LEDS: Providing Location-aware End-to-end Data Security in Wireless Sensor Networks

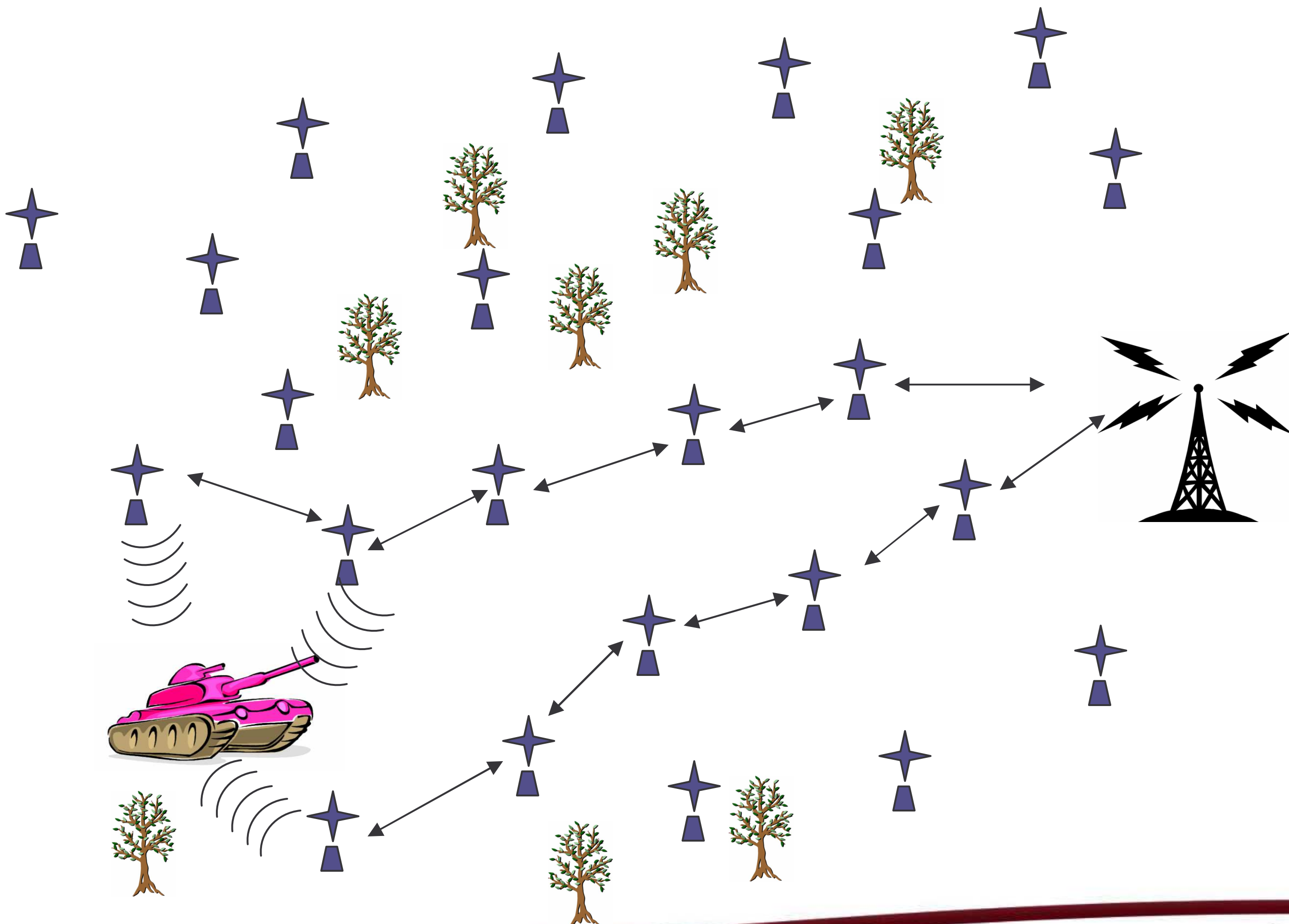
Kui Ren, Wenjing Lou
Worcester Polytechnic Institute

Yanchao Zhang
University of Florida

Introduction: Wireless Sensor Networks

- A wireless sensor network (WSN) is composed of a large number of sensor nodes
- Sensor nodes are typically small, low-cost, low-power devices
- Sensor nodes perform the following functionality:
  - Sense/monitor its local environment
  - Perform limited data processing
  - Communicate on short distance
- A WSN usually also contains a “sink” node(s) which collects data from sensor nodes and connects the WSN to the outside world
- Various sensing tasks
  - military sensing and tracking, remote sensing in hazardous venues, real time traffic monitoring, real time weather monitoring, wild animal monitoring and tracking, fire/flood detection, inventory control, etc.

An Exemplary WSN



Security issues in WSN

- Many applications in WSNs require communication to be highly secure
- Main security challenges:
  - Sensor nodes are resource constrained – computation, memory, communication bandwidth, energy, etc.
  - Sensor nodes are not temper resistant, are subject to compromise
  - Radio link makes attack easier – eavesdropping / false data injection, etc.
- General design guidelines
  - Lightweight: lightweight cryptographic tools, efficient protocol design for communication and storage efficiency
  - Resilient: be resilient against compromised nodes
  - Scalable: de-centralized, localized protocol

Related Work

- Statistical En-route Filtering (SEF) – Ye, Luo, Lu, and Zhang, *INFOCOM* 2004
- Interleaved Hop-by-Hop Authentication (IHA)
  - Zhu, Setia, Jojodia, Ning, *IEEE S&P* 2004
- Resilient Security – Yang, Ye, Yuan, Lu, and Arbaugh, *ACM Mobihoc* 2005

Vulnerable to report disruption attack and selective forwarding attack !

- Location-based Compromise-tolerant Security
  - Zhang, Liu, Lou, and Fang, *IEEE JSAC*, Feb 2006

Based on ID-based public key cryptography.

End-to-end Data Security

- Hop-by-hop vs. End-to-end
- Data Confidentiality
  - Intermediate relaying nodes should not read the event reports to the sink: end-to-end encryption
- Data Authenticity
  - The message has not been altered during the transmission: MAC.
  - It was indeed from the claimed source: collaborative endorsement.
- Data Availability
  - Resilient to selective forwarding attack and report disruption attack: one-to-many forwarding, secret sharing
  - In-network false data filtering: interleaved hop-by-hop filtering

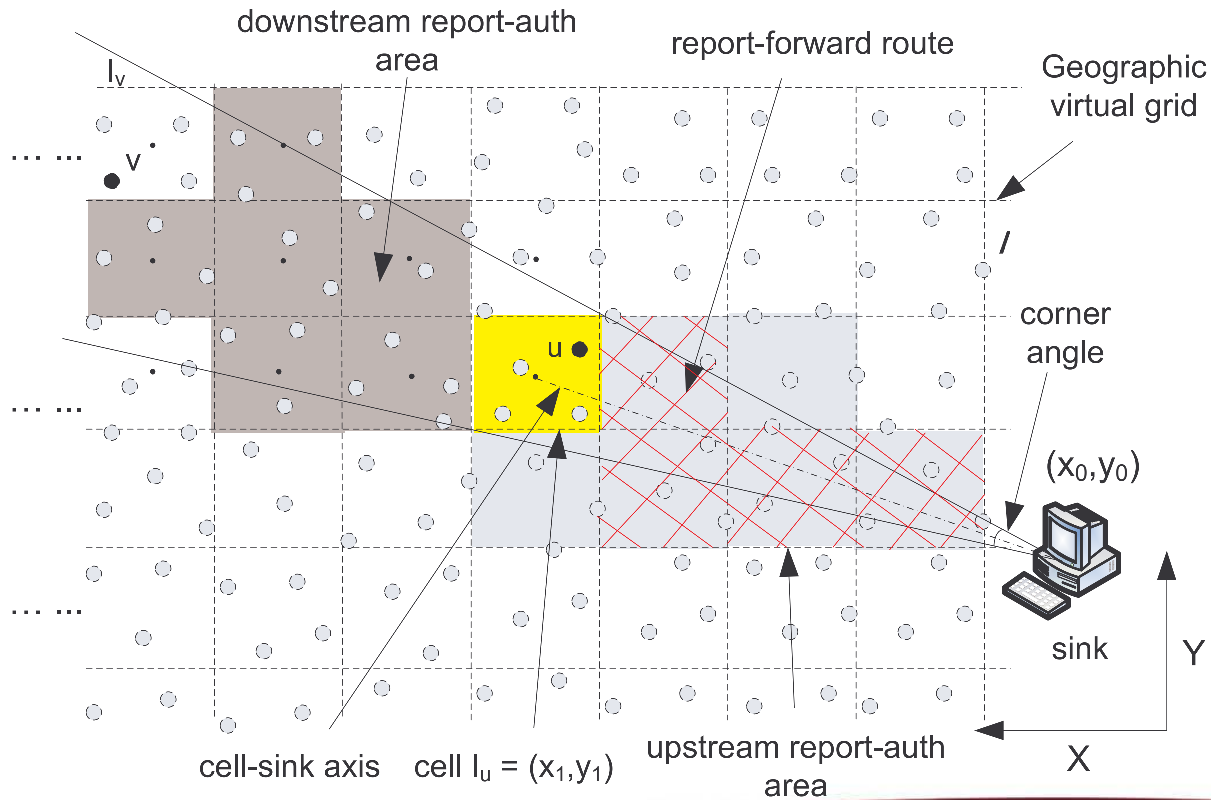
LEDS: Two Observations

- Stationary and location-awareness
  - Many WSN applications require sensor nodes be aware of their locations.
  - It is not difficult for each node to know its location and their neighbors' locations -- GPS based, GPS-free, sensor self-positioning algorithms, etc..
- Communication pattern
  - one-to-many: sink-to-node broadcast
  - many-to-one: node-to-sink data collection

WPI

LEDS: Cell-based geographic routing

- Geographic routing – No routing overhead
- Predictable routes
- One-to-many forwarding scheme – more resilient to node failure and compromise



LEDS: Location-aware key management framework

- System Secret K_M^I, K_M^{II}
- Each node computes a set of keys
  - Unique secret key $K_u^1 = H(K_M^I|u|I_u|0), \quad K_u^2 = H(K_M^I|u|I_u|1)$
  - Cell key shared among all the nodes in the cell: $K_{I_u} = H(K_M^I|I_u)$
  - Authentication keys shared with nodes along the routing path $H(K_M^{II}|(x_1, y_1)|(x_c, y_c))$
- Dynamic node addition
  - Nodes delete system secret but keep: $SK_u = H(K_M^{II}|I_u)$
  - New addition: $K_{I_u, I_w} = H(H(K_M^{II}|I_u)|I_w)$

Location information is embedded into each node's cryptographic keys. The damage caused by compromised nodes is minimized – a compromised node cannot launch attacks at locations other than where it actually is.

LEDS: End-to-end data security mechanism

- Local communication is protected by the cell key
- A data report is encrypted by the cell key
- Each participating node contributes a share of the encrypted data report

$$C_u = \mathcal{F}(K_u^1, K_u^2) = \sum_{0 \le i \le t-2} a_i (K_u^1)^{i+1} + a_{t-1}(K_u^2)^t \bmod p,$$

- Each node contributes a MAC for interleaved cell-by-cell false data filtering
  - Computation of authentication keys: If I_u is an upstream (closer to sink) cell of I_v , every node in I_u has the authentication key K_{I_u,I_v} with at least one node in I_v ; if the two cells are exactly i+1 cells away , every node in I_u shares the authentication key with every node in I_v
- Sink does the final verification

LEDS: An example

Formed at node m

$$\{I_u, m, s, u, C_m, C_s, C_u, Mac_{K_{I_u,I_v}}(C_m|C_s|C_u), Mac_{K_{I_u,I_z}}(C_m|C_s|C_u), Mac_{K_{I_u,I_o}}(C_m|C_s|C_u), Mac_{K_{I_u,I_{v'}}}(C_m|C_s|C_u)\}.$$

Sent at node v

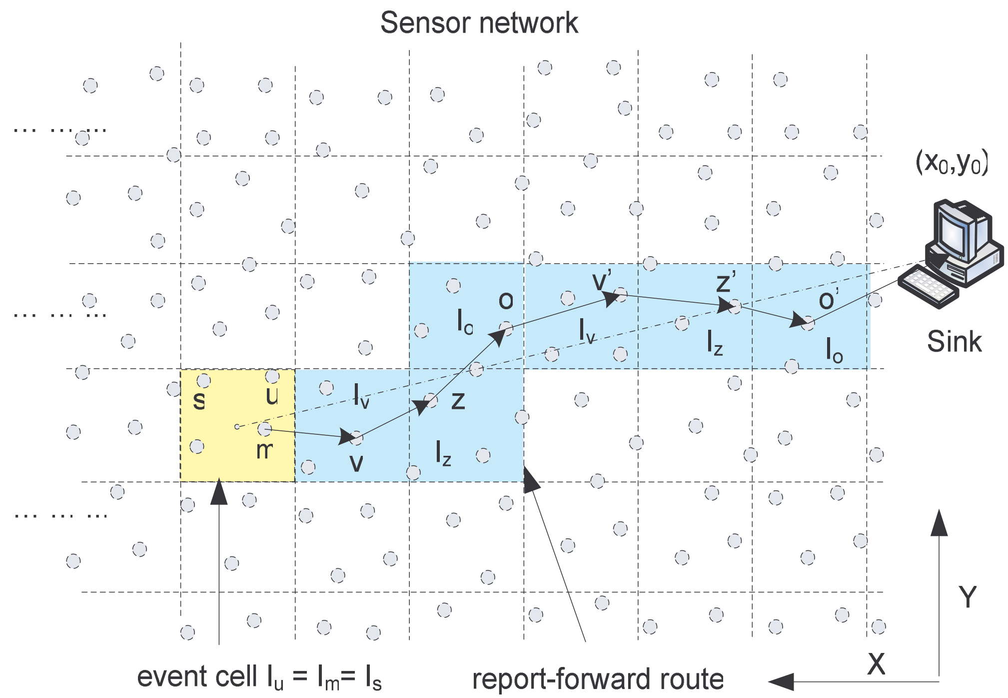
$$\{I_u, m, s, u, C_m, C_s, C_u, Mac_{K_{I_u,I_z}}(C_m|C_s|C_u), Mac_{K_{I_u,I_o}}(C_m|C_s|C_u), Mac_{K_{I_u,I_{v'}}}(C_m|C_s|C_u), Mac_{K_{I_v,I_{z'}}}(C_m|C_s|C_u)\}.$$

Received at node z'

$$\{I_u, m, s, u, C_m, C_s, C_u, Mac_{K_{I_v,I_{z'}}}(C_m|C_s|C_u), Mac_{K_{I_z,I_{o'}}}(C_m|C_s|C_u), Mac_{K_{I_o,sink}}(C_m|C_s|C_u), Mac_{K_{I_{v'},sink}}(C_m|C_s|C_u)\}.$$

Received at sink

$$\{I_u, m, s, u, C_m, C_s, C_u, Mac_{K_{I_o,sink}}(C_m|C_s|C_u), Mac_{K_{I_{v'},sink}}(C_m|C_s|C_u), Mac_{K_{I_{z'},sink}}(C_m|C_s|C_u) Mac_{K_{I_{o'},sink}}(C_m|C_s|C_u)\}.$$



Security Analysis: Data Confidentiality

- End-to-end encryption: the confidentiality of a data report is compromised only when at least one node in the event cell is compromised.

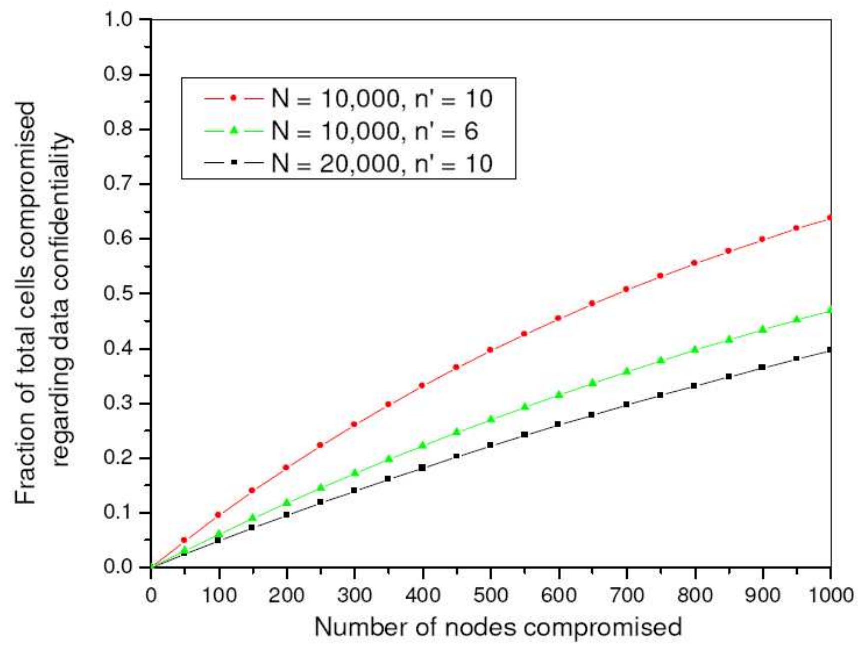


Fig. 4. Data confidentiality in LEDS under random node capture attacks

Security Analysis: Data Authenticity (1)

- Adversaries have to compromise at least *t* nodes in a single cell to fabricate a data report associated with that cell.

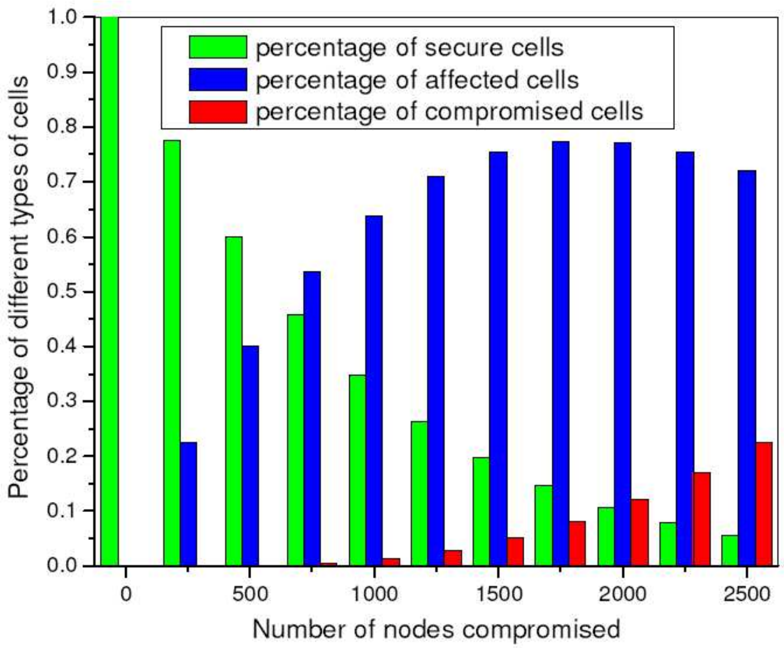


Fig. 5. Data authenticity in LEDS under random node capture attacks, where $N = 10,000$, $n' = 10$ and $(t, T) = (4, 5)$.

Security Analysis: Data Authenticity (2)

- High efficiency in false data filtering due to deterministic cell-by-cell en-route filtering

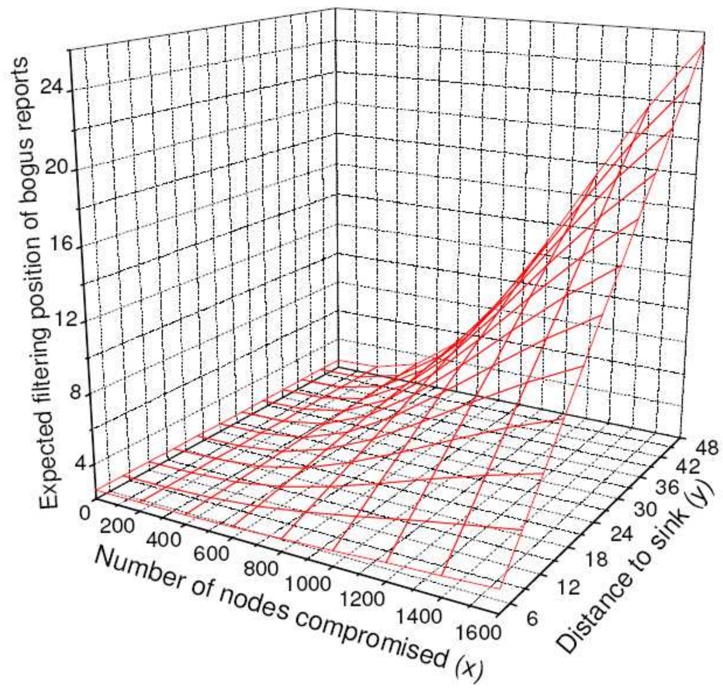


Fig. 6. Expected filtering position vs. number of compromised nodes with respect to different distances to the sink

Security Analysis: Data Availability (1)

- One-to-many forwarding to defend against selective forwarding attack

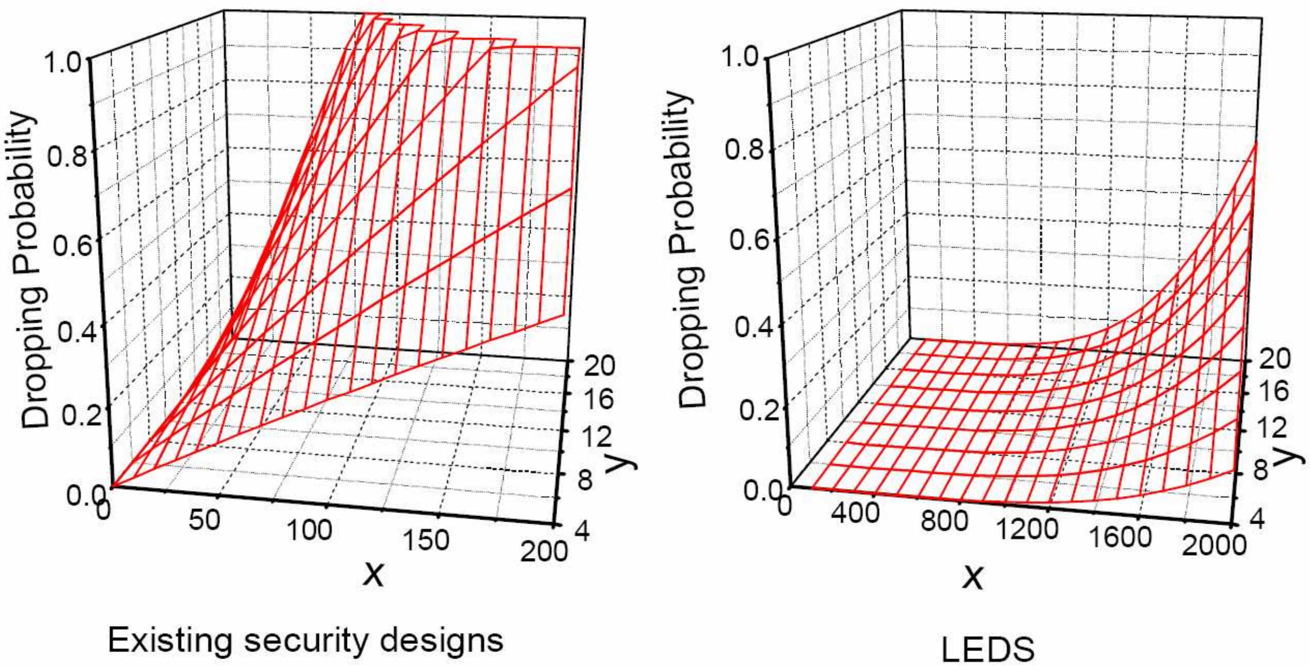


Fig. 8. Data availability in LEDS under selective forwarding attack

Security Analysis: Data Availability (2)

- Threshold secret sharing to defend against report disruption attack

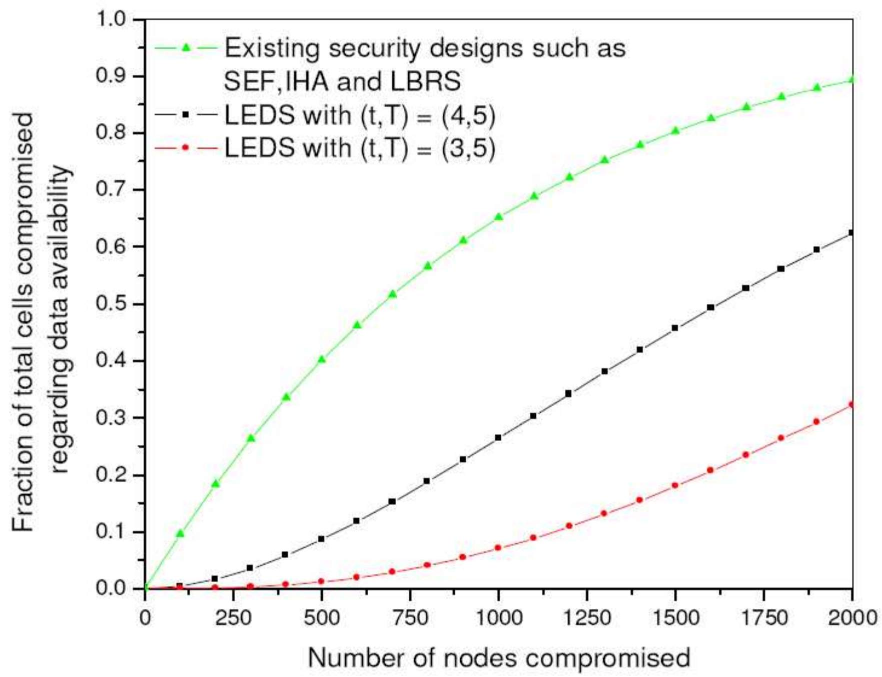
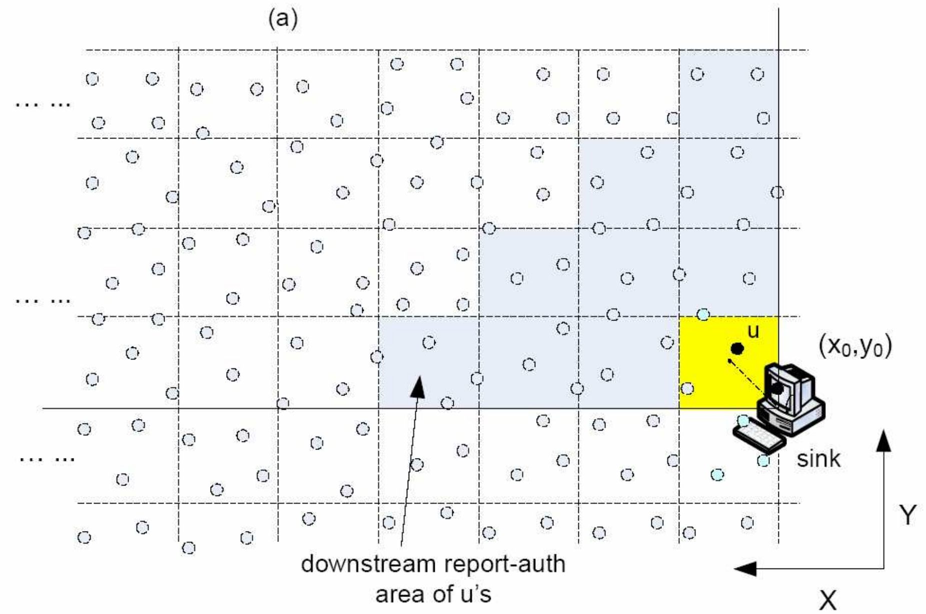


Fig. 7. Data availability in LEDS under report disruption attack

Performance Analysis

- Key storage overhead:
  - 2 unique keys
  - 1 cell key
  - 2 upstream authentication keys
  - Less than (T+1)(T+2)/2 downstream authentication keys
  - 1 half-key to accommodate node addition



- LEDS is also both communication- and computation-efficient
  - localized and independent key generation
  - based on symmetric key cryptography.

Conclusion

- We introduced a novel methodology of key establishment, which takes advantage of location awareness and communication pattern of a WSN.
- We designed LEDS, a lightweight, resilient and highly scalable end-to-end data security solution.
- WSNs are typically task or application specific, customized solutions might be the way to optimize the performance !

Thanks!

Questions?