DESIGN OF ENERGY EFFICIENT ONION ROUTING FOR MANETS USING AASR PROTOCOL

M.V. R.Jyothisree, Dr. S.Sreekanth, and Dr.D. Shravani
Research Scholar Computer Science Rayalaseema University Kurnool A.P. India
Professor Dept. CSE SITAMS JNTU A A.P. India
Rayalaseema University Kurnool A.P. India
jyothisree.manne@gmail.com pranavasree_2000@yahoo.co.in sravani.mummadi@gmail.com

Abstract—Anonymous communications are important for many applications of the mobile ad hoc networks (MANETs) deployed in adversary environments. A major requirement on the network is to provide unidentifiability and unlinkability for mobile nodes and their traffics. Although a number of anonymous secure routing protocols have been proposed, the requirement is not fully satisfied. The existing protocols are vulnerable to the attacks of fake routing packets. AASR is a new routing protocol, i.e., authenticated anonymous secure routing, to satisfy the requirement and defend the attacks. More specifically, the route request packets are authenticated by a group signature, to defend the potential active attacks without unveiling the node identities. The key-encrypted onion routing with a route secret verification message, is designed to prevent intermediate nodes from inferring a real destination. In this paper we have shown the packet modification attack and how it has been prevented in aasr. Node energy also plays a very important role in routing procedure and in data transmissions. So we also implemented the energy efficient secure routing in aasr to prevent the energy black hole attack.

Key words: MANET, AASR, onion routing, black hole attack section.