Ph: 9585554590, 9585554599
Email: support@salemsmartreach.com
URL: www.salemsmartreach.com

Exploiting Rateless Codes and Belief Propagation to Infer Identity of Polluters in MANET

Abstract:

We consider a scenario where nodes in a MANET disseminate data chunks using rateless codes. Any node is able to successfully decode any chunk by collecting enough coded blocks from several other nodes without any coordination. We consider the problem of identifying malicious nodes that launch a pollution attack by deliberately modifying the payload of coded blocks before transmitting. It follows that the original chunk can only be obtained if there are no malicious nodes among the chunk providers. In this paper we propose SIEVE, a fully distributed technique to infer the identity of malicious nodes. A node creates what we termed a check whenever a chunk is decoded; a check is a pair composed of the set of other nodes that provided coded blocks used to decode the chunk (the chunk uploaders) and a flag indicating whether the chunk is corrupted or not. SIEVE exploits rateless codes to detect chunk integrity and belief propagation to infer the identity of malicious nodes. In particular, every node autonomously constructs its own bipartite graph (a.k.a. factor graph in the literature) whose vertexes are checks and nodes, respectively. Then, it periodically runs the belief propagation algorithm on its factor graph to infer the probability of other nodes being malicious. We show by running detailed simulations using ns-3 that SIEVE is very accurate and robust under several attack scenarios and deceiving actions. We discuss how the topological properties of the factor graph impacts SIEVEperformance and show that nodes speed in the MANET plays a role on the identification accuracy. Furthermore, an interesting trade-off between coding efficiency and SIEVE accuracy, completeness, and reactivity is discovered. We

also show that SIEVE is efficient requiring low computational, memory, and communication resources.