Distributed Software-based Attestation for Node Compromise Detection in Sensor Networks

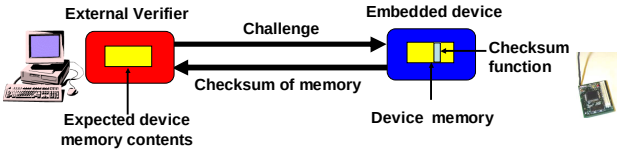
Yi Yang, Xinran Wang, Sencun Zhu, Guohong Cao

Node Compromises in Sensor Networks

- ✓ **Sensor Networks**
  - ❖ **Functions**
    - **Sensing**
    - **In-network Processing**
    - **Ad-hoc Communication**
  - ❖ **Applications**
    - **Military Surveillance**
    - **Homeland Security**

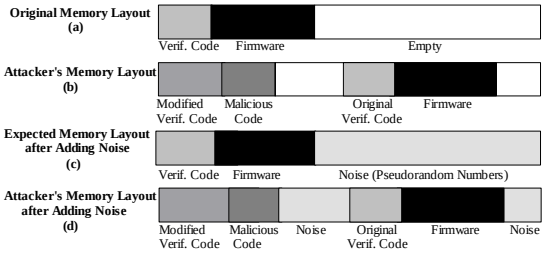
- ✓ **Node Compromises**
  - ❖ **Unattended, harsh, hostile environment**
  - ❖ **Temper-resistant hardware is expensive**
  - ❖ **Insider attacks become possible**
  - ❖ **Behavior-based detections are error-prone**

Current solutions and their limitations



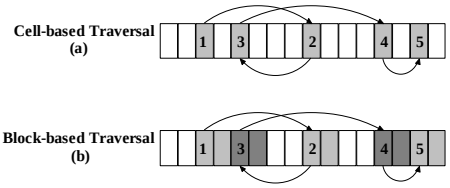
- ❖ **Millions of checksum computations to generate distinguishable time difference**
- ❖ **Untrustworthy mobile verifier to enter sensor's transmission range**
- ❖ **Remote attestation from BS can be affected by network channel collision and multi-hop distance**

Our Solutions – Distributed Software-based Attestation

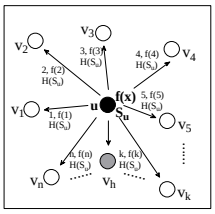


Pseudorandom noise injection

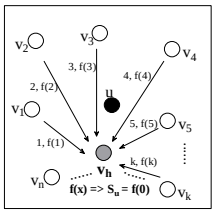
Block-based memory traversal



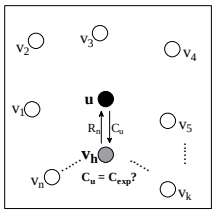
Scheme I: Threshold Secret Sharing



Share Distribution

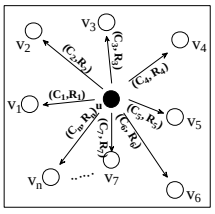


Seed Recovery

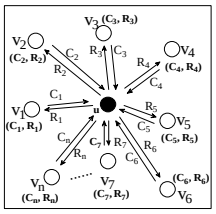


Attestation

Scheme II: Majority Voting



Information Distribution



Attestation

Security Analysis and Performance Evaluation

SECURITY COMPARISON OF OUR SCHEMES

	Detection Rate	False Positive	Attacker Reward	Eavesdrop	Replay	Message Dropping	Compromised Neighbors
Scheme I	High	Low	Low	Yes	Yes	No	Yes, except to compromised cluster head
Scheme II	Higher	Lower	Lower	Yes	Yes	Yes	Yes

Notations: Yes - the scheme can defend against this attack;
No - the scheme is vulnerable to this attack.

- ❖ **Prototype Implementation**
  - ❖ **ROM space: 21KB out of 128KB program memory**
  - ❖ **RAM space: 1KB out of 4KB data memory**