HolA: Holistic and Autonomous Attestation for IoT Networks

Alessandro Visintin[1], Flavio Toffalini[2,3], Eleonora Losiouk[1]
Mauro Conti[1], Jianying Zhou[2]

[1] University of Padua, Padua IT
[2] SUTD, Singapore SG
[3] EPFL, Lausanne CH

June, 23th 2022 - Rome

AIoTS Workshop @ ACNS 2022

Attestation.

The activity of making a claim about properties of a **prover** by supplying evidence to a **verifier**.

Remote attestation.

The activity of making a claim about properties of a **prover** by supplying evidence to a **REMOTE verifier**.

Collective Remote attestation (CRA).

SANA - Ambrosin, et al. (2016) Sana: Secure and scalable aggregate network attestation

SCAPI - Kohnhauser, et al. (2017) Scapi: A scalable attestation protocol to detect software and physical attacks

PASTA - Kohnhauser, et al. (2019) A practical attestation protocol for autonomous embedded systems

CRA operates on mesh networks.

Mesh-like networks enables only physical neighbours to communicate with each other.

Mesh-like networks do not consider intermediate machinery (e.g., switches, routers)

Current CRA do not consider Internet-like networks.

6LoWPAN - Shelby, et al. (2011) 6LoWPAN: The wireless embedded Internet

Thread - Group, T.: Thread, https://www.threadgroup.org/

Introducing HolA

Neighbourhood attestation - how do you define logical neighbours?

Absence detection - how do you detect physical attackers?

Network obfuscation - how do you hide the topology and operations of the network?

Chord protocol

Stoica, et al (2003) Chord: a scalable peer-to-peer lookup protocol for internet applications

Zave, P. (2012). Using lightweight modeling to understand Chord

Chord protocol

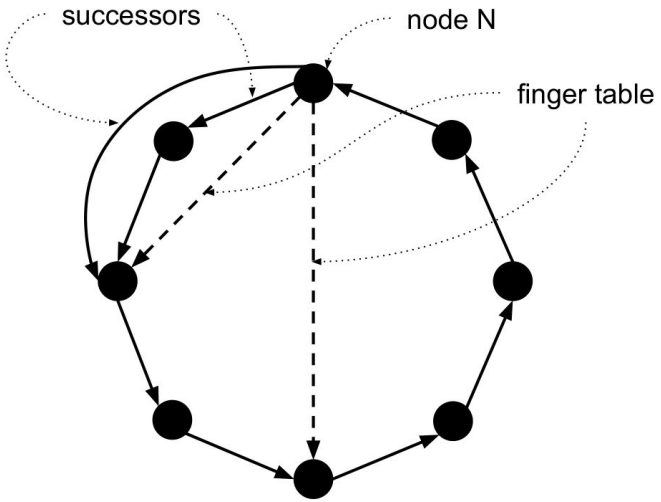


Table 1: Main components of the HolA devices.

Data Structure	Short Description
successors list	list of the direct successors of a device
finger table	list of intermediate devices in the network
`nodeId`	a progressive unique number that identifies a device in the network
`pubKey/privKey`	keys used for issuing secure communication channels.
`cert`	a certificate representing the device identity
`pubCAKey`	the CA `pubKey` used for certificate validation
`Status List (SL)`	a structure containing the status of each device in the network
`verifySF()`	function to ascertain the healthy status of a device
`role`	the privilege of a device

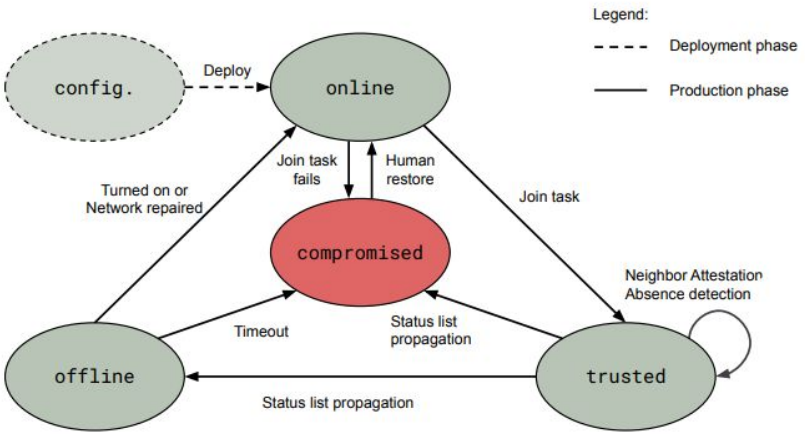


Fig. 1: Lifecycle of a network node deployed in the HolA CRA scheme.

Experimental setup

Raspberry Pi 0 - estimate the cost of cryptographic operations.

Raspberry Pi 3 - feasibility assessment with a network of 5 devices.

Network simulation - evaluate the performances in large networks.

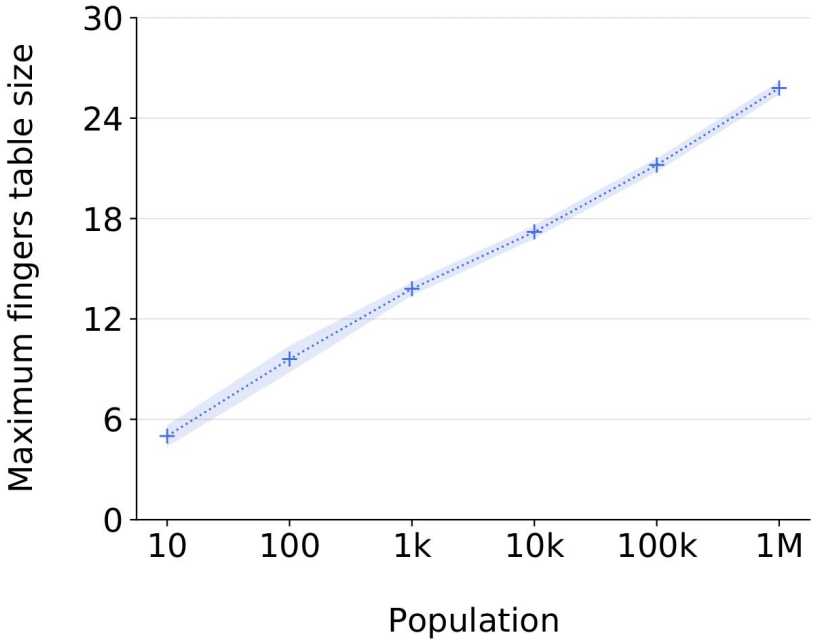
Security properties

Theorem 1 - Neighbourhood attestation guarantees continuous check of nodes.

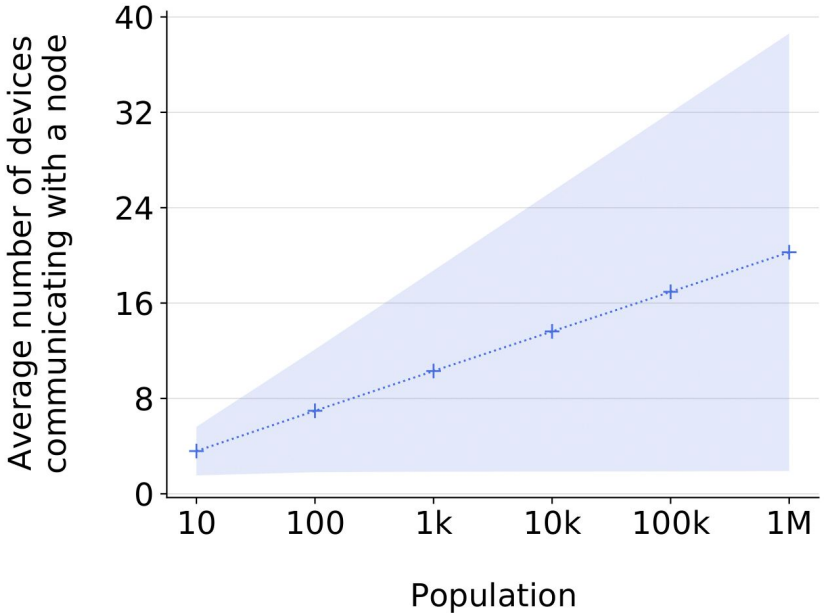
Theorem 2 - Absence detection guarantees the detection of offline nodes.

Theorem 3 - Status list propagation reaches all online devices.

Finger table size



Communicating nodes



Node memory usage

successor list - (132 x SLEN) B
finger table - (132 x $\log_2(N)$) B
Status list - (10 x N) B
cache (opt.) - (130 x $\log_2(N)$) B

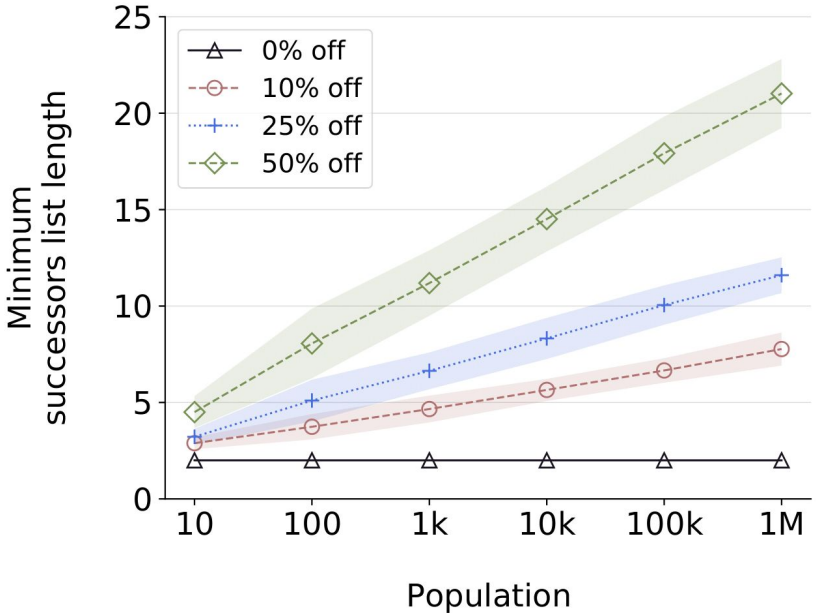
Comparing against PASTA (10k nodes), HolA is seven times lighter (105kB vs 700kB).

Communication overhead

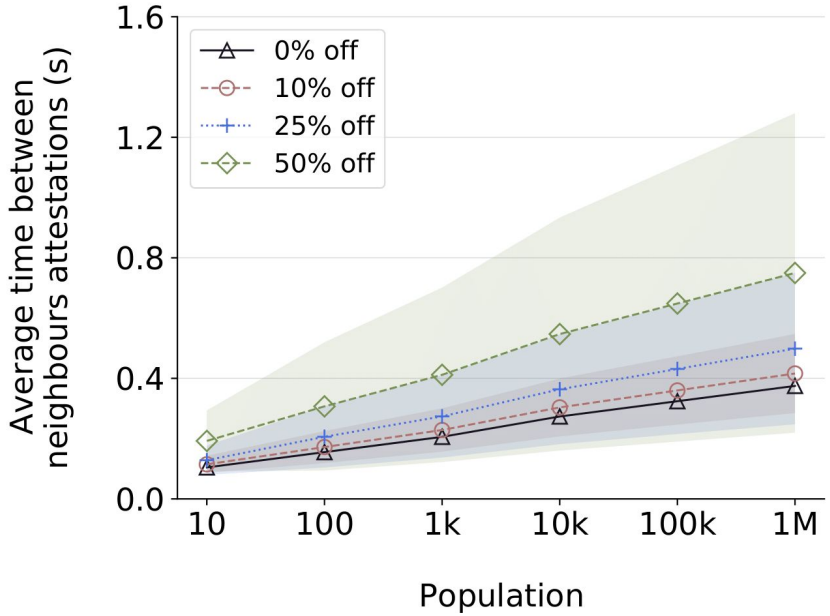
operational messages - 264×(SLEN +1)) B

In a network of 10k nodes, HolA operational messages are 3960 B. This is the same order of magnitude of PASTA and SCAPI (1341 B).

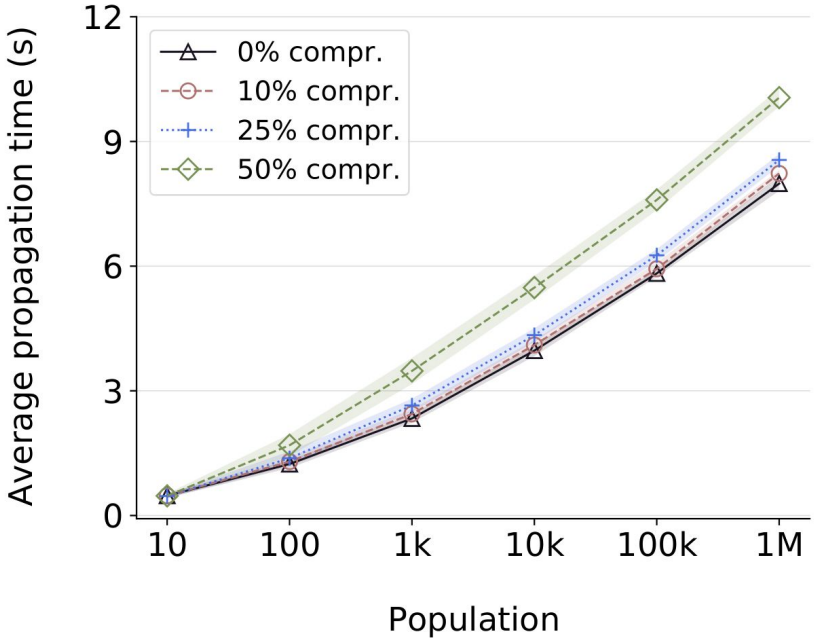
Resiliency


0% off
10% off
25% off
50% off
Minimum successors list length
0
5
10
15
20
25
10
100
1k
10k
100k
1M
Population

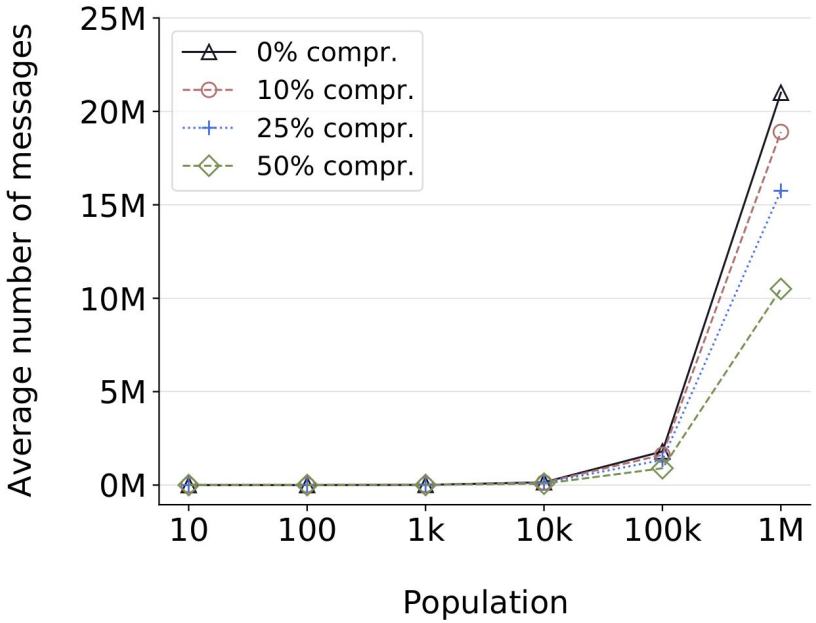
Time Delay for Neighbourhood Attestation



Status list propagation



Status list propagation



Discussion

Certificate revocation/expiration - trade-off between precise and probabilistic solutions

False positive - management through Admin nodes.

Devices loosely synchronized - common problem to distributed schemes. Further research needed.

HolA: Holistic and Autonomous Attestation for IoT Networks

Alessandro Visintin[1], Flavio Toffalini[2,3], Eleonora Losiouk[1]
Mauro Conti[1], Jianying Zhou[2]

[1] University of Padua, Padua IT
[2] SUTD, Singapore SG
[3] EPFL, Lausanne CH

June, 23th 2022 - Rome

AIoTS Workshop @ ACNS 2022