jurnal Informatika Ahmad Dahlan*, *7*(2), 104170.

Hardiono, G., & Harsasto, P. (2018). *Network*ing dalam Kebijakan Optimalisasi Terminal Terpadu Pulo Gebang. *Journal of Politic and Government Studies*, *7*(2), 161–170.

Hariyadi, M. (2016). *Implementasi Wireless VOIP Dan Routing Better Approach To Mobile Ad-Hoc Network (Batman) Pada Rural Area Berbasis Embedded System-Implemetation Wireless VOIP And Routing Better Approach To Mobile Adhoc Network (Batman) In Rural Areas Based Embedded System*. Institut Teknologi Sepuluh Nopember.

Kaur, P. (2016). An Overview on MANET-Advantages, Characteristics and Security Attacks. *International Journal of Computer Applications, 4th International Conference on Advancements in Engineering & Technology (ICAET 2016)*.

Koul, A., & Sharma, M. (2015). Cumulative Techniques for Overcoming Security Threats in Manets. *International Journal of Computer Network & Information Security*, *7*(5).

Kumar, A. (2011). Security attacks in MANET-a review. *IJCA Proceedings on National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing*.

Lucy, B., Si, P., Ht, C., Rizky, A. J., & Edu, B. L. I. (2012). *Dahsyatnya Brain Smart Teaching: Cara Super Jitu Optimalkan Kecerdasan Otak dan Prestasi Belajar Anak*. Penebar PLUS+.

e-ISSN 2774-5155
p-ISSN 2774-5147

Mufid, F. L. (2018). Kebijakan Integral Hukum Pidana dengan Technology Prevention dalam Upaya Pencegahan Kejahatan Cyberbullying. *Jurnal Rechtens*, *7*(2), 229–246.

Nuradhawati, R. (2019). Dinamika Sentralisasi Dan Desentralisasi Di Indonesia. *Jurnal Academia Praja*, *2*(01), 152–170.

Parwekar, P., & Arora, S. (2014). Security Issues and Its Counter Measures in Mobile Ad Hoc *Network*s. *ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India-Vol I*, 301–309.

Rai, A. P., Srivastava, V., & Bhatia, R. (2012). Wormhole attack detection in mobile ad hoc *network*s. *International Journal of Engineering and Innovative Technology*, *2*(2), 384–389.