ADIOS: Advanced Detection of Intrusions On Sensor Networks.

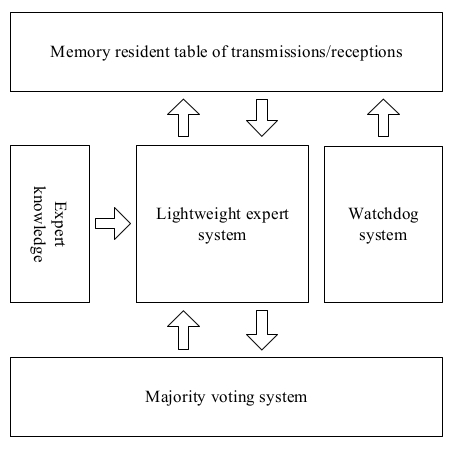
## Pendahuluan

Wireless Sensor Networks merupakan peralatan sistem embedded yang di dalamnya terdapat satu atau lebih sensor dan dilengkapi dengan peralatan sistem komunikasi, peralatan ini biasanya digunakan untuk monitoring lingkungan, keamanan kendaraan, keamanan gedung, dan sebagainya. Mengingat sifat kritis dari pengaplikasian ini, sangatlah penting untuk meyakinkan jika wireless sensor network arsitektur dapat diandalkan untu tetap berguna dan aman meskipun dengan keberadaan dari pengganggu. Node-node dari wireless ini didesain menjadi kecil, murah, dan tidak berat dan oleh karena itu dapat membatasi kapasitas komputasi dan baterai yang juga menimbulkan masalah tidak dapat digunakannya solusi-solusi kriptografi yang digunakan di PC pada peralatan ini. Sehingga hal ini dapat memungkinkan pengganggu untuk mencuri salah satu node dan melakukan reverse-engineering untuk mendapatkan kriptografi key atau informasi sensitif lainnya. Yang lebih parah lagi pengganggu juga dapat memperkenalkan node palsu merea sendiri pada jaringan untuk mengganggu aliran dari trafik jaringan atau juga dapat melakukan black hole attack(jenis dari DDOS attack pada ad hoc network).

Dan inilah tugas ADIOS, yaitu menyediakan fitur *watchdog* yang memanfaatkan mode *promisuous* untuk menangkap paket yang ditransmisikan dari node lain ke node yang lainnya sehingga diperoleh data-data yang nantinya diolah oleh inference engine untuk menentukan adanya *black-hole attack* dan juga memberikan tindakan untuk mengurangi dampak *black hole attack*.

## Arsitetektur dari ADIOS

ADIOS terdiri dari lima komponen utama: yaitu lightweight *expert system(inference engine)*, *expert knowledge(knowledge base)*, *memory resident table*, *majority voting system*, dan *watchdog system*.



## Komponen ADIOS

# Lightweight Expert System

Lightweight expert system(LES) merupakan bagian utama dari ADIOS. Bagian LES ini merupakan bagian di mana *reasoning engine* terletak dan di mana *inferencing* dilakukan. Di bagian ini juga pertimbangan dilakukan mengenai aktivitas jaringan yang dicurigai. Bagian LES ini mengambil input dari semua module kecuali watchdog system. Bagian LES ini selanjutnya melanjutkan data kepada dan dari *majority voting system* dan *memory resident table*.

# Expert Knowledge(Knowledge Base)

Expert Knowledge Module berisi aturan-aturan, definisi-definisi dan urutan-urutan kejadian yang mendeskripsikan kepada LES seperti apa serangan black hole. Expert knowledge ini merupakan file definisi-definisi secara efektif yang akan diproses oleh LES. Expert Knowledge dapat di *swap out* untuk memperoleh expert knowledge lain yang akan membuat ADIOS dapat mendetesi serangan-serangan baru dan variasi-variasi dari serangan lama.

# Watchdog System

Modul *watchdog* terdiri dari *network interface card* (dengan mode *promisuous*) dan memiliki kemampuan untuk membaca dan menuliskan pada *memory resident table*. Watchdog ini merekam aktivitas yang menarik di *memory resident table* untuk nantinya dianalisis oleh LES. Watchdog ini memanfaatkan keuntungan dari fakta-fakta yang diperoleh interface saat mode promiscuous sehingga dapat menerima tranmisi-tranmisi yang dikirimkan pada tujuan lain dan dapat memanfaatkan informasi ini untuk mengidentifikasi kondisi tidak normal dari proses routing pada jaringan.

# Memory Resident Table

*Memory Resident Table* pada dasarnya merupakan workspace umum yang ADIOS gunakan. Kejadian-kejadian pada jaringan seperti *route request*, *route replies*, dan *abnormal forwarding* oleh sebuah node tetangga disimpan sementara pada MRT untuk nantinya diproses oleh LES. MRT diharapkan menjadi subsistem yang menkonsumsi sejumlah besar dari memori yang digunakan oleh ADIOS. Semakin besar MRT dapat melacak lebih dari kejadian-kejadian jaringan dan mungkin menjadi lebih efektif untuk identifikasi serangan-serangan tetapi berhubungan dengan batasan sumber daya dari sensor node memberikan trade-off yang dilakukan berdasarkan konsumsi memori dan akurasi deteksi serangan.

# Majority Voting System

Majority Voting System merupakan bagian yang bertanggung jawab untuk mengurangi dampak dari serangan pada jaringan. Saat dipanggil, majority voting system berkomunikasi dengan node-node tetangga berhubungan dengan sebuah potensi serangan. Dengan mnggunakan majority voting, lebih dari satu node pada jaringan menentukan apakah node tertentu melakukan kejahatan. Ini dapat menghasilkan sistem yang dapat diandalkan karena mengandalkan opini lebih dari satu node untuk menentukan node mana yang melakukan kejahatan. Setelah node yang melakukan kejahatan ditemukan maka node ini diusir dari jaringan dengan cara blacklisting atau key revocation.