How to Transmit Messages via WSN in a Hostile Environment

Michał Koza, Marek Klonowski and Mirosław Kutyłowski
Institute of Mathematics and Computer Science, Wroclaw University of Technology, POLAND
Politechnika Wrocławska

Introduction

- Model
  - wireless sensor network
  - multi-hop
  - severely constrained devices
- Goal
  - providing confidentiality of transmitted message
- Problems
  - devices can be captured by adversary
  - all secrets stored can be accessed easily
- Solution
  - message partition
  - routing algorithm
  - adversary needs to capture specific subset of nodes to learn the message

Model

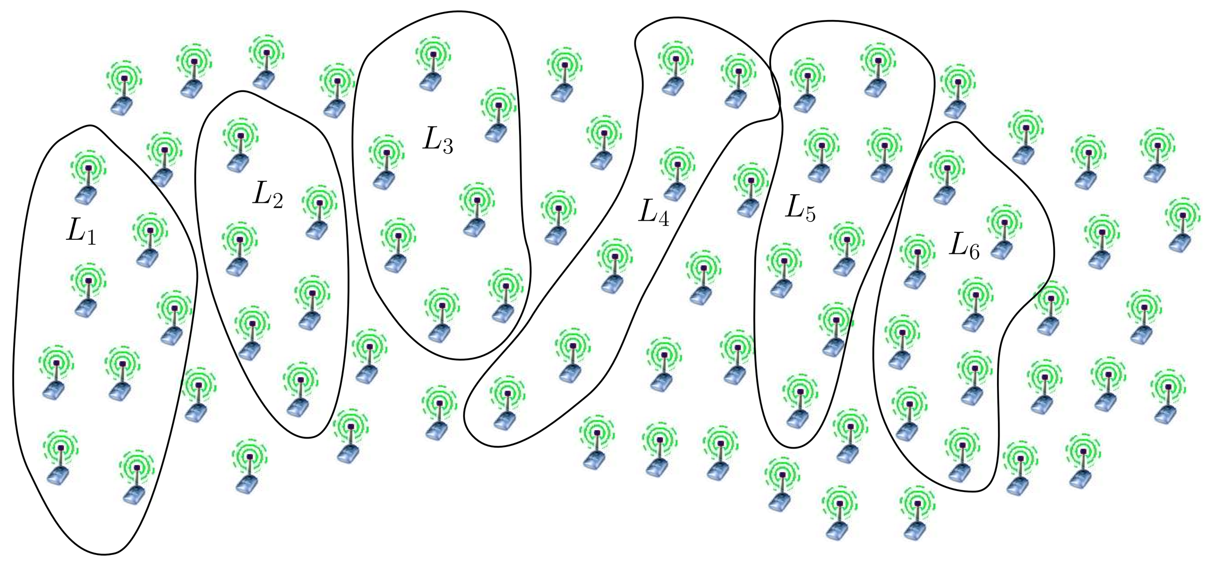

Figure: Exemplary distribution of nodes and layers

- layered structure (possibly constructed ad-hoc)
  - $L_1, L_2, \ldots, L_t$
  - assuming no overlaps
  - assuming n devices in each layer
- each pair of nodes in consecutive layers share a symmetric key
- nodes in consecutive layers are in transmission range of each other

Adversary

- wants to learn the message transmitted through the network
- can capture some devices
- can eavesdrop communication in the network
- can retrieve all information stored on captured device

Protocol

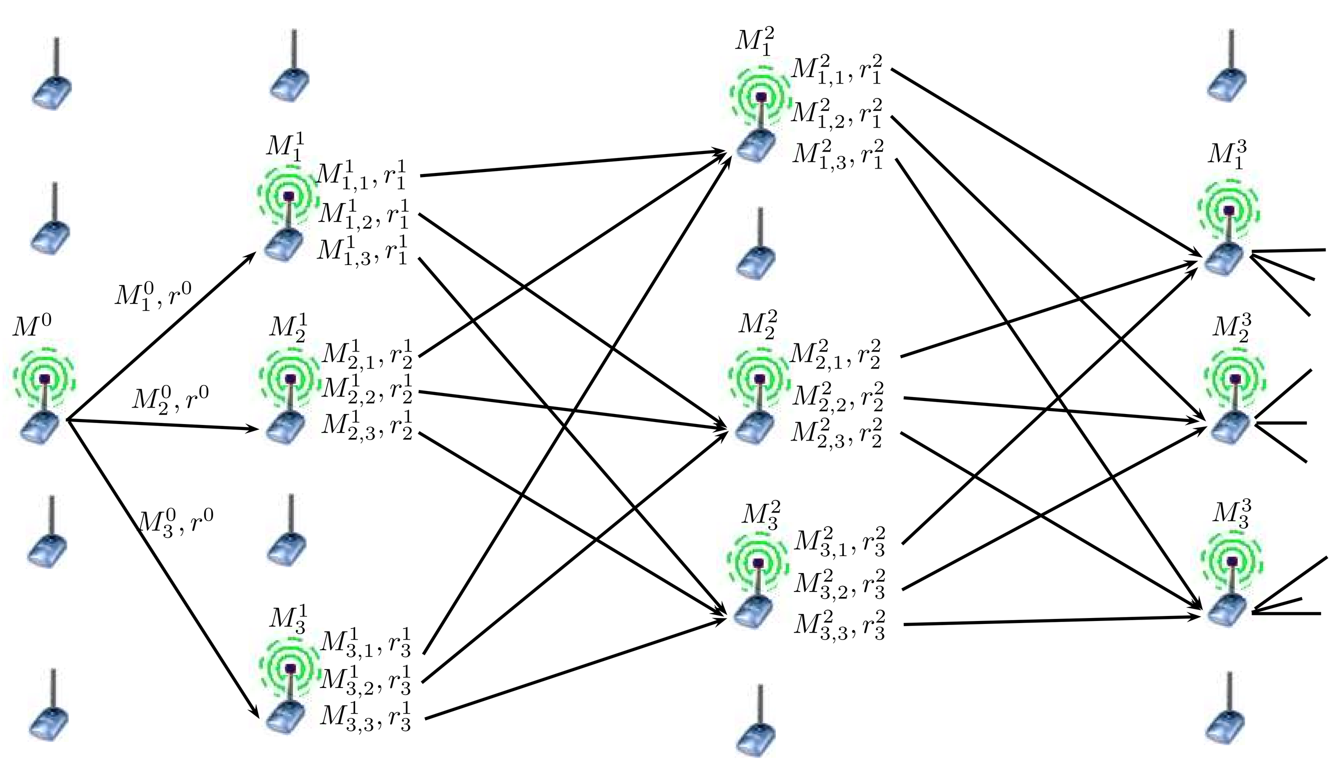

Figure: Exemplary protocol execution for one message and $l = 3$

- standard XOR-based secret sharing is employed
- at each layer, a subset of l nodes participates in message M transmission
  - l is a protocol (forking) parameter
- there are l^2 message parts traveling between consecutive layers
- in order to learn the message adversary needs to capture **all** l devices at one layer
- informations learned at one layer does not help at other layers

Protocol: Message Partition

- Initialization
  - source splits M into l parts, and sends them to l nodes in next layer
- Step
  - each of l devices splits the message part again into l parts and sends them to l devices in next layer
  - each device choose the same l devices to sent the message to (See **Routing).**
- at each layer, a subset of l nodes participates in message M transmission
  - l is a protocol (forking) parameter
- there are l^2 message parts traveling between each layer

Protocol: Routing

- Initialization
  - source chooses r at random and sends it to l devices in next layer
  - the devices basing on r determine set of receivers in next layer
- Step
  - each device generates new random value r' and sends it along with its l message parts
  - each device in the following layer has the same set of l r' and can determine receivers in next layer

Attack scenarios

It is assumed that adversary can capture up to K devices.

- Nonadaptive Attack
  - Adversary chooses devices before transmission
- Random Attack
  - Adversary chooses devices at random (e.g. trying to locate them in grass)
- Adaptive attack
  - Nodes chosen after transmission

Security analysis

- Nonadaptive Attack
  - It is optimal for the adversary to choose devices from one layer
  - **Theorem** Corrupting nodes from one layer adversary chance for learning the message for $l \le K < n$ is $\binom{K}{l} / \binom{n}{l}$
- Random Attack
  - **Theorem** Chance for learning the message is $S_n = \sum_{i=1}^{t} (-1)^{i+1} \binom{t}{i} \frac{(K^{il})_+}{L^{il}} < \cdot \frac{1}{2} \left(\left(1 + \frac{1}{t}\right)^t - \left(1 - \frac{1}{t}\right)^t \right)$
- Adaptive attack
  - Attack when single message is transmitted is trivial
  - For N messages going simultaneously we have the following **Theorem** For $\log\left(\binom{n}{K} N\right) < Np$ following relation holds: $\Pr\left[MAX_{n,K} \ge Np + 1.5\sqrt{N \log\left(\binom{n}{K} N\right) p} \right] \le \frac{1}{N}$. Where $MAX_{n,K}$ denotes number of learned messages and $p = \binom{K}{l} / \binom{n}{l}$

Summary and Extensions

- Secret sharing can employ some error correcting codes to improve robustness
- MAC sum can be attached in order to prevent modifications of transmitted message
- Parameter l is a trade-off between security and communication complexity.
- l^2 is not much as even $l = 2$ is significant security improvement