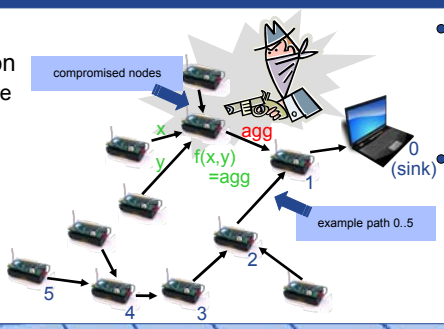
ESAWN-NR – Authentic Aggregation and Non-Repudiation in Wireless Sensor Networks

Motivation & Contribution

- Assumptions
  - In-network processing / data aggregation
    - Average of **δ** nodes send data to the same parent
    - Only leaf nodes take measurements
  - Strong attacker model
    - Adversary gains possibly physical access to a fraction of at most **β**% of all **n** nodes
  - Key distribution
    - Nodes communicating own pairwise symmetric keys



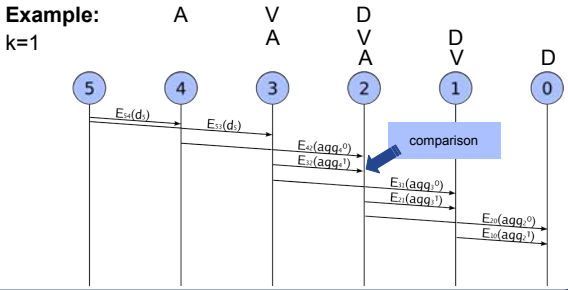
- Idea
  - Trade-off security and energy
    - Using a configurable parameter (**k**)
  - Probabilistic security guarantees
- Contributions of this work
  - **ESAWN** guarantees authenticity of aggregates with at least **P**% using symmetric cryptography
  - **P** depends on
    - network parameters **n**, **β**, **δ**
    - user configurable parameter **k**

Extended Secure Aggregation for Wireless Sensor Networks (ESAWN)

- Aggregates are checked to assert authenticity
  - Each aggregate sent by an aggregating node (A) is verified by several predecessors (V)
  - The following node (D) compares the aggregates and decides how to proceed
  - Authenticity is established by following this scheme inductively
- Three protocol variants with different behavior towards compromised nodes

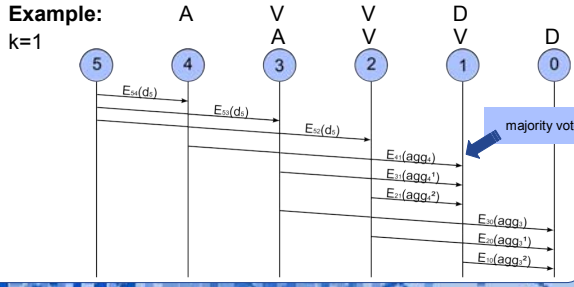
ESAWN-1 (detection)

- Aggregating node A and its **k** predecessors (V) send data to **k+1** predecessor (D)
- The following node (D) compares the aggregates
- → Compromised aggregates get detected. Run is stopped if comparison fails.



ESAWN-2 (compensation)

- Aggregating node A and its **2k** predecessors (V) send data to **2k+1** predecessor (D)
- This node (D) resolves correct aggregate using a majority vote on all received aggregates
- → Compromised aggregates get compensated.



ESAWN-NR (compensation & notification)

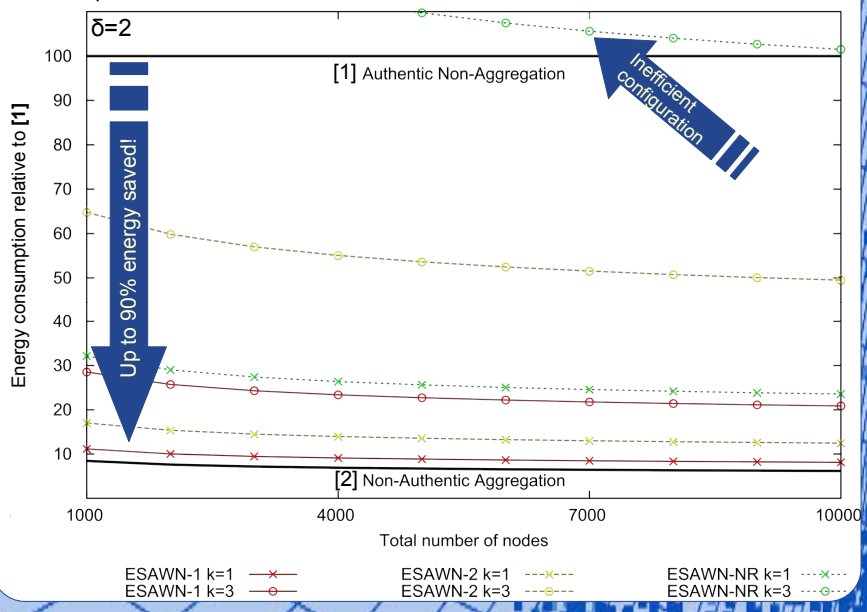
- Aggregation and majority vote as with ESAWN-2
- Forwarding of data packets is modified, such that all predecessors log each others messages. Sent packages cannot repudiated
- → If comparison fails, other nodes are notified of this incident. Disclosing its communication keys enables the node (D) to prove its report.

Demo

Evaluation

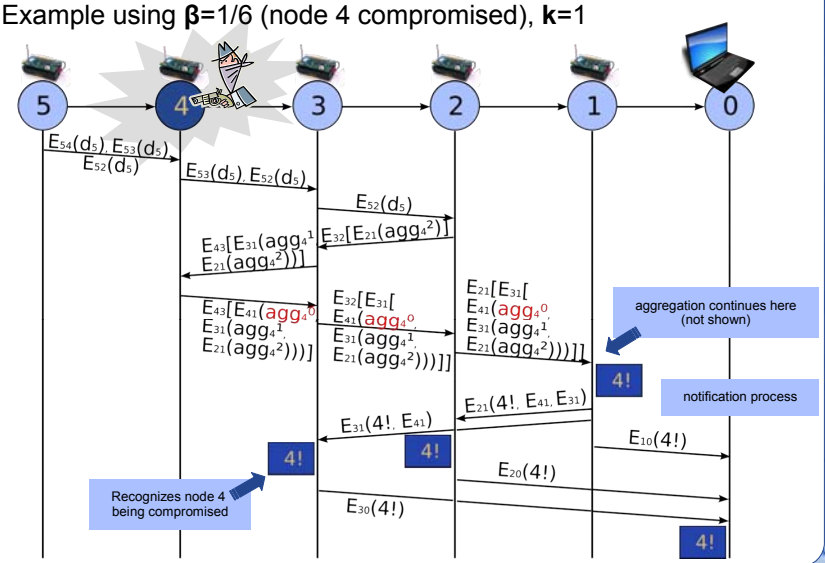
- Comparison of ESAWN's energy consumption in contrast to
  [1] Non-Authentic Aggregation (no authenticity, lowest energy consumption) **P=0%**
  [2] Authentic Non-Aggregation (full authenticity, not energy efficient) **P=100%**
- Simulative results
  - of authenticity probability **P** *(right)*
  - of energy consumption *(below)*
    - Reference platform: Mica2/TinyOS
  - Shows Security/Energy Trade-Off by choosing **k** and protocol-variant

δ=2	compromised nodes	k=	1	2	3
Probability P of authentic aggregation	β=1%	ESAWN-1	94,6%	99,9%	100,0%
		ESAWN-2 ESAWN-NR	89,5%	99,7%	100,0%
	β=10%	ESAWN-1	0,4%	60,6%	95,3%
		ESAWN-2 ESAWN-NR	0,1%	13,7%	60,1%



ESAWN-NR Demo

- Example using **β**=1/6 (node 4 compromised), **k**=1



Dipl.-Inform. Joachim Wilke, Dr. Erik-Oliver Blaß, Prof. Dr. Martina Zitterbart

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

Institute of Telematics
www.tm.uka.de
Universität Karlsruhe (TH)
Research University · founded 1825