Implementation of 5G Authentication and Key Agreement Protocol on XBee Networks

5G – Security Group

Provenance for Communication in a Network of Connected Devices

Abstract

- With 5G, a number of multi-hop next generation networks will evolve, e.g., Vehicular networks.
- These require ultra reliability and low latency communication.
- Provenance is used to add an additional security layer at the time of payload transmission wherein each node embeds its identity so that the destination is able to recover the path.
- We demonstrate low latency provenance algorithm using bloom filters on a testbed of 6 XBee devices.

Motivation

- Traditional multi-hop packet relaying schemes,e.g., amplify and forward scheme satisfy latency conditions but are unable to help the destination to detect security threats in an unknown topology scenario.
- Developing provenance algorithms to satisfy the 5G low latency constraints is crucial for D2D communication.
- Learning the path can help in detecting security threats such as impersonation attack.

Contribution

- Failure of node embedding technique to detect path in an unknown topology environment led us to explore other embedding techniques in the bloom filter. We started with the idea of embedding edges and then reached to our contribution of double-edge embedding technique.

Embedding Techniques

Edge embedding

- For a h-hop path, the total number of nodes that embeds the edges is h.
- Each node in the path embeds the identity of its previous edge.

Double-Edge embedding

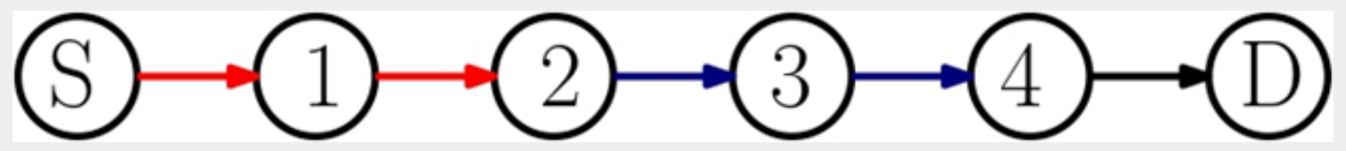
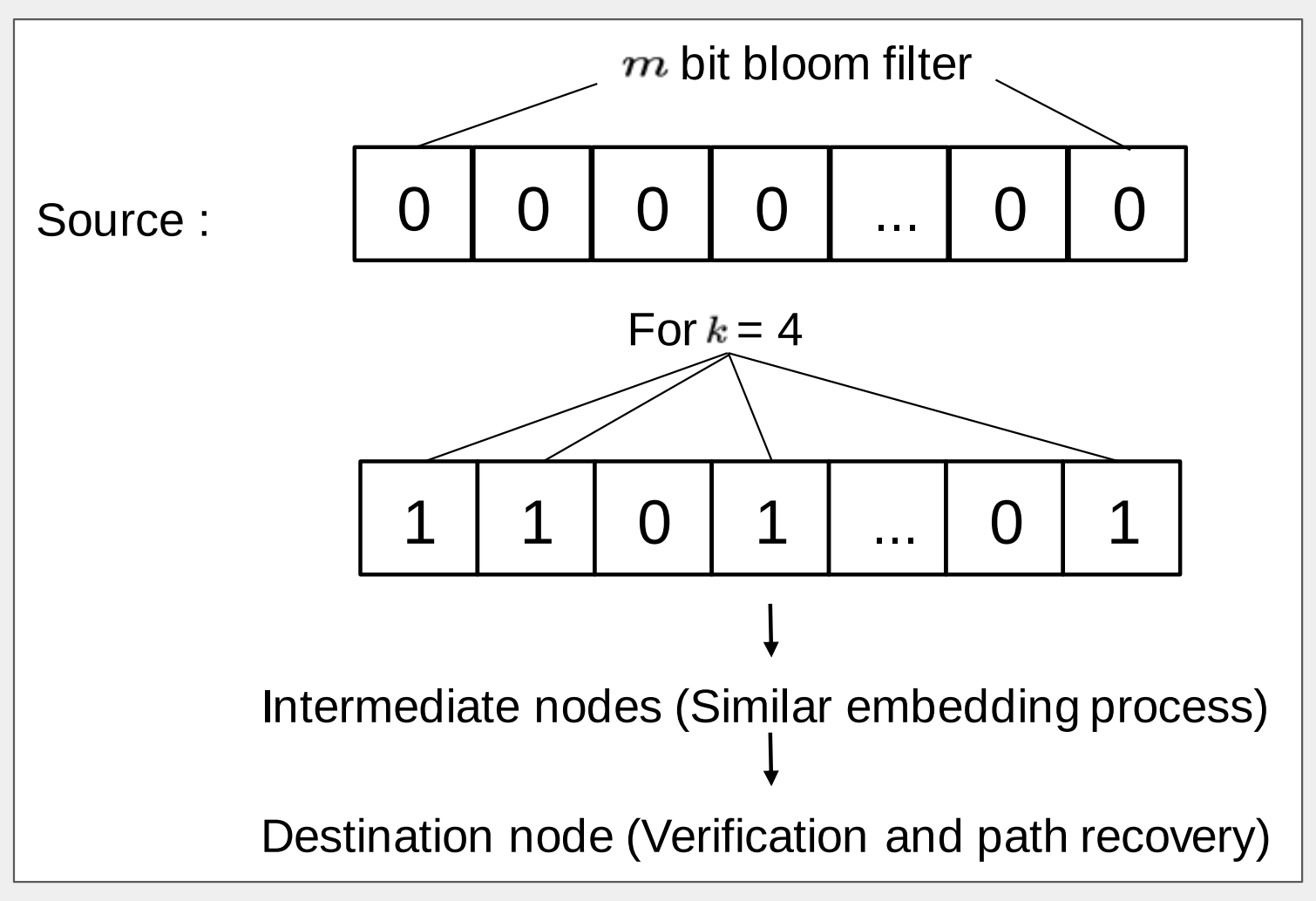


Fig. - Double-edge around node 1 and node 3

- Each alternative node in the path embeds the combination of previous and successive edges.
- Therefore, for a h-hop path, the total number of nodes that embed the double-edges is $\left\lfloor \frac{h}{2} \right\rfloor$.

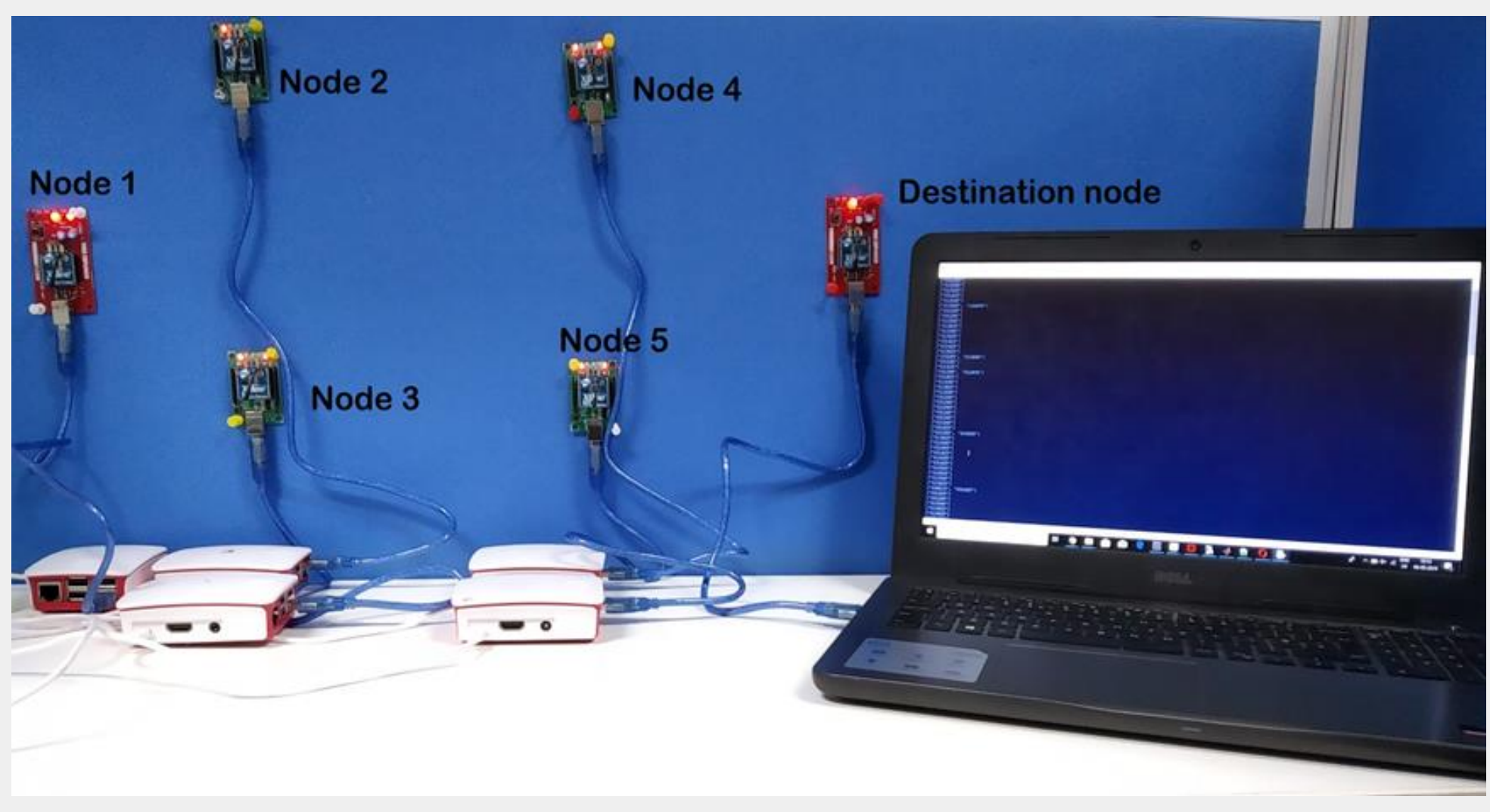
Bloom Filter based Provenance


m bit bloom filter
Source :
0 0 0 0 ... 0 0
For k = 4
1 1 0 1 ... 0 1
Intermediate nodes (Similar embedding process)
Destination node (Verification and path recovery)

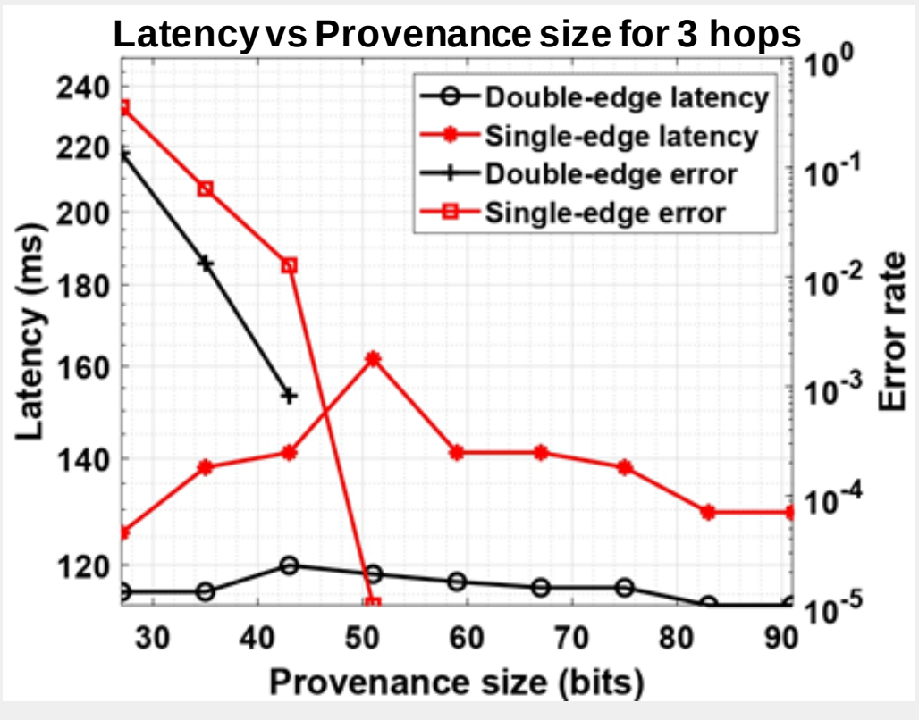
- Source node creates a bloom filter of m bits.
- Each node embeds the identity of its edge into the bloom filter with the help of k-hash functions.
- In case of double-edge embedding, alternate nodes in the path embed the identity of the double edge.
- The destination node, regenerates the bloom filter with the help of the network table (identities and keys) and verifies it with the received bloom filter.
- The destination then generates a list of possible edges that may have participated in the embedding process.
- The destination retraces all the paths formed by the list of possible edges.
- The event in which more than one path is retraced is called a false positive, and in such events the destination discards the packet.

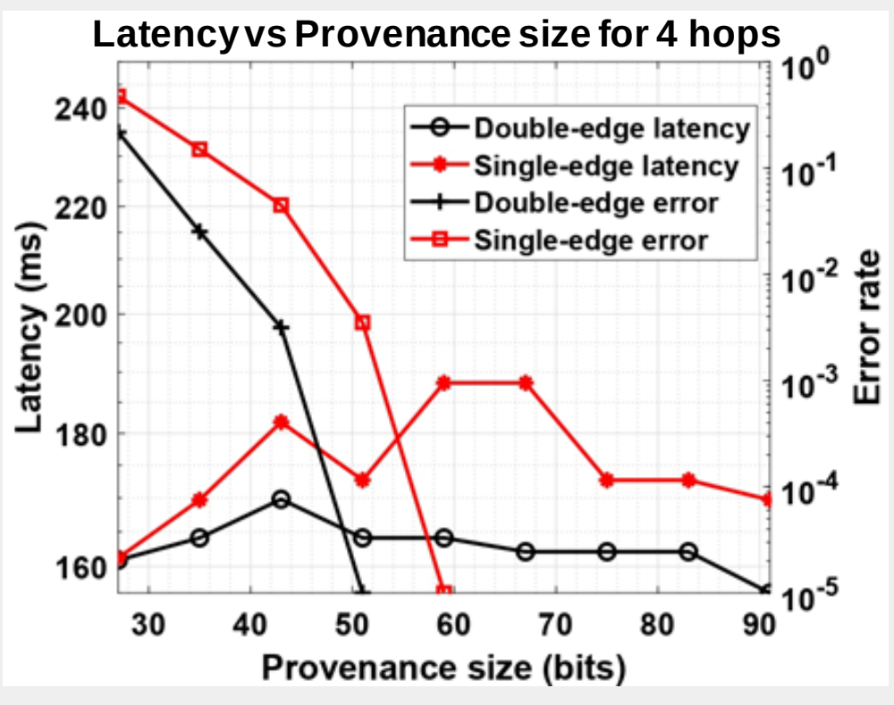
Demo Setup and Results

- Demo testbed consists of 6 nodes; 1 source, 1 destination, 4 relaying nodes.



- Each node consists of 1 XBee S2C device that acts as a transceiver and 1 Raspberry Pi that acts as the processing unit.
- The packet travels in an ad-hoc fashion and this is done by a random function.





- Path length can be 3 hops, 4 hops or 5 hops.
- Bloom Filter parameters : Bloom filter size = 80, k = 2, hop counter = 3 bits.
- Bloom filter parameters are chosen to drive false positives below a given threshold.
- Latency is the parameter of interest to compare between the two embedding techniques.

Assumptions

- Authentication is carried out using 5G compliant Authentication and Key Agreement (AKA) protocol.
- Encryption key is transferred to the source and destination node and a hashing key is given to all the nodes.
- In an unknown topology, the nodes create and share their edge and double-edge identities to the destination node during network discovery process.

Discussion and Conclusion

- We demonstrate double-edge embedding technique on a testbed of 6 XBee devices.
- We compare the latency of the two embedding techniques while driving the false positive error to 10^{-5}, and we have chosen the bloom filter parameters accordingly.
- We show the advantages of double-edge embedding technique over edge-embedding technique.

Acknowledgement

This work is funded by the Indigenous 5G Test Bed project from the Department of Telecommunications, Ministry of Communications, New Delhi, India.

References

[1] N. A. Johansson, Y. E. Wang, E. Eriksson and M. Hessler, "Radio Access for Ultra-Reliable and Low-Latency 5G communications," in the Proc. of 2015 IEEE International Conference on Communication Workshop (ICCW), London, 2015.

[2] S. Sultana, G. Ghinita, E. Bertino, and M. Shehab, "A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks," in IEEE Transactions on Dependable and Secure Computing, no. 3, 2015.