Sensor Network Security

R. Blom, "*An optimal class of symmetric key generation systems,*" *Advances in Cryptology: Proceedings of EUROCRYPT 84*, Lecture Notes in Computer Science, Springer-Verlag, 209:335–338, 1985.

Reference on application to sensor networks

Wenliang Du, Jing Deng, Yunghsiang S. Han, and Pramod Varshney, "A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks," *Proceedings of the 10th ACM Conference on Computer and Communications Security*, Washington DC, October 2003.

Motivation

- Ad hoc networks with no trusted infrastructure support
- Sensors have limited computation, storage, and energy resources
  - use symmetric key encryption
- Standard solutions to enable key agreement between computing devices are not appropriate
  - Public key algorithms
  - Trusted server

Pre-distribution of symmetric keys

- Naïve solution – each node has the same master key
  - One node compromised => entire network compromised
- For a network of N nodes, each node is pre-installed with N-1 symmetric keys for all other nodes
  - Not scalable

Blom's key pre-distribution scheme

λ-secure property

- When an adversary compromises less than or equal to λ nodes, uncompromised nodes are perfectly secure.
- When an adversary compromises more than λ nodes, all pairwise keys of the entire network are compromised

Pre-deployment phase

- A trusted controller first constructs a $(\lambda+1)\times N$ matrix, G, over a finite field $GF(q)$, where
  - N is the number of nodes
  - G is public information
  - q is a prime number larger than 2^n , where n is number of bits in a key
- Then the controller
  - creates a *random* $(\lambda+1)\times(\lambda+1)$ symmetric matrix D over GF(q)
  - Matrix D is secret known only to the controller
  - The controller computes an $N\times(\lambda+1)$ matrix

$$A = (D.G)^T$$

where $(D.G)^T$ is the transpose of matrix D.G

Pre-deployment phase (2)

- Because D is symmetric, we have

$$A.G = (D.G)^T.G = G^T.D^T.G = G^T.D.G$$
$$= G^T.A^T = (AG)^T$$

Thus, AG is a symmetric matrix to be denoted by

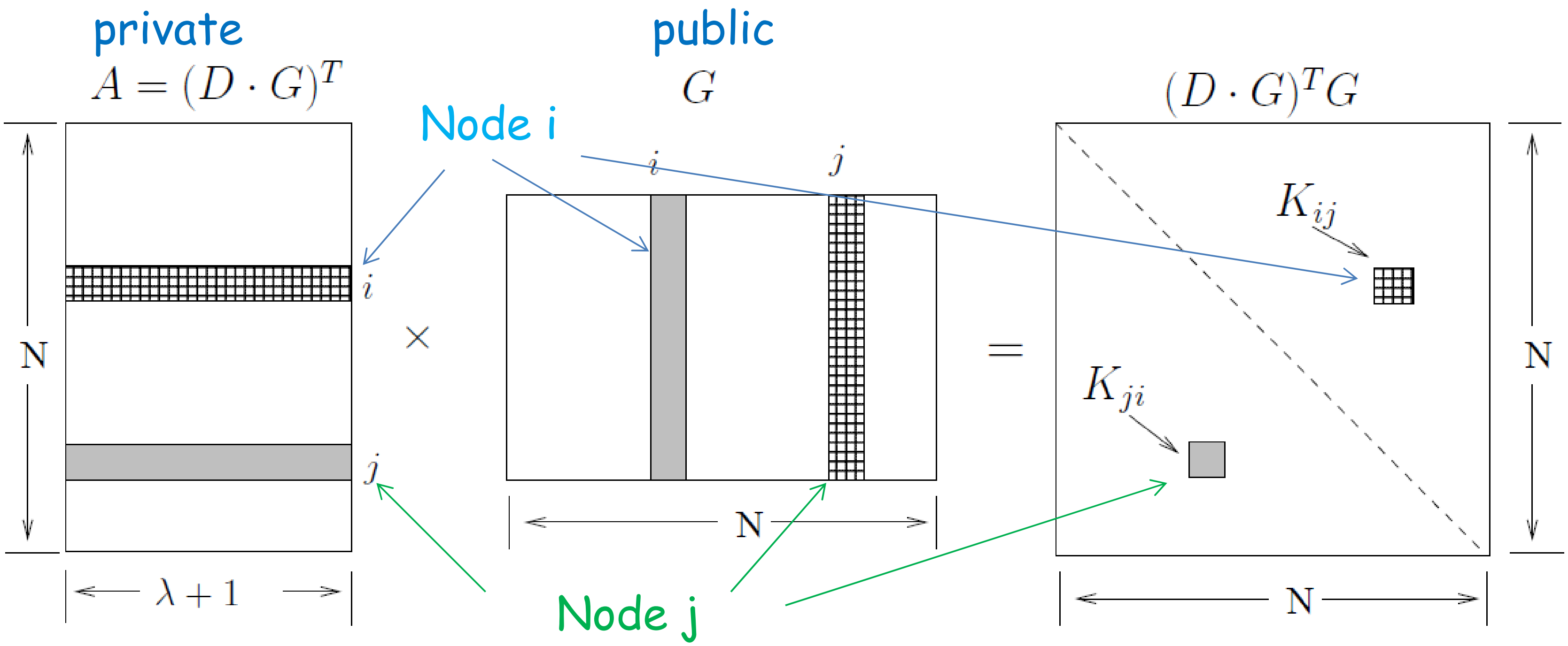
$K = AG$, where $K_{ij} = K_{ji}$, for all $1 \leq i, j \leq N$, which can be used as the pairwise key between nodes i and j

Comment: Since i and j share a private key, encrypted messages between them may be relayed by other nodes

Blom's key pre-distribution

- The controller stores
  the kth row of matrix *A* in node k, and
  the kth column of matrix *G* at node k
- When nodes i and j need to communicate confidentially,
  - they first exchange their columns of *G* (which is public info) in plaintext
  - **then i and j compute K_{ij} and K_{ji}** , respectively, using each node's private info (row of *A*) and received column of *G*

Blom's scheme illustrated



If *any* λ+1 columns of G are linearly independent, then the above scheme is λ-secure

An example of matrix G

- Let each pairwise key be an element in the finite field GF(q), where q is the smallest prime number larger than 2^n
  - for keys represented by n bits
- Let s be a primitive element of GF(q) and q > N
  - each nonzero element in GF(q) can be represented by some power of s
  - $s^i \neq s^j$ for $i \neq j$

An example of matrix G (cont.)

A Vandermonde matrix !

$$G = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ s & s^2 & s^3 & \cdots & s^N \\ s^2 & (s^2)^2 & (s^3)^2 & \cdots & (s^N)^2 \\ & & & \vdots & \\ s^\lambda & (s^2)^\lambda & (s^3)^\lambda & \cdots & (s^N)^\lambda \end{bmatrix}$$

- $s, s^2 \ldots, s^N$ are all distinct
- any λ+1 columns of G are linearly independent
- only the seed s^k of the kth column is stored in node k

The End