Abstract

Mohamed M Mohamed Fouad Eltaweel

A Pairwise Key Pre-distribution Scheme Based on Prior Deployment Knowledge

Still, the security problems remain one of the major barriers somehow preventing the complete utilization of wireless sensor networks (WSN) technology. Securing the communication channel through encrypting messages sent between nodes grow to be a must. Message encryption using the public key cryptosystems [1] in WSN is infeasible due to its constrained resources. A random key pre-distribution scheme [2] is of popular approaches that perfectly securing a WSN and conserving its resources. The random key pre-distribution scheme its enhanced editions is applied with assumptions of no prior deployment knowledge. The paper proposes a scheme that uses prior deployment knowledge in terms of the energy level carried by each node for modifying the polynomial pool based key pre-distribution scheme proposed in [3]. The paper shows that the node energy level observation can be used to control the creation and the ion of polynomial keys hold by this node. For the purpose of evaluating the proposed scheme it's applied on the A3 protocol as one of known topology control protocols [4]. The proposed scheme avoids the unnecessary key assignment and it reduces the number of active nodes per topology construction that positively reflects on the performance of the whole WSN.