IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET)
ISSN(E): 2321-8843; ISSN(P): 2347-4599
Vol. 2, Issue 3, Mar 2014, 45-50

SECURE ROUTING PROTOCOL IN SENSOR NETWORK FOR VAMPIRE ATTACK

S. RENUKA DEVI & R. DEVI

CSE(M.E), Sri Venkateswara College of Engineering and Technology, Anna University, Tamil Nadu, India

ABSTRACT

Ad hoc low-power wireless sensor networks are an exciting research direction in sensing and pervasive computing. Prior security work in this area has focused primarily on denial of communication at the routing or medium access control levels. This paper makes three primary contributions. First, we thoroughly evaluate the vulnerabilities of existing protocols to routing layer battery depletion attacks. We observe that security measures to prevent Vampire attacks are orthogonal to those used to protect routing infrastructure, and so existing secure routing protocols such as Ariadne, SAODV and SEAD do not protect against Vampire attacks. Existing work on secure routing attempts to ensure that adversaries cannot cause path discovery to return an invalid network path, but Vampires do not disrupt or alter discovered paths, instead using existing valid network paths and protocol-compliant messages. Protocols that maximize power efficiency are also inappropriate, since they rely on cooperative node behavior and cannot optimize out malicious action.

KEYWORDS: DSDV, DSR, MAC, OSLR, SEAD