Pengembangan algortima kriptografi berbasis fibonacci dan one time pad teracak untuk mendukung privasi

Amiruddin, author

Abstrak

ABSTRAK
Jumlah dan ragam aplikasi terus meningkat seiring dengan perkembangan teknologi untuk Internet of Things (IoT) seperti pada Wireless Sensor Network (WSN), Mobile Ad hoc Network (MANET), dan ZigBee. Namun, isu keamanan juga terus meningkat dan meluas, termasuk pada area MANET, WSN, dan ZigBee, terutama peranti-peranti dengan memori, daya komputasi, dan sumber energi kecil. Perlindungan privasi adalah salah satu isu keamanan yang sangat penting dalam MANET, WSN dan ZigBee karena sangat terkait dengan keselamatan data yang ditransmisikan.
Pada penelitian ini, diusulkan algoritma-algoritma baru untuk pembangkitan kunci acak, enkripsi, dan dekripsi dalam mendukung perlindungan privasi untuk aplikasi pada MANET, WSN, dan ZigBee. Algoritma pembangkitan kunci acak usulan menggunakan Fibonacci teracak dengan penambahan faktor pengacak untuk menghasilkan rangkaian kunci acak dan panjang tetapi memiliki komputasi rendah, sedangkan algoritma enkripsi/dekripsi menggunakan One Time Pad (OTP) teracak dengan penambahan faktor pengacak yang bertujuan untuk memenuhi uji keacakan, difusi, dan konfusi pada Ciphertext yang dihasilkan. Simulasi untuk evaluasi algoritma dilakukan dengan menggunakan perangkat lunak Matlab, NS-2, dan peranti ZigBee.
Hasil penelitian menunjukkan bahwa algoritma-algoritma usulan menghasilkan rangkaian kunci dan Ciphertext yang acak. Melalui pengujian kecepatan, korelasi, autokorelasi, difusi, dan konfusi, hasil simulasi menunjukkan kelebihan algoritmaalgoritma usulan dibanding algoritma lain. Untuk pembuktian konsep, algoritmaalgoritma usulan sudah dismulasikan pada MANET dengan perangkat lunak simulator jaringan, NS-2. Hasil simulasi jaringan memperlihatkan adanya peningkatan throughput seiring dengan meningkatnya jumlah node dalam jaringan serta delay yang relatif tetap untuk 20- 60 nodes yang mengindikasikan bahwa proses algoritma-algoritma usulan tidak mengurangi secara signifikan kinerja jaringan. Sementara implementasi testbed pada ZigBee memperlihatkan bahwa dengan memvariasikan ukuran data, transmisi data menghasilkan delay yang meningkat perlahan yang menunjukkan bahwa ukuran data mempengaruhi proses transmisi. Persentase rata-rata Packet Delivery Ratio (PDR) untuk satu perangkat akhir dan satu koordinator mencapai kisaran 80% dan menurun seiring dengan meningkatnya jumlah perangkat akhir. PDR ini menunjukkan nilai yang baik dan mendekati nilai normal sebagaimana diketahui bahwa rata-rata PDR untuk ZigBee dengan Baudrate 9600 menggunakan Crystal Frequency 12.000 MegaCycles (MC)
adalah 85%. Sementara, jarak antara dua node yang berkomunikasi juga mempengaruhi

nilai rata-rata persentase PDR, semakin jauh jaraknya, semakin rendah persentase PDR. Pada penelitian terakhir dari disertasi ini telah dikembangkan sebuah gateway multiprotokol yang dapat mengakomodir protokol-protokol RF/WiFi/Etherent, ZigBee, BLE, dan memanfaatkan protokol TCP/IP untuk pemrosesan data lebih lanjut setelah melewati gateway. Selain itu, ditambahkan algoritma enkripsi data untuk perlindungan privasi/data yang ditransmisikan melalui gateway usulan tersebut. Simulasi pengiriman data terenkripsi dari beberapa end-device ZigBee, BLE, dan WiFI ke gateway telah berhasil dilakukan. Untuk menampilkan data yang diterima server, ditambahkan halaman dashboard untuk gateway. Secara umum, proses dekripsi memerlukan waktu pemrosesan yang sedikit lebih lama dibanding proses enkripsi untuk ukuran data yang sama. Hal ini dapat terjadi karena pada algoritma enkripsi dan dekripsi terjadi dua proses fungsi yang sama yaitu AND, XOR, dan Circular Shift, dan satu proses fungsi yang berbeda yaitu Addition pada proses enkripsi dan Subtraction pada proses dekripsi. Perbedaan kedua fungsi tersebut mungkin menyebabkan terjadinya perbedaan lamanya waktu pemrosesan data. Hasil testbed menunjukkan bahwa protokol WiFi mengungguli XBee dan BLE dalam kinerja throughput. XBee memiliki nilai throughput yang terendah di antara ketiga protokol. Meskipun demikian, ketiga protokol mengalami peningkatan nilai throughput ketika ukuran data yang diproses juga meningkat untuk rentang ukuran data 10-100 Bytes. Terjadinya peningkatan throughput pada saat ukuran data meningkat mungkin dapat terjadi selama masih di bawah ukuran maksimal kapasitas jaringan yang digunakan
<hr>
ABSTRACT
The number and variety of applications continue to increase along with the development of technology for the Internet of Things (IoT) such as Wireless Sensor Network (WSN), Mobile Ad hoc Network (MANET), and ZigBee. However, security issues are also increasing and widespread, including in areas of MANET, WSN, and ZigBee that have low-capacity devices in terms of memory, computing power, and energy sources. Privacy preservation is one of the most important security issues in MANET, WSN and ZigBee as it is closely related to the security of transmitted data.
In this research, new algorithms are proposed for random key generation, encryption, and decryption to support privacy preservation on WSN, MANET and ZigBee. The random key generation algorithm uses scrambled Fibonacci with the addition of scrambling factor to generate random key sequence with required length, but having a low computational overhead, while the encryption/decryption algorithm uses scrambled One Time Pad (OTP) with the addition of scrambling factor that aims to satisfy randomness test, diffusion, and confusion of the generated Ciphertext. Evaluation of the proposed algorithms is conducted using Matlab, NS-2, and ZigBee devices.
The results show that the proposed algorithms produce a series of keys and random Ciphertext. Through speed, correlation, autocorrelation, diffusion, and confusion testing, the simulation results show the advantages of proposed algorithms over other algorithms. To prove the concept, the proposed algorithms have been simulated on MANET with network simulator software, NS-2. Network simulation results show an

increase in throughput along with an increase in the number of nodes in the network and a relatively fixed delay of 20-60 nodes indicating that the proposed algorithm processes do not significantly reduce network performance. While the testbed implementation on ZigBee shows that by varying the size of the data, data transmission generates slowly increasing delay which indicates that the size of the data affects the transmission process. The average percentage of Packet Delivery Ratio (PDR) for one end-device and one coordinator reaches the 80% range and decreases as the number of end-devices increases. This PDR shows good value and close to normal value as it is known that the average PDR for ZigBee with Baudrate 9600 using Crystal Frequency 12,000 MegaCycles (MC) is 85%. Meanwhile, the distance between two communicating nodes also affects the mean value of PDR percentage, the farther the distance, the lower the PDR percentage.

In the last part of the research for this dissertation, a multi-protocol gateway has been developed that can accommodate RF / WiFi / Etherent, ZigBee, BLE protocols and utilize TCP / IP protocol for further data processing after passing through the gateway. In addition, a data encryption algorithm is added for the security of the data transmitted through the proposed gateway. In general, the decryption process takes a bit longer processing time than the encryption process for the same data size. This can happen because the encryption and decryption algorithms even though they apply the same operations of AND, XOR, and Circular Shift, they have a different function that is Addition for the encryption process and Subtraction for the decryption process. The difference between the two functions may cause the difference in data processing time. The testbed results show that the WiFi protocol outperforms XBee and BLE in throughput performance. XBee has the lowest throughput value among the three protocols. Nevertheless, all three protocols have an increase in throughput value when the size of the processed data is also increased for a range of 10-100 Bytes of data size. An increase in throughput at the time of increased data size may occur as long as it remains below the maximum capacity of the network used.