Emerging technology space: Sensor and building networks

Class of cryptographic requirements: Identity-based cryptography

Title: Secure location and energy aware routing in Wireless Sensor Networks using Identity-based cryptography

Authors:

Harsh Kupwade-Patil
Dept. of CSE
Lyle School of Engineering
Southern Methodist University
Dallas, Texas
Email: hkupwade@smu.edu

Joseph Camp
Dept. of EE
Lyle School of Engineering
Southern Methodist University
Dallas, Texas

Stephen A. Szygenda
Dept. of CSE
Lyle School of Engineering
Southern Methodist University
Dallas, Texas

Abstract:

Wireless Sensor Networks (WSN) have played a crucial role in many military and civilian applications. As more low cost, low power and multifunctional sensor nodes are being deployed, security in such sensor networks becomes a prominent issue in WSN. Recent advances in wireless networks did not give the necessary attention to security with regard to device constraints, since they base their design on legacy wireless networks. As more security solutions are being proposed in WSN, there is an increase in the lack of co-ordination between various security measures at different layers, leading to functional redundancy and increased overhead. In this paper, we review the classical selective forwarding attack in WSN and see how an identity-based cryptographic scheme using a cross-layer design approach is helpful in circumventing such an attack. Subsequently, we propose a novel secure location and energy-aware routing scheme using identity-based cryptography to prevent such selective forwarding attacks. The experiments were conducted on MICA2 Mote, which has an ATmega128 8-bit processor, 128 KB EEPROM chip and a 4KB RAM chip. The ID based cryptographic security schemes use a pairing based cryptographic library suitable for MICA2 motes called Tinypbc. We make an adept implementation of squaring, modular reduction, multiplication and inversion in $F_{2^{163}}$ (NIST irreducible polynomial for the finite field $f(z) = z_{163} + z_7 + z_6 + z_3 + 1$) and $F_{2^{233}}$. Point multiplication is implemented on generic binary curves and Koblitz curves. We implement the mesh and star topology on an emulator called Advanced wireleSS Environment Research Testbed (ASSERT) to test our secure ID based cryptographic mechanisms. ASSERT emulates node mobility, link interference and creates virtual distances using controlled attenuation.

References

- Harsh Kupwade Patil and Stephen A. Szygenda "Security for Wireless Sensor Networks using Identity-Based Cryptography", ISBN-10: 1439869014, Taylor & Francis LLC - CRC Press, June 2012
- H. Kupwade Patil, J. Camp and S. Szygenda, "Identity based authentication using a Cross Layer Design approach inWireless Sensor Networks," in *World Multiconference on Systemics, Cybernetics and Informatics (WMSCI 2011)*, Orlando, July 19th - 22nd, 2011
- Harsh Kupwade Patil, Stephen A. Szygenda, "Identity-based key distribution schemes using an adaptive approach in Wireless Sensor Networks", in Journal of Information Systems Technology & Planning - JISTP, vol. 4, issue 6, May 2011.
- H. Kupwade Patil and S. Szygenda, "Identity based key distribution schemes using a Cross Layer Design approach in Wireless Sensor etworks," in *Proc. of Intellectbase International Consortium*, vol. 15, pp. 109-118, March 2011.