International Journal of Computer Science and Engineering (IJCSE)
ISSN(P): 2278-9960; ISSN(E): 2278-9979
Vol. 3, Issue 2, Mar 2014, 111-126

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

MITIGATING A TRUST-AWARE ROUTING FRAMEWORK FOR CATCHING PACKET MODIFIERS IN WSNs

MADHIRALA CHANDRAKALA[1] & D. KOTESWARA RAO[2]

[1]PG Student, Department of Computer Science and Engineering, Chadalawada Ramanamma Engineering College, Tirupathi, Andhra Pradesh, India

[2]Associate Professor, Department of Computer Science and Engineering, Chadalawada Ramanamma Engineering College, Tirupathi, Andhra Pradesh, India

ABSTRACT

Packet dropping and modification are common attacks that can be launched by an adversary to disrupt communication in wireless multihop sensor networks. Many schemes have been proposed to mitigate or tolerate such attacks, but very few can effectively and efficiently identify the intruders. To address this problem, to secure the WSNs against adversaries misdirecting the multihop routing, we have designed and implemented TARF, a robust trust-aware routing framework for dynamic WSNs. Without tight time synchronization or known geographic information, TARF provides trustworthy and energy-efficient route. Most importantly, TARF proves effective against those harmful attacks developed out of identity deception; the resilience of TARF is verified through extensive evaluation with both simulation and empirical experiments on large-scale WSNs under various scenarios including mobile and RF-shielding network conditions. Further, we have implemented a low-overhead TARF module in Tiny OS; as demonstrated, this implementation can be incorporated into existing routing protocols with the least effort. Based on TARF, we also demonstrated a proof-of-concept mobile target detection application that functions well against an anti detection mechanism.

KEYWORDS: Wireless Sensor Networks, Routing Protocols, Security