Pengembangan Skema Baru Cryptographic Key Update untuk Meningkatkan Keamanan Protokol Long Range Wide Area Network (LoRaWAN) = The Development of New Cryptographic Key Updating Schemes to Improve the Security of Long Range Wide Area Network (LoRaWAN) Protocol

Nur Hayati, author

Abstrak

Long-range wide area network (LoRaWAN) memiliki kelemahan dalam hal manajemen kunci kriptografinya, yaitu root key dan session key. Root key LoRaWAN tidak pernah berubah sepanjang masa pakai perangkat, sedangkan session key digunakan untuk mengamankan beberapa sesi komunikasi. Kelemahan tersebut membahayakan keamanan LoRaWAN. Oleh karena itu, penelitian ini mengusulkan skema baru cryptographic key update yang secara berkala mengubah nilai root key dan session key. Skema root key update bekerja berdasarkan algoritma CTR_AES DRBG 128 dan memiliki dua tahap berurutan: inisialisasi dan proses root key update. Sementara itu, skema session key update terdiri dari tiga tahapan: tahap inisialisasi, penyiapan keying material, dan tahap key update berdasarkan algoritma Truncated Photon-256 dengan keying material yang dapat diperbarui. Semua tahapan disusun oleh seperangkat protokol komunikasi baru. Untuk memvalidasi skema yang diusulkan, dilakukan pengujian keacakan urutan bit dari root key dan session yang dihasilkan oleh setiap algoritma dan pengujian keamanan protokol komunikasi. Hasil pengujian menunjukkan bahwa setiap algoritma menghasilkan kunci yang lulus semua 15 parameter rangkaian uji statistik NIST 800-22 dengan nilai proporsi untuk root key berada diantara 0,9855 hingga 0,9936 dan nilai proporsi untuk session key berada diantara 0,9831 hingga 0,9945. Selanjutnya, Scyther tools membuktikan bahwa protokol komunikasi yang diusulkan tersebut memastikan skema pembaharuan LoRaWAN yang aman dan menjamin bahwa intersepsi aktif tidak terjadi. Analisis keamanan formal menggunakan GNY logic menunjukkan bahwa tujuan keamanan secara keseluruhan yang didefinisikan telah terverifikasi secara logis. Penjelasan analisis keamanan root key update difokuskan pada pada fitur perlindungan integritas, perfect forward secrecy, dan ketahanan replay attack. Sementara, analisis skema session key update juga membahas semua fitur keamanan tersebut dengan tambahan analisis terhadap dua hal: kerahasiaan data dan mutual authentication. Terakhir, dilakukan evaluasi terhadap kinerja skema cryptographic key update. Skema root key update hanya membutuhkan proses komputasi sebanyak 2N atau dua langkah protokol pada sisi end device. Selain itu, skema root key update mendukung proses pembaharuan secara dinamis, simultan, dilakukan secara remote pada kondisi saat end device ditempatkan di area yang jauh di dalam cakupan area LoRaWAN. Semantara kinerja pada skema session key dievaluasi dalam hal tiga hal yaitu biaya komputasi, biaya komunikasi dan penyimpanan. Biaya komputasi session key update pada sisi backend system sangat kecil sehingga dapat dianggap tidak menambah beban arsitektur jaringan. Berikutnya, skema session key update menghemat biaya komunikasi sehingga menjadi 14,28% pada skenario yang telah dijelaskan, serta dengan peningkatan kinerja yang diperoleh hanya memerlukan tambahan penyimpanan data yang sangat kecil yaitu sebesar 19 Byte dibandingkan total media penyimpanan pada end device LoRaWAN.

.....The root key and session key of a long-range wide area network (LoRaWAN) have flaws in their

cryptographic key management. The root key LoRaWAN is constant over the device's lifetime, while the session key is used to secure many communication sessions. The security of LoRaWAN is at risk due to these flaws. As a result, this study suggests novel cryptographic key updating schemes that change the root key and session key on a regular basis. The root key updating scheme comprises two sequential phases: the initialization and the root key update process based on the CTR AES DRBG 128 algorithm. On the other hand, the session key updating scheme is composed of three consecutive stages: initial, preparation of the keying materials, and key updating stage using the truncated Photon-256 algorithm and updatable keying materials. Sets of novel communication protocols govern all stages. The proposed schemes are put to the test in two different ways: the security test of the communication protocols and a random bit sequence test of the root key and session key generated by each technique. The results show that each algorithm generates keys that satisfy all 15 criteria of the NIST 800-22 statistical test suites, with the root key's proportion value between 0.9855 and 0.9936 and the session key's proportion between 0.9831 and 0.9945. The Scyther tools subsequently demonstrate that such communication protocols assure the security of LoRaWAN key update schemes and provide assurance against active interceptions. The formal security assessments based on GNY logic indicate that the general security objectives are logically supported. By concentrating on the security attributes of integrity protection, perfect forward secrecy, and replay attack resistance, the analysis of the root key updating technique is further developed. Data confidentiality and mutual authentication are two additional security factors that are elaborated on as part of the session key update scheme study. Finally, the performances of the suggested cryptographic key schemes are assessed. On the end device side, the root key update approach only necessitates a computing procedure of 2N or two protocol steps. When the end device is placed in a remote location inside the LoRaWAN coverage region, the root key updating scheme also supports dynamic, concurrent, remote update procedures. Meanwhile, the proposed session key update scheme is assessed in terms of computational, communication, and storage costs. The very low computational cost of the technique shows that the backend system is not put under any additional strain. In the described situation outlined, the cost of communication becomes 14.28 percent, showing that the proposed method uses less traffic than the previous solution. However, the scheme provides LoRaWAN with more robust security by generating a new key for each communication session. In comparison to the total amount of storage on the LoRaWAN end device, the scheme only requires a small amount of extra space, i.e.,19 Bytes.