An Authenticated Key Agreement Scheme for Sensor Networks Using Symmetric Key Cryptography

Mee Loong Yang, Adnan Al-Anbuky, William Liu

WHAT WE ACHIEVED

A fast, efficient, and secure non-interactive key agreement scheme for pairs of sensor nodes to compute their pairwise secret key after obtaining their counterpart's *ID*

BACKGROUND

Pairwise keys are required to protect the communications between nodes. For large mobile ad hoc networks, key agreement schemes for establishing pairwise keys are most suitable. With limited resources in sensor devices, a symmetric key agrememt scheme such as the Blom's scheme would be useful. However it has limitations due to the large memory required for large networks.

OBJECTIVES

Develop a new scheme based on the Blom's scheme which is suitable for large scale use without requiring proportionally large storage.

Analyse how the scheme may be broken and calculate the security strength of the scheme.

METHODS

The Blom's scheme was modified by using multiple master keys and multiple public key (IDs) for each node. These are used in permutations to compute multiple private keys which are stored in a random order in the nodes. The computations are over a small prime field, e.g. 31. As a result, the private-public-master key associations (PPMka) are lost. Without the PPMka, captured private keys cannot be used to break the scheme.

By analysing the scheme using combinatronics and probabilities, we proved that, with suitable parameters, the most eficient methods to discover the PPMka requires verly large node captures and infeasible amounts of time and effort.

IMPLEMENTATION

Trusted Authority (TA):

1. Generates N secret symmetric (m x m) matrices M_j for $j = 1, \ldots, N$ over prime field F_p,
2. Assigns each node an *ID,* a 16 bit integer which is a factor of η

Computes the node *i*'s public key vectors

$$\mathbf{V}_i^T = \left[1 \quad s_i \quad s_i^2 \cdots s_i^{m-1} \right] \pmod q$$

$$\text{where} \quad s_i = ID + i - 1, \quad \text{for} \quad i = 1, \cdots, \eta$$

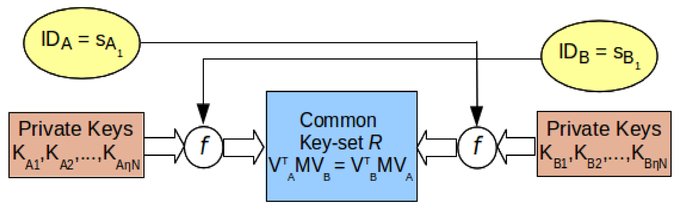
Compute the node's private keys

$$\mathbf{K}_{ij} = \mathbf{V}_i^T \mathbf{M}_j \pmod p$$

$$\text{for } i = 1, \cdots, \eta \text{ and } j = 1, \cdots, N$$

Pairwise key derivation:

1. Nodes A and B exchange their *ID*s
2. Generate counterpart's public key vectors V
   compute the key-set R using all permutations of V and private keys
3. Sort the set R and extract bits to form the pairwise key K_{AB}



RESULTS

Security features:

1. Large pairwise keys
2. Mutual authentication
3. To break the scheme, requires capturing n_c nodes, or Φ solutions of (m x m) system of equations

Performance features:

1. Fixed memory size for private keys even with large network sizes
2. Few exchange bits
3. Fast computation times

Security Strength & key size (bits)	Nodes n_c	Operations Φ	ROM $Q_o(B)$	Computation Time $T_{comp}(ms)$	p	m	η	N
192	6.63×10^4	1.00×10^{58}	1824	342	61	38	4	12
128	1.38×10^7	9.04×10^{38}	1170	279	31	26	5	9
112	4.55×10^5	2.33×10^{36}	920	185	31	23	4	11
80	2.30×10^4	1.84×10^{25}	612	104	31	17	3	12
64	1.02×10^6	8.47×10^{18}	468	85	17	13	3	12

Reference

Yang, M.L., Al-Anbuky, A., & Liu, W. (2014, June), *An Authenticated Key Agreement Scheme for Wireless Sensor Networks*, Journal of Sensors and Actuator Networks, 2014, 3(3), pp. 181-206; doi:10.3390/jsan3030181