TESTBED EVALUATION OF SELF-ADAPTIVE TRUST MODEL FOR COOPERATIVE GEOGRAPHIC ROUTING IN WIRELESS SENSOR NETWORKS

P. Raghu Vamsi and Krishna Kant
Department of Computer Science and Engineering,
Jaypee Institute of Information Technology, Noida, India.
E-mails: prvonline@yahoo.co.in, k.kant@jiit.ac.in

Submitted: May 12, 2016 ***Accepted: July 14, 2016*** ***Published: Sep. 1, 2016***

Wireless Sensor Networks (WSNs) are often deployed in remote and hostile environments to monitor the mission critical tasks. In such environments, cooperation among nodes plays a vital role for successful execution of protocol operations. However, node cooperation may not be guaranteed when malicious activities are present in the WSNs. Trust management based security has received considerable attention to use along with cryptography based security to improve the cooperation among nodes in the presence of malicious activities in the network. This paper proposes the self-adaptive trust model for cooperative geographic routing in WSNs. Unlike existing trust models, nodes running the proposed trust model systematically observe the behavior of their neighboring nodes and evaluate the trust values with adaptive weight assessment. The proposed method has been integrated with conventional Greedy Perimeter Stateless Routing (GPSR) protocol. Further, it has been coded with nesC programming in TinyOS environment and evaluated on a WSN testbed consisting of 15 Telosb sensor nodes. The experimental results show that the proposed method significantly improved the packet delivery ratio in the presence of packet dropping and modification attacks.

Index terms: Adaptive weights, cooperative routing, geographic routing, GPSR, nesC, security, test-bed implementation, TinyOS, trust management.