Pengamanan Sesi Kunci pada Autentikasi Broadcast di Jaringan Sensor Nirkabel

Timothy Jefrin Viali Samosir[1], Dr. Farah Afianti, S.T., M.T.[2], Prasti Eko Yunanto, S.T., M.Kom.[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[4]Divisi Digital Service PT Telekomunikasi Indonesia
[1]timothyjefrin@students.telkomuniversity.ac.id, [2]farahafi@telkomuniversity.ac.id,
[3]gppras@telkomuniversity.ac.id

Abstrak

Perkembangan *internet of things* (IoT) sudah semakin berkembang, seperti jaringan sensor nirkabel (JSN). Pemanfaatan JSN dalam kehidupan sehari-hari sudah banyak membantu di berbagai bidang. JSN memiliki node-node yang saling berhubungan dengan memori, sumber daya, dan komputasi terbatas. Karena keterbatasan tersebut, pesan atau data yang ada pada node-node tersebut terancam dirusak atau diketahui oleh penyerang. Dalam perkembangannya, JSN memiliki beberapa metode untuk mengamankan pesan atau data tersebut. Contohnya dengan skema autentikasi *broadcast* dan skema *puzzle* dengan memanfaatkan kunci sesi [1]**. Dalam makalah ini, mengusulkan modifikasi skema autentikasi *broadcast* dengan menambahkan aspek *confidentiality* pada pesan dan kunci sesinya. Kunci sesi tersebut diamankan dengan enkripsi *hill cipher* yang sudah dimodifikasi. Hasil pengujian dari implementasi *hill cipher* menunjukkan, waktu yang dibutuhkan untuk eknripsi dengan Backward Keychain lebih rendah 98.697% dibandingkan enkripsi dengan ECDH.**

Kata kunci : IoT, JSN, autentikasi *broadcast, hill cipher*.