Abstract

Mohamed M Mohamed Fouad Eltaweel

SOPK: Second Opportunity Pairwise Key Scheme for Topology Control Protocols

Sensor networks typically consist of a very large number of nodes with no centralized supervision. As a result, sensor networks are highly prone to an enormous number of logical and physical attacks. These attacks vary from eaves ping on sensitive information, imputing inaccurate information, to the unintentional failure of nodes as in Denial of Service (DoS) attacks. Many approaches have been proposed for assuring the Hop-to-hop encryption using different short keys in each node along the path from source to destination, for example the random key pre-distribution scheme. This random key pre-distribution scheme and its enhanced editions were 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 [1]. The paper shows that the node energy level observation can be used to control the ion of polynomial keys held by this node. The proposed scheme shows that it is suitable to be applied on topology control protocols such as the A3 protocol [2]. The proposed scheme reduces the energy consumption and computational overhead through controlling the use of security keys according to specific network's energy threshold that positively reflects on the performance of the whole WSN.