Distributed Trust Management and Revocation:Voting Strategies and Consensus

Dmitriy Kuptsov, Oscar-Garcia Morchon, Klaus Wehrle, Andrei Gurtov

dmitriy.kuptsov@hiit.fi, oscar.garcia@philips.com, klaus.wehrle@cs.rwth-aachen.de, gurtov@hiit.fi

Cooperative security

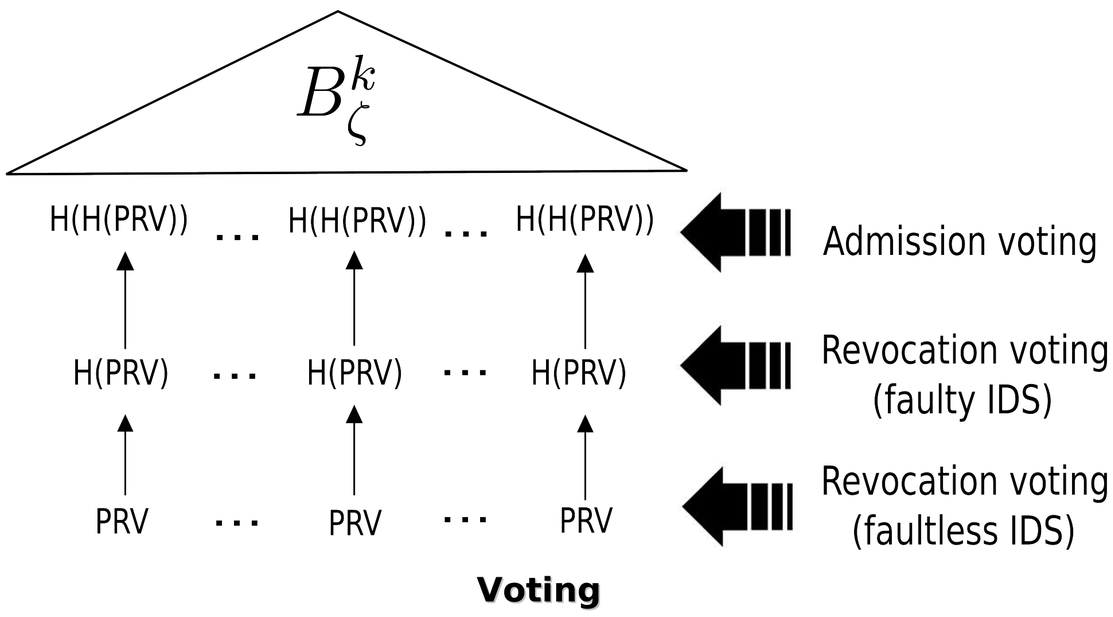
Consider a network comprising **n** nodes, in which arbitrary nodes are subjects to **failures** caused by an adversary**.** The protocol designed around the concepts of cooperative security, due to Garcia et al.[1], allows a group of nodes to isolate such nodes from the network. Accordingly, the contributions of this work are (i) efficient keying material structure, and (ii) the voting strategies, whereas both allow the reduced memory and communication complexity, as well as increased overall system security

Protocol operation

Each node in the network carries a set of secret information – partial revocation votes **(PRV)** – disclosure of which to its neighbors is mandatory to join the network. After the disclosure of PRVs a set of neighbors vote to agree on node's admission and if succeed they form a node's Dynamic Trusted Security Domain **(DTSD)** – and continue to monitor node's behavior. If a node becomes suspicious the DTSD starts voting for revocation. And if nodes agree, i.e., sufficient number of PRVs revealed, a DTSD can reconstruct a network wide revocation vote **(RV)** and further isolate a node from the whole network**.**

Keying material

Keying material comprises three Merkle trees (i) Global tree **(GNRVT)** – authenticates node identities; root element is shared between all nodes (ii) **re-keying tree** – unique to a particular node and mapped to a corresponding leaf in the GNRVT; allows communication session authentication, and (iii) **revocation session tree** – authenticates PRVs and RV of a particular node which we present in figure below. PRVs are shares generated from a polynomial and allow RV reconstruction following Shamir's algorithm.

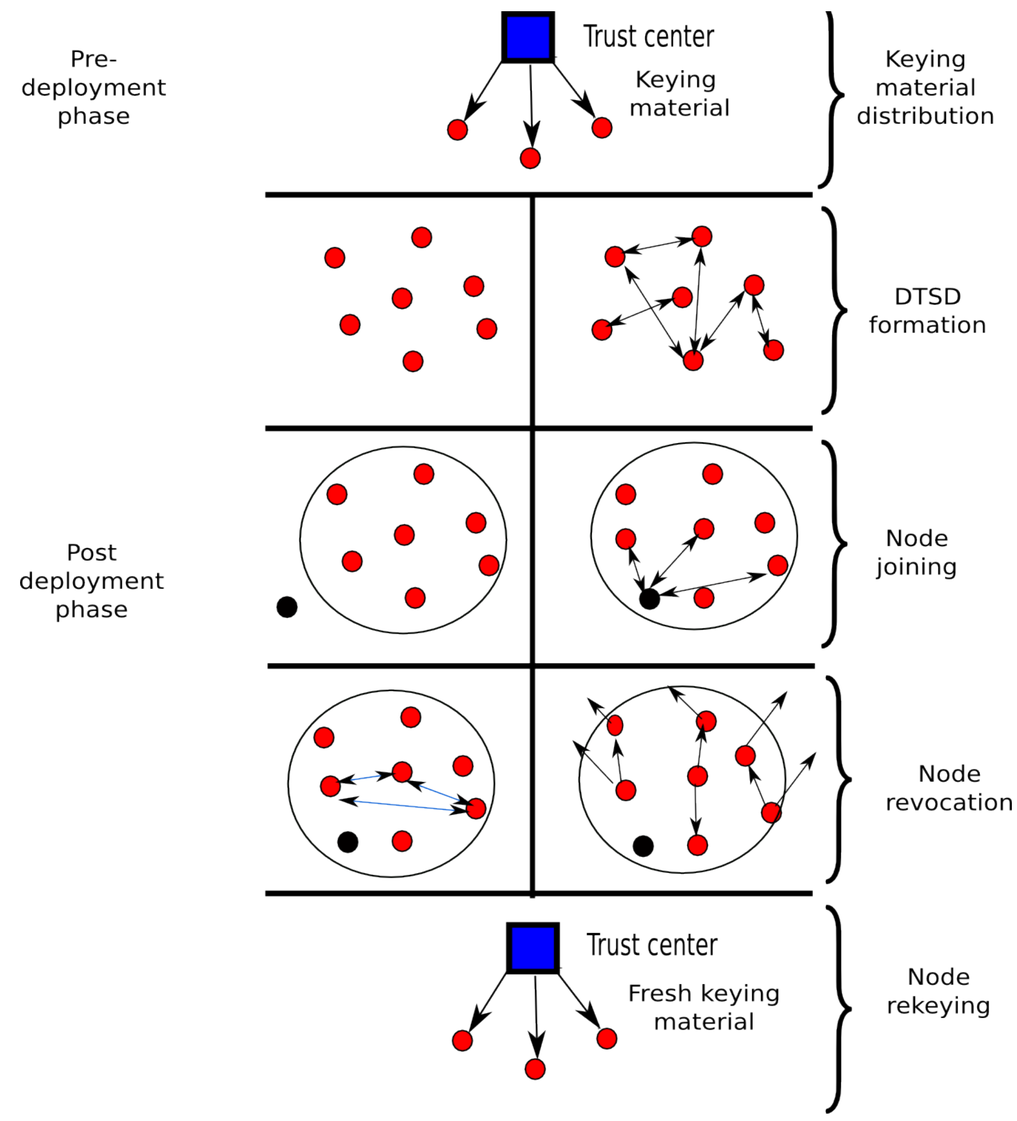


Voting

Voting is an essential part of the protocol. Voting allows reaching consensus during node admission and revocation. Two voting strategies are possible: (i) **Yes/No voting** – a type of Binary Byzantine Agreement and (ii) **Verifiable Broadcast** – direct disclosure of PRVs or its hash – allows to reduce communication complexity when compared to Yes/No voting

Model definition

- Failure-free atomic broadcast communication
- Cryptographic identity authentication
- Honest nodes always comply the protocol and don't delay messages
- The revocation decisions are triggered by intrusion detection algorithm **(IDS)**, which can be: (i) faulty – no false-negatives, but false-positives are possible with a small probability (ii) ideal – no false-positives nor false-negatives are possible



Analysis

When number of nodes in a DTSD is **3t+1** and IDS is non-faulty, the protocol is t-resilient, e.g., can sustain **33%** of faulty nodes. A protocol is still t-resilient with probability following binomial distribution if IDS is faulty. The protocol is adaptive regarding the number of nodes in a DTSD – needed requirement for real-life applications

[1] Garcia-Morchon, O., Baldus, H., Heer, T., Wehrle, K.: Cooperative Security in Distributed Sensor Networks, Proceedings of the 3rd International Conference on Collaborative Computing, pp. 96-105, 2007