

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320-088X

IJCSMC, Vol. 3, Issue. 2, February 2014, pg.328 – 336



RESEARCH ARTICLE

VAMPIRE ATTACKS: PROTOCOL ROUTING INFRASTRUCTURE IN WIRELESS SENSOR NETWORKS

T.Nivethitha¹, S.Muthukrishnan², S. Navaneethakrishnan³

¹ PG Scholar, Electronics and communication, Sri Eshwar college of Engineering, Tamil Nadu, India

²Professor, Electronics and communication, Sri Eshwar college of Engineering, Tamil Nadu, India

³PG Scholar, Electronics and communication, Sri Eshwar college of Engineering, Tamil Nadu, India
Nivethitha1704@gmail.com, logisweety@gmail.com, navaneethan2eee@gmail.com

Abstract

Ad hoc low-power wireless networks square measure an exciting analysis direction in sensing and pervasive computing. Previous security work in this space has targeted totally on denial of communication at the routing or medium access management levels. It explores resource depletion attacks at the routing protocol layer that for good disable networks by quickly exhausting nodes battery power. These “Vampire” attacks don't seem to be specific to any specific protocol, however rather trust the properties of the many standard categories of routing protocols. We discover that each one examined protocols square measure liable to lamia attacks, that square measure devastating, troublesome to observe, and are easy to hold out victimization as few in concert malicious business executive causation solely protocol-compliant messages. We have a tendency to discuss ways to mitigate these styles of attacks, as well as a brand new proof-of-concept protocol that incontrovertibly bounds the injury caused by Vampires during the packet forwarding section.

Keywords: WSN, Routing, malicious adversaries, lamia attacks

Full Text: <http://www.ijcsmc.com/docs/papers/February2014/V3I2201465.pdf>