Reliable and Secure End-to-End Data Aggregation Using Secret Sharing in WSNs

ABSTRACT

Data aggregation in WSNs (Wireless Sensor Networks) refers to the process of gathering and representing data in a summary form. It can effectively reduce the data size, resulting in significant energy reduction in transmitting and receiving data. Typically, a WSN is partitioned into clusters with a cluster head in each cluster. Each cluster head gathers data from its members, aggregates the data, and sends the aggregated data to the base station. There are many security requirements for data aggregation, including data confidentiality, data integrity, data freshness, data availability, authentication, and non-repudiation.

EXISTING SYSTEM

In Existing System, Another limitation with these approaches is that aggregators send the aggregated data to the base station directly. There are two major problems with the direct communication between aggregators and the base station. Firstly, aggregators consume a large amount of energy due to long distance communication, especially in a large WSN. Secondly, sensor nodes typically have a limited communication range in order to save energy, and the aggregators far from the base station may not communicate with the base station directly. Therefore, a routing topology such as tree is desirable.

DIS ADVANTAGES

- Attacks may make data aggregation unsecure.
- Selective forwarding attacks, a malicious sensor node may deliberately drop some packets.

PROPOSED SYSTEM

In Proposed System, two reliable and secure end-to-end data aggregation approaches that not only conceal the sensed data but also allow the base station to detect both the selective forwarding attacks and the modification attacks. The simulation results shows that both of our approaches perform better than PIP and RCDA-HOMO in terms of the aggregation processing time and the sensor processing time, and they significantly perform better than PIP in terms of the network lifetime, the network delay, and the aggregation energy consumption. One limitation with our approaches is that aggregators consume much more energy than other sensor nodes. As a result, they will die much sooner. In order to increase the network lifetime, we need to rotate aggregators. Another limitation with our approaches is that aggregators send the aggregated data to the base station directly.

ADVANTAGES

- Investigate the reliable and secure end to- end data aggregation problem are removed.
- Selective forwarding attacks and modification attacks in homogeneous cluster-based WSNs are solved.

SYSTEM REQUIREMENTS

H/W System Configuration:-

Processor	-	Pentium –III
RAM	-	256 MB (min)
Hard Disk	-	20 GB
Key Board	-	Standard Windows Keyboard
Mouse	-	Two or Three Button Mouse

Monitor	-	SVGA

S/W System Configuration:-

Operating System	:	Windows95/98/2000/XP
Application Server	:	Tomcat5.0/6.X
Front End	:	HTML, Jsp
Scripts	:	JavaScript.
Server side Script	:	Java Server Pages.
Database	:	MySQL 5.0
Database Connectivity	:	JDBC