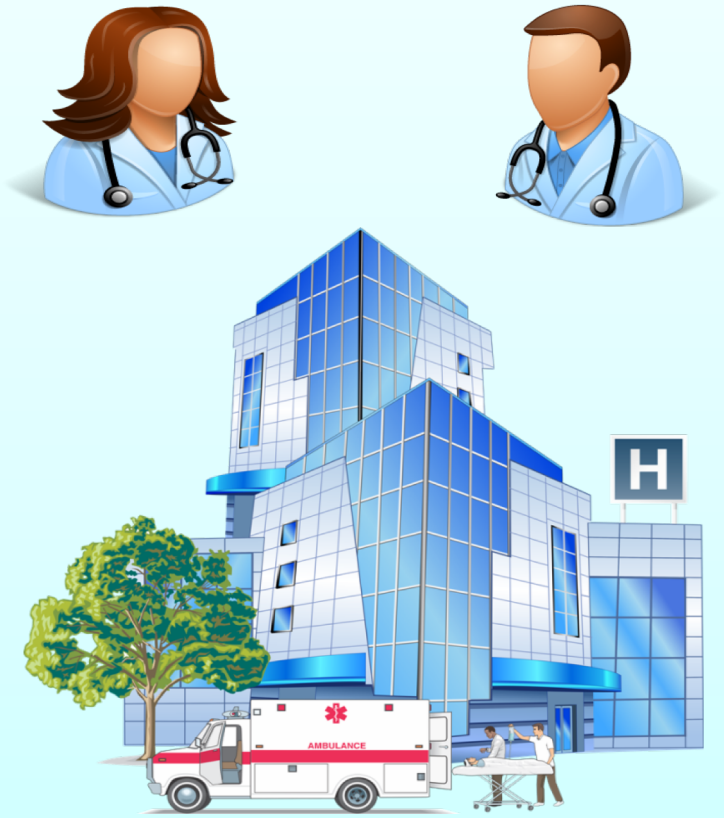
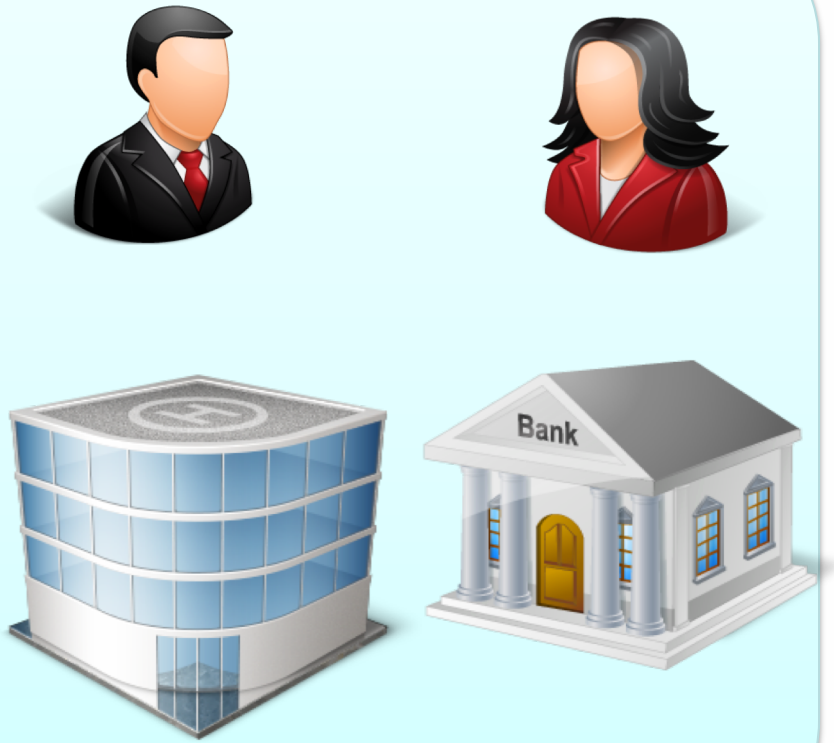
Location Proof - Motivation

Hospitals



Bank, Organizations



Location Proof: System Model

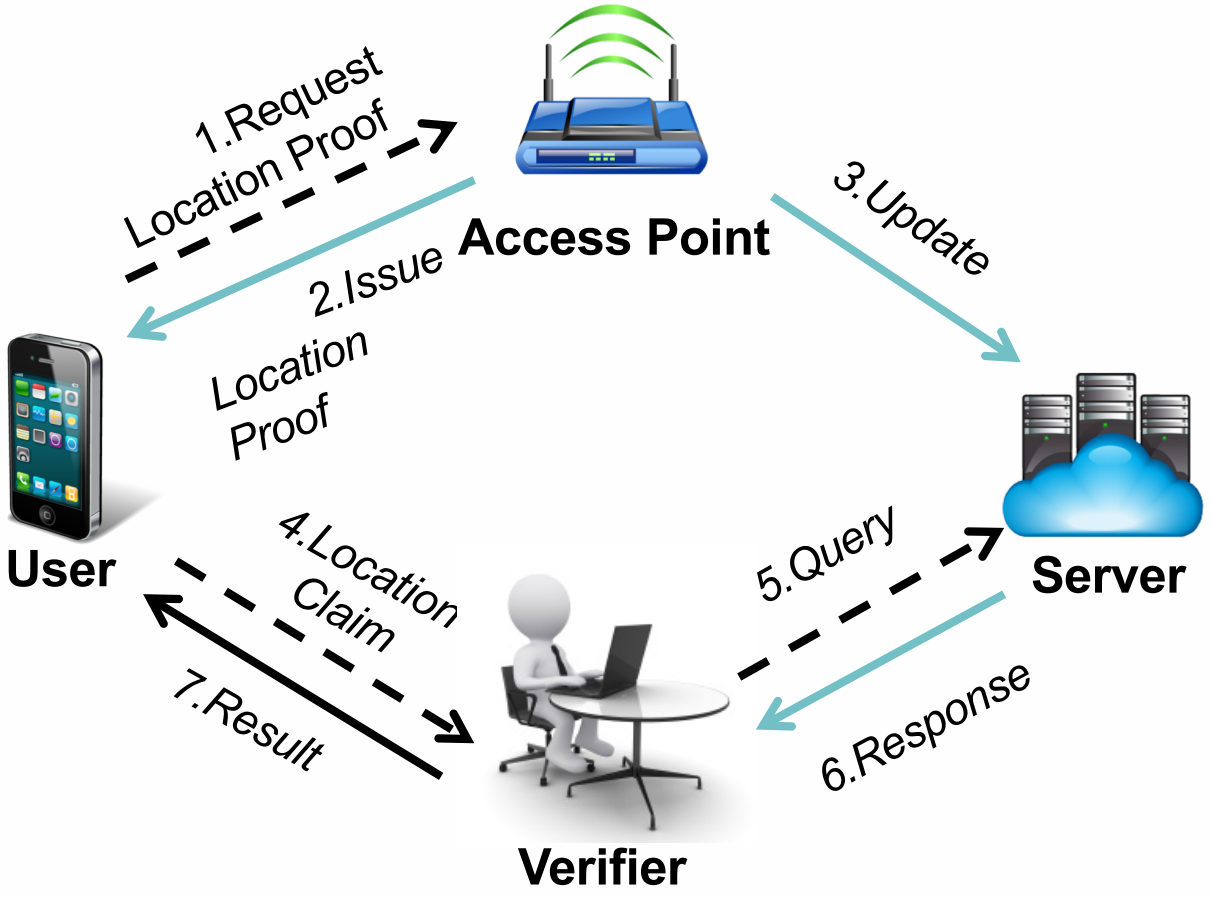


Figure 1: System Model

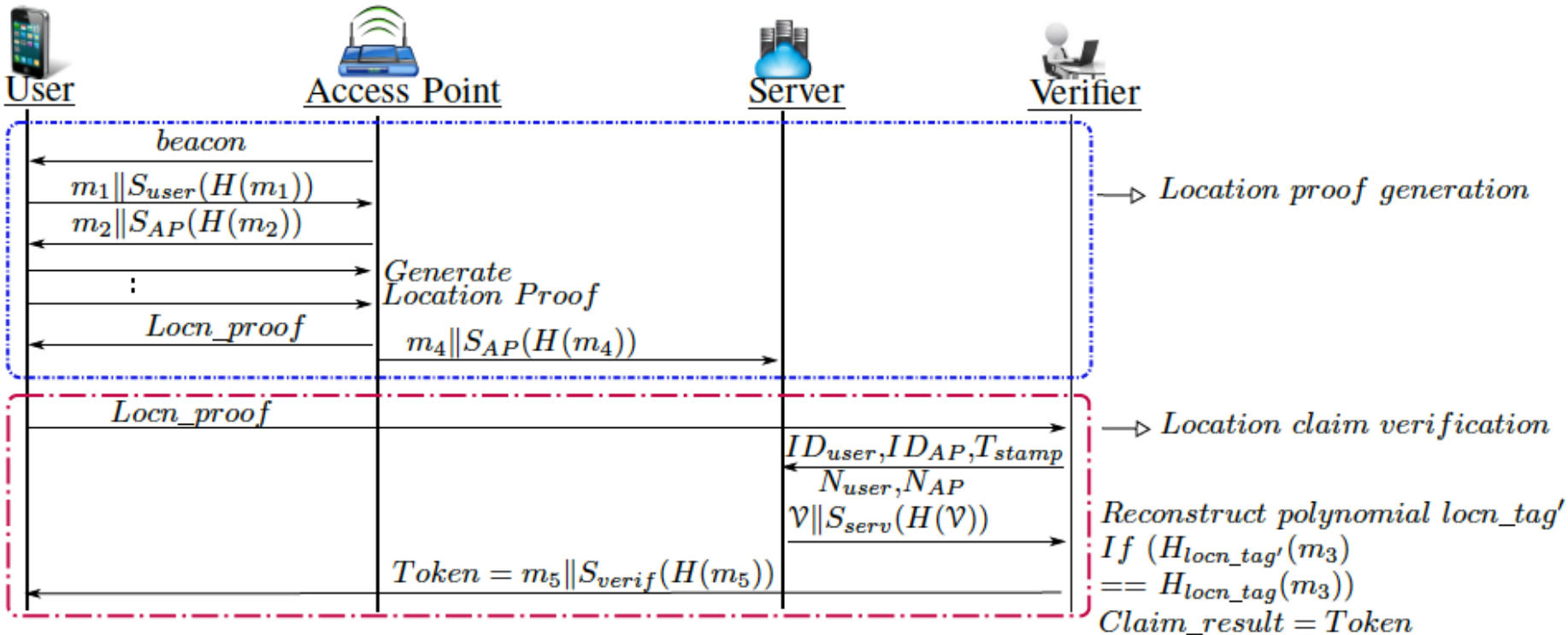
Location Proof: Basic Ideas

- Generation of the location tag based on wireless PHY layer characteristics
- Information theoretically secure (Fuzzy Extractor/Vault based schemes)
- Non-reproducible by an adversary
- Assumptions:
  - AP and Verifier are honest
  - Users are registered with LBS
  - Public-private key pairs are certified by Certificate Authority (CA)
  - Users and APs are recognized by their identities public keys

Fuzzy Vault Scheme (Juels and Sudan)

- A nice Crypto scheme to hide secret *S* in a vault using set *A*
- Unlocking of Vault: secret revealed only if set *B* is close to set *A*
  - *B* shares sufficient number of values to *A*
- We use channel state information (CSI) to construct shared secret
  - AP extracts the CSI from all the received packets
  - - Also gets coarse-grained location of user (a DB of mapped grid of location available at AP)

Protocol for Location Tag



$m_1 = Req \| ID_{user} \| N_{user} \| seq\_id$, $m_2 = Ack \| ID_{user} \| N_{user}$,

$m_3 = E_{verif}(\mathcal{B}) \| ID_{user} \| N_{user} \| ID_{AP} \| N_{AP} \| T_{stamp}$, $Locn\_proof = m_3 \| S_{AP}(H_{locn\_tag}(m_3))$

$m_4 = \mathcal{V} \| ID_{user} \| N_{user} \| ID_{AP} \| N_{AP} \| T_{stamp}$, $m_5 = N_{verif} \| locn\_tag$

Fig. 2: Message flow between the four entities of our proposed solution.

Location Proof: Security Properties

- If a User creates his/her own location claim and submits to the Verifier?
- If a User tampers the location proof to gain benefits for a different location and time?
- If a User transfers his/her location proof to another User?
- Can an adversary obtain information from locn_tag from vault V?
- Can an adversary modify the token?

For details:

Chitra Javali, Girish Revadigar, Kasper Bonne Rasmussen, Wen Hu, and Sanjay Jha, *"I Am Alice, I Was in Wonderland: Secure Location Proof Generation and Verification Protocol",* The 41st IEEE Conference on Local Computer Networks (LCN) Dubai, UAE, November 7-10, 2016

Thread Group (ARM, Consortium of Qualcomm, and Samsung …)

- Adopts PKC for authentication
- AES Symmetric key for confidentiality
- IPv6 Low-power Wireless Personal Area Networks (6LoWPAN) to minimize the energy consumption from wireless communications
- How to build secure-over-air reprogramming for IoT Devices (heterogeneous)?

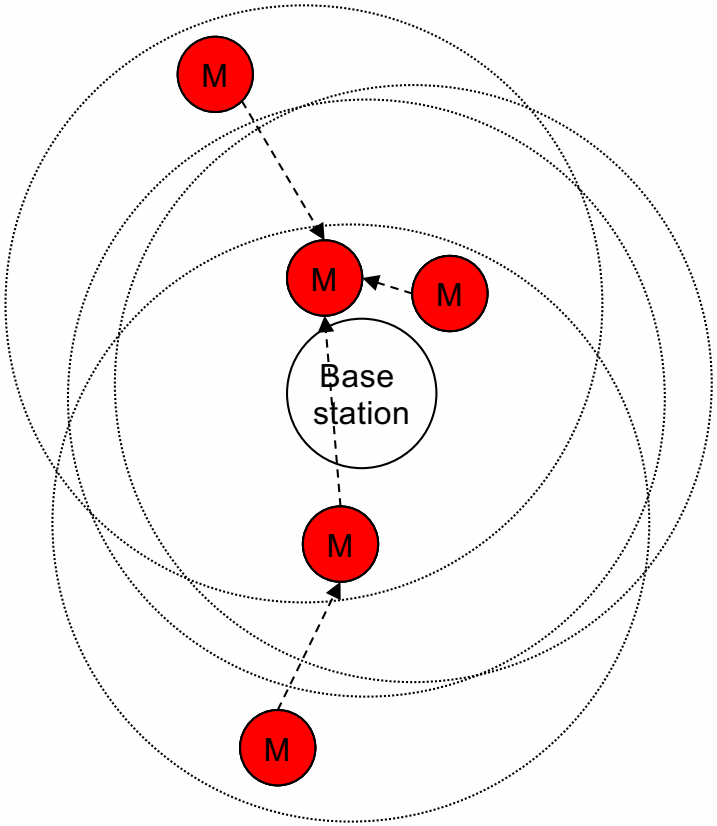
Broadcast Security – for IoT

- Broadcast applications need security
  - Packet injection or eavesdropping is easy
- Security solutions for point-to-point communication not scalable for large deployments
- Broadcast challenges
  - Scale to large audiences
  - Dynamic membership
  - Low overhead (computation & communication)
  - Packet loss
    - How to achieve reliability in broadcasts?

WSN Code Dissemination

- Assumes Homogenous Sensor Network
- Epidemic Communication Model
- Exploits spatial multiplexing
  - Parallel transmission in various parts of the network
- Node with the newer version program image becomes a sender and a node with an older version becomes the receiver
- Employ techniques: digital signature, Merkle hash tree, one-way hash functions , pairwise encryption.

WSN Secure Network Programming



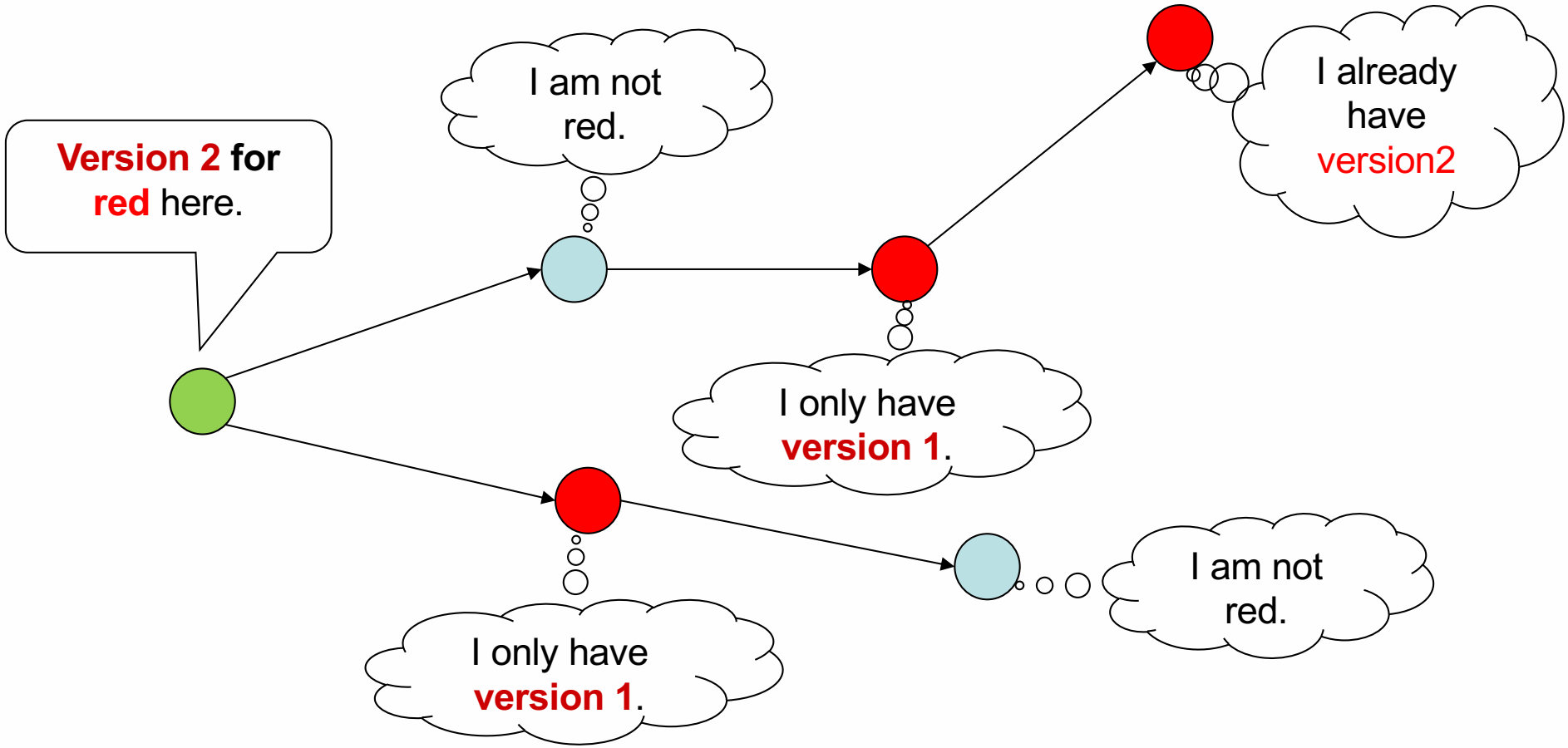
H. Tan, D. Ostry, J. Zic and S. **Jha**, "Secure Multi-hop Network Programming With Multiple One-way Key Chains", IEEE Transactions on Mobile Computing (TMC), Vol 10(1), pp 16-31, Jan 2011

SEDA: SEcure Over the air code Dissemination Arhitecture

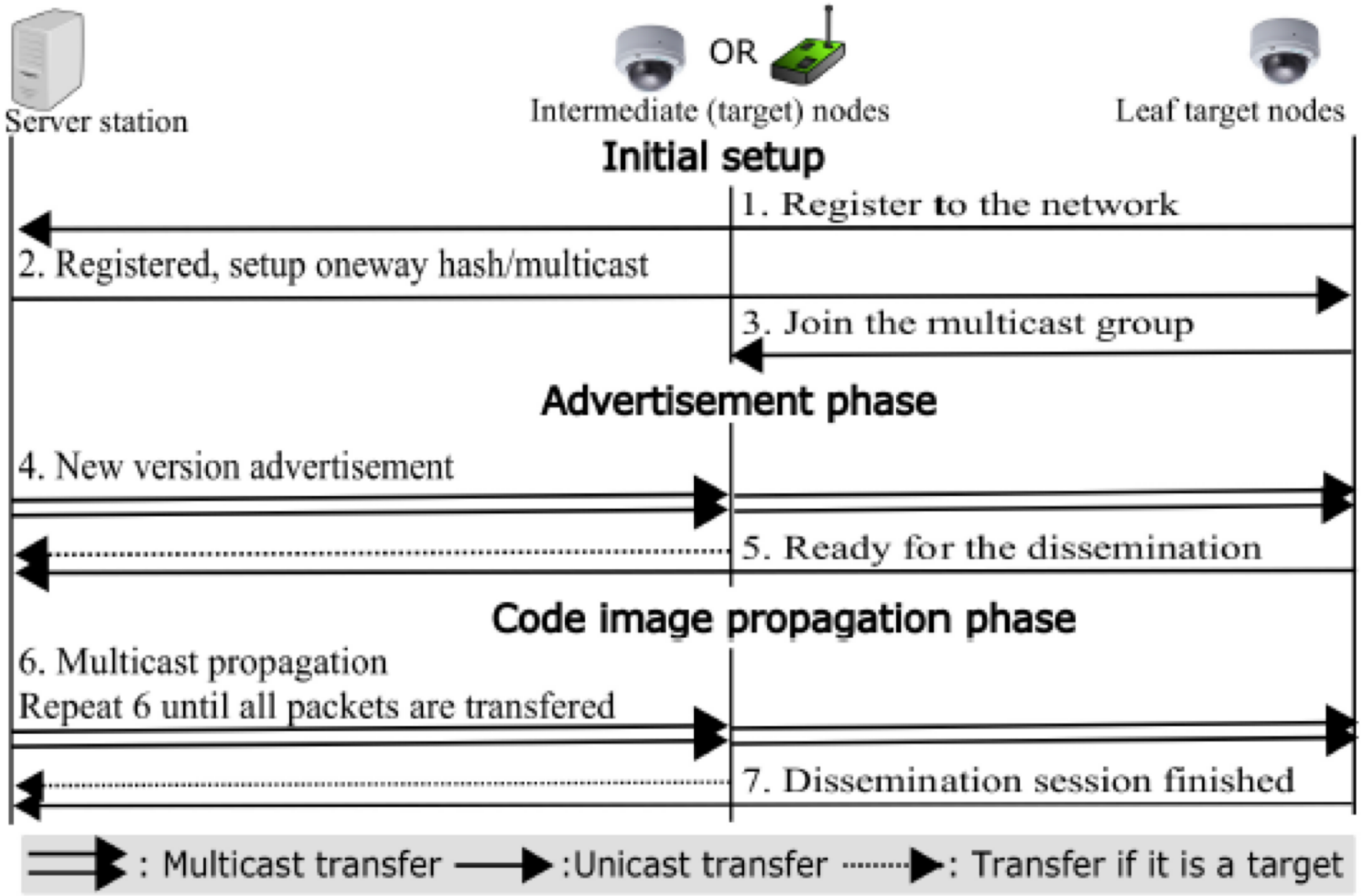
- Motivation: To produce experimental system which serves as a guideline for future deployment
- Use overlay multicast communication model for efficient dissemination and key distribution
- Public key cryptographic broadcast encryption scheme (BGWt) - for efficient group key distribution/management, and low decryption overhead.
- Identify potential security threats and defensive measures
- Experimentally validate the architecture and provide performance benchmark

Broadcast propagation

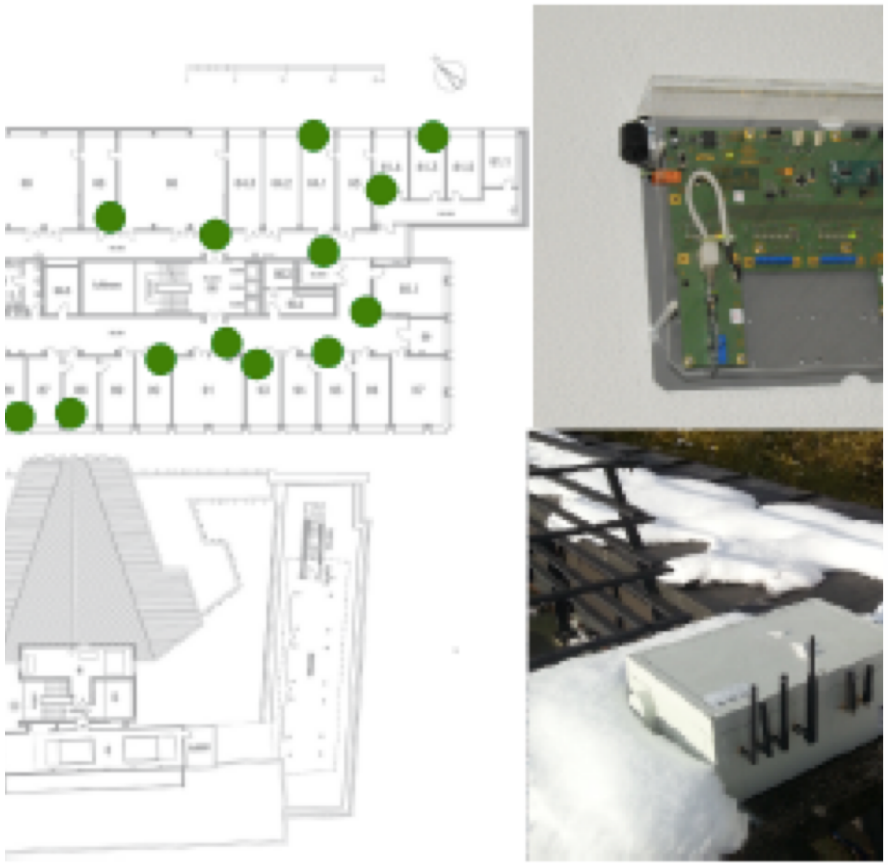
Server periodically broadcasts new version

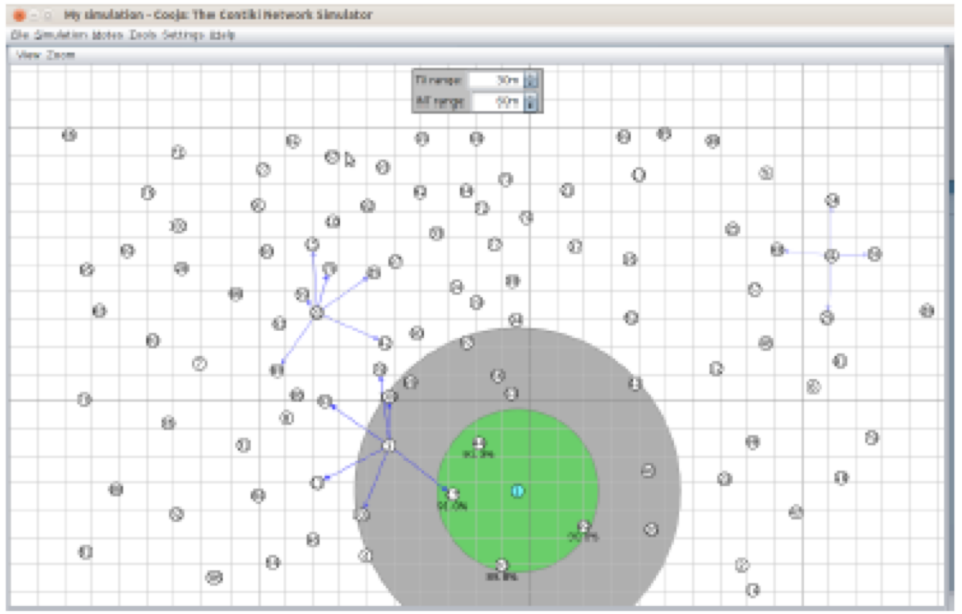


SEDA Protocol Overview



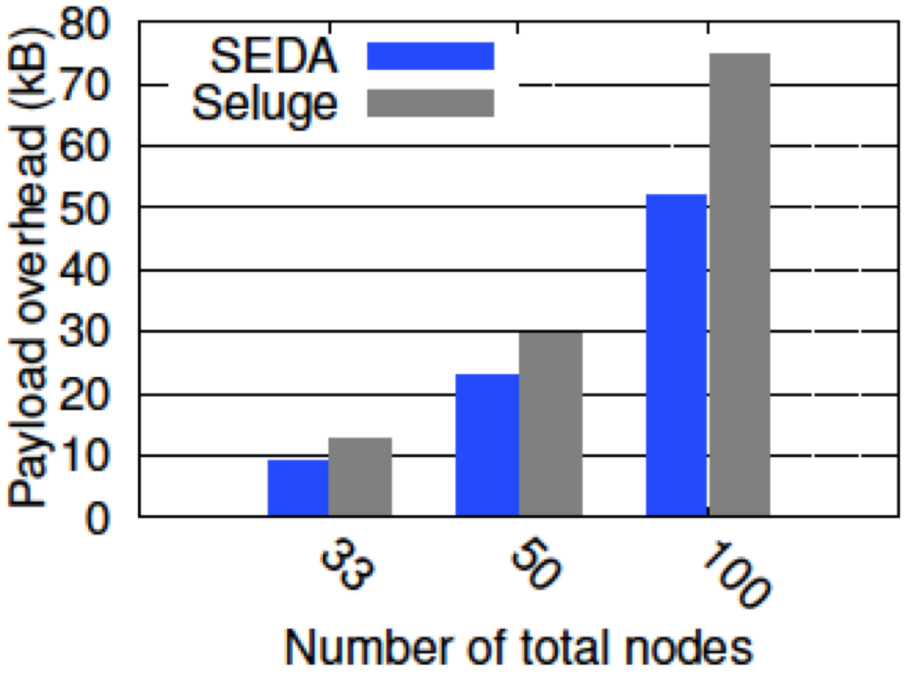
Flock Testbed and Cooja simulator



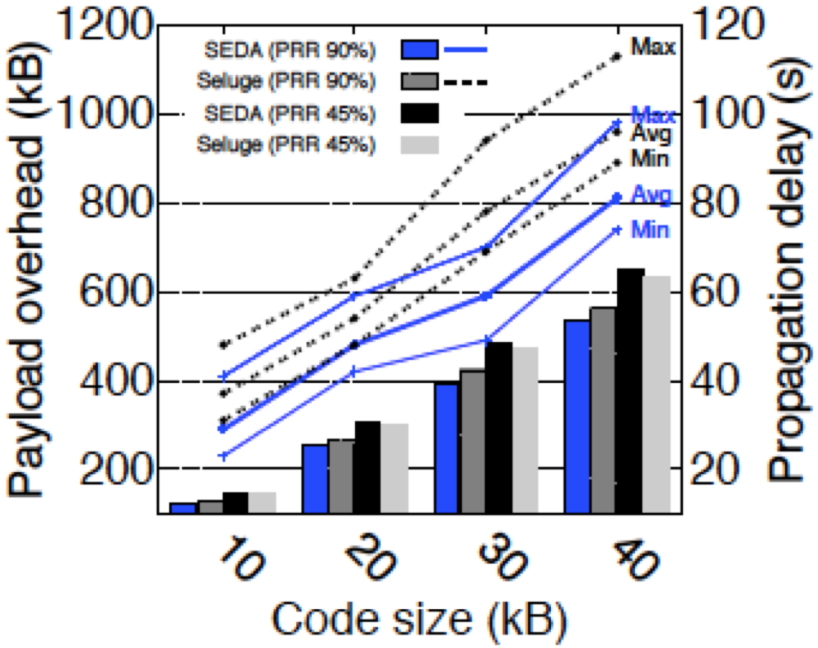


(c) Cooja simulator setting for a 100 node network.

Results



(a) Key establishment overhead comparis



(b) Propagation overhead (bar, left axis) and delay (line, right axis) comparison.

Research Contributions

- The selection and implementation of a public key cryptographic broadcast encryption scheme e.g. variation of BGW
- Experimentally validate through a prototype IoT platform and demonstrate the efficiency in practical settings
- Publicly release implementation as an open-source code

Selected Publications

- Weitao Xu, Sanjay **Jha**, Wen Hu, Exploring the Feasibility of Physical Layer Key Generation for LoRaWAN, In proceedings of The 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (Turstcom), New York, USA,
- Weitao Xu, Sanjay **Jha**, Wen Hu, LoRa-Key: Secure Key Generation System for LoRa-based Network . IEEE IoT Journal (SCI IF: 5.863). In-press, accepted in Dec 2018.
- Jun Young Kim, Ralph Holz, Wen Hu, and Sanjay **Jha**. Automated Analysis of Secure Internet of Things Protocols. *In Proceedings of the 33rd Annual Computer Security Applications Conference (ACSAC 2017)*. ACM, New York, NY, USA, 238-249.
- Quantifying the impact of adversarial evasion attacks on machine learning based android malware classifiers
  Z Abaid, MA Kaafar, S **Jha**, *IEEE 16th International Symposium on Network Computing and Applications* (NCA), 2017
- J. Y. Kim; W. Hu; H. Shafagh; S**. Jha**, "SEDA: Secure Over-The-Air Code Dissemination Protocol for the Internet of Things," *IEEE Transactions on Dependable and Secure Computing* , vol.PP, no.99, pp.1-1, 15 Dec 2016
- Z Abaid, MA Kaafar, S ,**Jha**, Early Detection of In-the-Wild Botnet Attacks by Exploiting Network Communication Uniformity: An Empirical Study - Proc. IFIP Networking, 2017
- Chitra Javali, Girish Revadigar, Kasper Bonne Rasmussen, Wen Hu, and Sanjay **Jha**, "I Am Alice, I Was in Wonderland: Secure Location Proof Generation and Verification Protocol", The *41st IEEE Conference on Local Computer Networks (LCN) Dubai*, UAE, November 7-10, 2016.
- Girish Revadigar, Chitra Javali, Wen Hu and Sanjay **Jha**, "DLINK: Dual Link Based Radio Frequency Fingerprinting for Wearable Devices". *40th IEEE Conference on Local Computer Networks (LCN)*, Florida, USA, October 2015
- Chitra Javali, Girish Revadigar, Lavy Libman and Sanjay **Jha**, "SeAK: Secure Authentication and Key generation Protocol based on Dual Antennas for Wireless Body Area Networks" by, RFIDSec 2014, Co-

Selected Publications

- M. Rezvani, V. Sekulic, A. Ignjatovic, E. Bertino and S. **Jha**, "Interdependent Security Risk Analysis of Hosts and Flows", Accepted in IEEE Transactions on Information Forensics and Security, 2015.
- M. Rezvani, A. Ignjatovic, E. Bertino and S. Jha, "Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks", IEEE Transactions on Dependable and Secure Computing, 12(1): 98-110, January 2015.
- M. Rezvani, A. Ignjatovic, M. Pagnucco and S. Jha, Anomaly-Free Policy Composition in Software-Defined Networks. The IFIP Networking 2016 Conference (NETWORKING 2016).
- Z. Abaid, M. Rezvani, S. Jha, MalwareMonitor: An SDN-based Framework for Securing Large Networks., ACM CoNEXT'14, Student Workshop, December 2014.
- T. Ali, V. Sivaraman, A. Radford, and S. Jha, "Securing Networks Using Software Defined Networking: A Survey", IEEE Trans. on Reliability Special Section on Trustworthy Computing.
- T. Ali, V. Sivaraman, D. Ostry, G. Tsudik and S. Jha, Securing First-Hop Data Provenance for Bodyworn Devices using Wireless Link Fingerprints, IEEE Transactions on Information Forensics & Security
- Abaid, Z., Sarkar, D., Kaafar, M.A., & Jha, S. "The Early Bird Gets the Botnet: A Markov Chain Based Early Warning System for Botnet Attacks", The 41st IEEE Conference on Local Computer Networks (LCN) Dubai, UAE, November 7-10, 2016.
- M. *Rezvani,* A. Ignjatovic, E. Bertino and S. **Jha**, "A Robust Iterative Filtering Technique for Wireless Sensor Networks in the Presence of Malicious Attacks (Poster Paper)" in proceedings of 13th ACM Conference on Embedded Networked Sensor Systems (SenSys 2013), November 11-13 2013. (accepted 22nd August 2013)