

INTEGRATED VERIFICATION OF RELAY GENERATED NODE KEY & USER BASED MUTUAL WITH ERASURE CONCEPTS

Kaviya.S1,Nirmala.R2, Mr Madhan Kumar.S3

12UG Scholar, Dept. of CSE, GRT Institute of Engineering and Technology

3Assistant. Professor, Dept. Of CSE,GRT Institute of Engineering and Technology

The present protocols for creating pairwise secrets between nodes in a wireless network, so that these secrets are secure from an eavesdropper, Eve, with unbounded computational and memory capabilities, but with limited network presence. The first present a basic secret-agreement protocol for single-hop networks, where secrets are constructed using traffic exchanged between the nodes, and we show that under standard theoretical assumptions, our protocol is information-theoretically secure. Second, propose a secret-agreement protocol for arbitrary, multi-hop networks that build on the basic protocol but also comprises design features for leveraging additional sources, that multi-hop offers, for secrecy. Finally, evaluate our protocols, and provide experimental evidence that it is feasible to create thousands of secret bits per second, in realistic wireless setups, the security of which is independent of Eve's computational capabilities.