Journal of Electrical Engineering and Electronic Technology

Opinion Article A SCITECHNOL JOURNAL

Secured Routing against Black hole Attack in Wireless Sensor Networks

Adeel Ashraf*

Department of Electrical Engineering, University of Louvain, Louvain, Belgium

***Corresponding Author:** Adeel Ashraf, Department of Electrical Engineering, University of Louvain, Louvain, Belgium. E-mail: ashrafking@gmail.com

Received date: 24 August, 2022, Manuscript No. JEEET-22-54794;

Editor assigned date: 26 August, 2022, Pre QC No. JEEET-22-54794(PQ);

Reviewed date: 31 August, 2022, QC No. JEEET-22-54794;

Revised date: 16 September, 2022, Manuscript No. JEEET-22-54794 (R);

Published date: 30 September, 2022, DOI: 10.4172/jeeet.1000930

Description

Wireless sensor networks have a wide range of potential applications to industry, science, transportation, civil infrastructure, and security. Energy efficiency and improving the network lifetime are the fundamental challenges in wireless sensor networks. Lack of centralized administration and coordinator are the reasons for wireless sensor networks to be vulnerable to active attack like black hole. The affected node, without knowing a reliable route to destination, spuriously replies to have shortest reliable route to destination and entice the traffic towards itself to drop it. Network of such nodes may not work according to the protocol being used for the routing. Use of multiple sinks can improve the data collection resulting in improved throughput, reduced delay and congestion but due to black hole attack the overall performance of the network is reduced. In this paper a data collection algorithm using least cost path and ant colony optimization is used to address this issue which increases the network throughput and conserves energy resulting in maximum network lifetime and also designed a mechanism to tackle black hole attack. A zone based partition is applied to implement the shortest path using ant colony optimization and a mechanism to detect a black hole attack and the affected routes at an early stage. The residual energy of each node is calculated and the shortest path is selected using least cost and ant colony optimization A valid value is attached with RREP which ensures that there are no attacks occurring along the path. This approach is validated through the simulations in NS2.

Wireless Sensor Network

The work deals with the improvement in energy efficiency of the wireless sensor network using shortest reliable route and thus improving the throughput, delay and packet loss of the network and network secured with black hole attack. Existing work shows the MULE architecture where the sensors transmit data only over a short range that requires less transmission power. Let's consider in a city traffic monitoring application vehicles can act as MULES, in a habitat monitoring scenario, the role can be served by animals, in a national park monitoring scenario and people can be MULES. In the scenarios where the trajectories of the mobile sinks are constrained or predetermined, efficient data collection problems are often concerned to improve the network performance. The sink mobility can improve the performance of wireless sensor networks; where mobile sinks are mounted on some people or animals moving randomly to collect information of interest sensed by the sensor nodes where the sink is at random. The path constrained sink mobility is used to improve the energy efficiency of single hop sensor networks which may be in feasible due to the limits of the path location and communication power. This paper focuses on dense WSNs with path constrained mobile sinks that may exists in real world applications, such as ecological, environment monitoring and health monitoring. The mobile sink collects data from the sensor nodes while moving close to them. According to the communication range the monitored region can be divided into two parts, the direct communication area (DCA), and multihop communication area (MCA) for far off sensors. Sensor nodes with DCA, called subsinks can directly transmit data to the mobile sink due to their close proximity of the trajectory. On the other hand sensors with MCA, called members must first relay the data to the subsinks which completes the final data transmission to the mobile sink. The throughput depends on the data collected and the number of members belonging to each subsink. The existing research on sink mobility can be classified into the following categories: random path, controllable path and constrained path. Various attacks against WSNs is explained in the literature. Various measures were proposed to face these attacks. The attacks are classified as passive attacks from the active attacks. The passive attacks are limited to listening and analyze exchanged traffic. This type of attacks is easier to realize and it is difficult to detect. Since, the attacker is not allowed to make any modification on exchanged information.

Routing Information

The intention of the attacker is the cluster head node and confidential data. In the active attacks, an attacker modifies the message in the network. He can also modify his own traffic or replay of old messages in order to disturb the operation of the network or to cause a denial of service. The active attacks are as follows: Tampering: is the result of physical access to the node by an attacker; whose purpose will be to recover cryptographic material. Black hole: a node falsifies routing information to force the passage of the data by itself, later on; its only mission is then, nothing to transfer, creating a sink or black hole in the network. Selective forwarding: as mentioned above, a node play the role of router, in a selective forwarding attack, malicious nodes may refuse to forward certain messages and simply drop them. Sybil attack: Newsome et al. attacker can use the identities of the others nodes in order to take part in distributed algorithms such as the election. HELLO flood attack: many routing protocols use "HELLO" packet to discover neighboring nodes and thus to establish a topology of the network. The simplest attack for an attacker is sending a flood of data to flood the network and to prevent other messages from being exchanged. Jamming: it consists in disturbing the radio channel by sending useless information on the frequency band used. This jamming can be temporary, or permanent. Blackmail attack: In this a malicious node announces that another legitimate node is malicious to eliminate this last from the network. If the malicious node is successful in managing to tackle a significant number of nodes, it will be responsible to disturb the operation of the network.

In random path the mobile sinks are placed on randomly moving creatures like animals, human beings. Due to this random mobility it is difficult to bound the data transfer latency and the data delivery ratio. An analytical model based on queuing theory is presented for random path which incorporates many detailed aspects such as different mule mobility models, radio characteristics. Architecture of wireless sensor

All articles published in Journal of Electrical Engineering and Electronic Technology are the property of SciTechnol and is protected by copyright laws. Copyright © 2022, SciTechnol, All Rights Reserved.

networks with mobile sinks (MSSN) is proposed for traffic surveillance application. It is also assumed that all sensor nodes in MSSN are located within the direct communication range of the mobile sink. A communication protocol and a speed control algorithm of the mobile sink are suggested to improve the energy performance and the amount of data collected by the sink. A routing protocol called Mobiroute is suggested for WSNs with a path predictable mobile sink to prolong the network life time and improve the packet delivery ratio, where the sink is moved at some anchor points and the halt time is much longer than the movement time. Accordingly, the mobile sink has enough amount time to collect data, which is different from the designed scenario. Moreover, in Mobiroute all sensor nodes need to know the topological changes caused by the sink mobility. Mobile element scheduling problem is studied, where the path of the mobile sink is optimized to visit each node and collect data before buffer overflow occurs. A portioning based algorithm is presented to schedule the movements of the mobile element to avoid buffer overflow. The mobile sinks will visit all sensor nodes to collect data accordingly and the path optimization is based on the constraint of buffer and data generation rate of each node. The path selection problem of a mobile device is focused to achieve the smallest data delivery latency in the case of minimum energy consumption at each sensor. It is however assumed that each sensor node will send its data directly to the mobile device. Single hop communication is not feasible due to the limitation of road infrastructure and requirement on delivery latency. A rendezvous based data collection approach is proposed to select the optimal path due to the delay limitation in WSNs with a mobile base station.