Distributed Key Certification using Accumulators for Wireless Sensor Networks

{Jun-Young.Bae, Franck.Rousseau}@imag.fr
{Claude.Castelluccia, Cedric.Lauradoux}@inria.fr

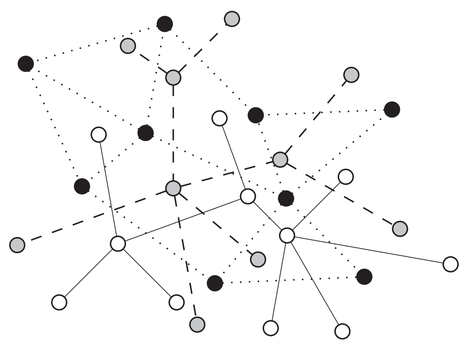
Wireless Sensor Networks (WSNs)

- Large networks composed of inexpensive low-power and energy-constrained wireless sensors.
- Will play critical roles in information gathering, management and control.
- Possible applications: military, medical, environmental, electrical, industrial etc.

Security in WSNs

- Any networked system should include at least rudimentary security.
- Wireless communications are easy to eavesdrop and manipulate.
- Requires data confidentiality, authentication and network availability

Overlapping WSNs



Motivations

- A critical issue in WSN security is key certification.
- A Certificate Authority (CA) may not be reachable during network deployment.
- Sensor nodes must be authenticated before they are enrolled to the network.
- Authentication becomes especially crucial when multiple networks are overlapping.
- The need for a lightweight, distributed key certification arises.

Our Contributions

- We propose a distributed key certification protocol that uses cryptographic accumulators.
- We examine and compare both asymmetric and symmetric accumulator-based implementations.

Cryptographic Accumulators

- Probabilistic data structure that allows a user to verify if an item belongs to a given set.
- Based on one-way, commutative functions.
- Two types of accumulators exist: asymmetric [1] and symmetric [2].

Node-to-Node Key Verification

Node 1 (N_1)
$(PK_{N_1}, SK_{N_1}), \mathbf{z}, w_1$

Node 2 (N_2)
$(PK_{N_2}, SK_{N_2}), \mathbf{z}, w_2$

PK_{N_2}, w_2 ⟵

Verify($\mathbf{z}, PK_{N_2}, w_2$)

PK_{N_1}, w_1 ⟶

Verify($\mathbf{z}, PK_{N_1}, w_1$)

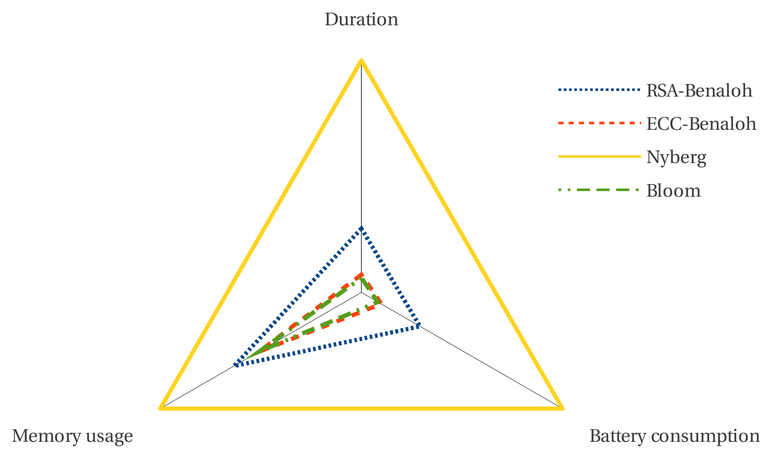
Notation Summary

Notations	Meaning
(PK_{N_i}, SK_{N_i})	Node i's public/private key
$\mathbf{z}$	Accumulator
w_i	Node i's accumulator witness

The Verify($\mathbf{z}, PK, w$) function

if Lookup(T,PK)$= false$ **then**
  if Authenticate($\mathbf{z}, PK, w$)$= true$ **then**
    Put(T, PK)
  end if
else
  Do nothing (key already verified)
end if

Comparative Results



Future work

- Be able to safely add and remove nodes from the network.
- Study how our security protocol copes with other WSN protocols.

References

[1] J. Benaloh, M. de Mare. One-Way Accumulators: A Decentralized Alternative to Digital Signatures in *EUROCRYPT 1993*
[2] D. Yum, J. Seo, P. Lee. Generalized Combinatoric Accumulator in *IEICE Transactions on Information and Systems 2008*

Acknowledgements

This work is funded by the European Union's Seventh Framework Programme (FP7): CALIPSO (`http://www.ict-calipso.eu`).