Energy Efficient Method in Wireless Sensor Network for Securing Compromised Data Aggregation against the Collusion Attack

International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 146 - Number 13

Year of Publication: 2016

Authors:
Jagtap Anagha M., Ingle Madhav D.

Abstract

Due to sensors storage capacity limit, communication bandwidth and computation ability WSN has some limitations. Due to this limited resources the amount of data transmission in network should be reduced. Data aggregation is new method for the above purpose. From the present algorithms for data aggregation the efficient is Iterative Filtering (IF) algorithm, which provides trust evaluation to the various sources from where the data aggregation is done. Trust assessment is given as weights, to cure the vulnerability of the fundamental averaging aggregation strategy to the attacks. Iterative filtering algorithms are stronger than the straightforward averaging procedure but they are not competent to deal with the novel advanced attack which exploits the false information through number of compromised nodes. Iterative filtering is improved to oversee novel complex attack by initial trust estimate, which increases the robustness and preciseness of the IF algorithm. Present system considers attack only on cluster members and not on aggregator. The information is transferred to aggregator by cluster members, and at last to the base station, in this process if attack happens on aggregator, present system gets fails. This problem is discovered by considering attacks on both
cluster members as well as on aggregator. The aggregator selection method is proposed which elects new aggregator depending upon maximum remaining energy and distance to the base station, when an attack is detected on aggregator. This makes the system more robust against the compromised aggregator node also it saves time and energy compared to the existing system.

References


Index Terms

Computer Science
Wireless
Keywords

Wireless Sensor Networks, Data Aggregation, Iterative Filtering, Collusion Attack, Trust, Reputation.