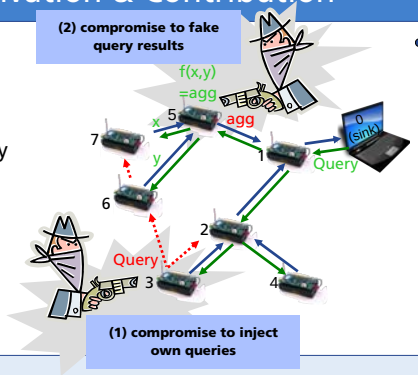
Authentic Query Dissemination and Data Aggregation in Wireless Sensor Networks

Motivation & Contribution

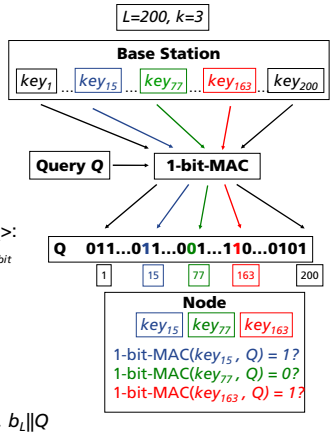
- Idea: Trade-off Security and Energy
  - Probabilistic authenticity
    - Messages authentic with predefined probability
  - Configurable probability (parameters)
  - Authenticity with higher probability requires more energy
- Contributions
  - **AQF** guarantees authenticity of queries with a predefined probability P_1
  - **ESAWN** guarantees authenticity of aggregates with a predefined probability P_2
  - Only symmetric cryptography used
  - Trade-off probabilistic authenticity and energy usage



- System Model
  - Only energy efficient security operations
  - In-network processing / data aggregation
    - Uses an aggregation function $f(\ldots) = agg$
    - Reduces communication, saves energy
  - Strong attacker model
    - Reprogram nodes, read-out memory (i.e., keys)
    - Adversary gains physical access to at most β% of all nodes (node compromise)
  - Possible attacks
    - **(1)** Inject own queries to the network
    - **(2)** Fake aggregation results

AQF: Authenticated Query Flooding

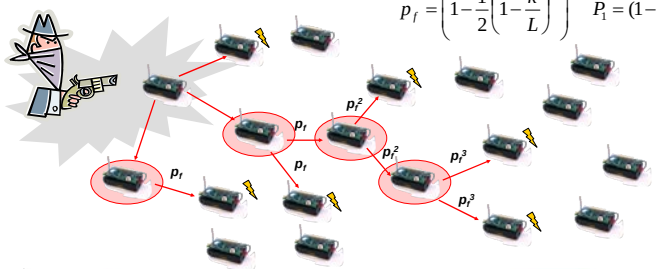
- Initialization
  - Known to all:
    - Hash function $h()$
  - Base Station:
    - L symmetric keys: $key_1, \ldots, key_L$
  - Each node:
    - k keys from L (randomly chosen)
- Base Station: compute authenticator
  - Query Q, compute $h(Q)$
  - Compute authenticator (L bits) $<b_1 \ldots b_L>$:
    - b_i = **1-bit-MAC**$(key_i, Q) = [h(key_i, h(Q))]_{last_bit}$
  - Send message $m_Q = b_1 \ldots b_L \| Q$
- Node: verify authenticator
  - Compute $h(Q)$
  - For each known key_i do:
    - 1-bit-MAC$(key_i, Q) = b_i$?
    - If $\neq$, reject Q
  - If all 1-bit-MACs correct, send $m_Q = b_1 \ldots b_L \| Q$

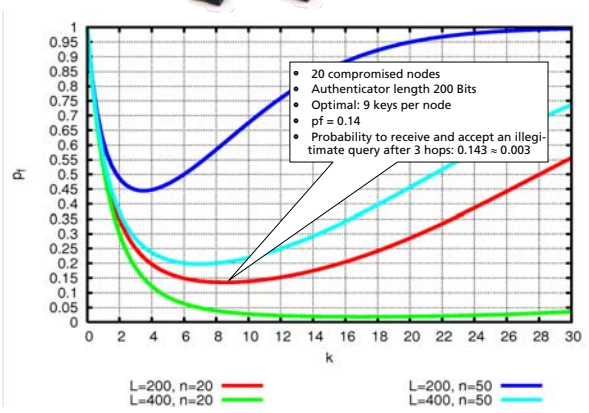


Analysis / Security-Energy-Tradeoff

- n compromised nodes (i.e., some keys known to the adversary)
- Adversary guesses all other authenticator bits
- Probability to accept the illegitimate query:

$$p_f = \left(1 - \frac{1}{2}\left(1 - \frac{k}{L}\right)^n\right)^k \qquad P_1 = (1 - p_f)$$

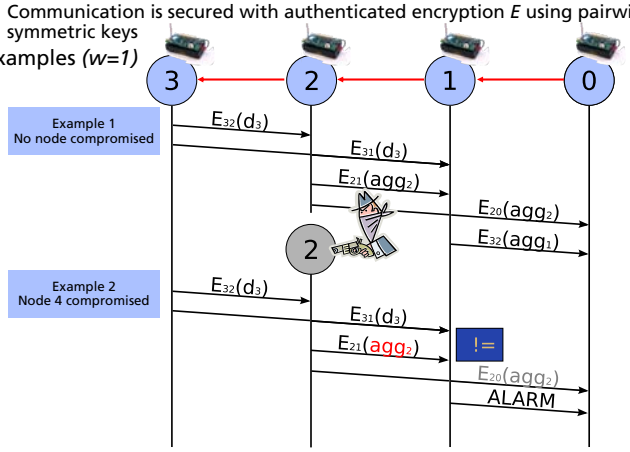




- Adjustment to the number of compromised nodes possible
- Trade-off: authenticator longer ⇒ p_f smaller ⇒ more security ⇒ more energy used

ESAWN: Extended Secure Aggregation for Wireless Sensor Networks

- Basic Protocol
  - Each node i is assigned w witnesses (the first w predecesssor of i in the tree)
  - The witnesses re-compute the aggregate of i (agg_i) and compare both
    - An alarm if sent towards the sink if any comparison fails
  - Communication is secured with authenticated encryption E using pairwise symmetric keys
- Examples *(w=1)*

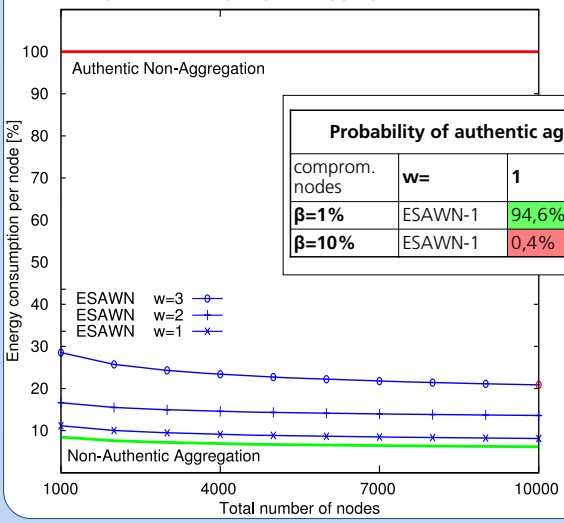


- Drawback: Alarms cannot be verified, no possibility to identify compromised nodes (for this, refer to the ESAWN-Framework [1])

[1] Joachim Wilke, Erik-Oliver Blaß, Felix C. Freiling, Martina Zitterbart: A Framework for Probabilistic, Authentic Aggregation in Wireless Sensor Networks. Praxis der Informationsverarbeitung und Kommunikation, 2:116–126, 04/2009, ISBN 978-3-598-01234-1.

Evaluation / Security-Energy-Tradeoff

- Comparison of ESAWN's energy consumption in contrast to traditional communication schemes
  - Non-Authentic Aggregation (no security, lowest energy consumption)
  - Authentic Non-Aggregation (full security, not energy efficient)
- Simulative results
  - Average of incoming edges in aggregation tree δ=2



Probability of authentic aggregation (P_2)

compromn. nodes	w=	1	2	3
β=1%	ESAWN-1	94,6%	99,9%	100%
β=10%	ESAWN-1	0,4%	60,6%	95,3%

UNIVERSITÄT MANNHEIM
Zinaida Benenson, Michael Heinold, Felix Freiling
{benenson, heinold, freiling}@uni-mannheim.de
Dependable Distributed Systems, University of Mannheim

ZeuS LANDESSTIFTUNG Baden-Württemberg
This work is part of the "ZeuS" research project funded by "Landesstiftung Baden-Württemberg", Germany.

Joachim Wilke, Benno Evers, Martina Zitterbart
{wilke, evers, zit}@tm.uka.de
Insitute of Telematics, Universität Karlsruhe (TH)
Universität Karlsruhe (TH)
Research University · founded 1825