An Efficient Routing Approach in Wireless Sensor Network using Fuzzy based Trust Model

Ashwini B V  Clara Kanmani A
PG Scholar Senior Assistant Professor
Dept of CSE Dept of CSE
NHCE, Bangalore NHCE, Bangalore
bvashwinigowda31@gmail.com claracalton.joseph@gmail.com

Abstract

Wireless sensor network consists of large number of sensor nodes which can be used to keep track of the environment. Because of the low cost, small size and nature of WSNs we can sense the information in various hostile environment. So to achieve better capacity of WSN sensor nodes to cooperate in distributing topology information. They operate in multi-hop routing. In this paper mainly we concentrate on security and network reliability in WSNs.
Introduction

Wireless sensor network are highly distributed network which consist of hundreds or thousands of small and lightweight wireless nodes. These nodes are connected via radio link and deployed in large number to monitor their surrounding environment or system. Each sensor node detects some events or collects information and communicates it in a wireless manner. Each of these scattered nodes has capability to route data to other sensor nodes or to base station.

Though there are technologies for networking and security, wireless sensor network still face some problem. As these networks operate in ad hoc manner, nodes are self organized. Due to self organized nature of sensor network malicious node may enter the network and eavesdropping can be easily performed. So, the communication here is multihop communication and is mainly relying on cooperation among nodes to achieve basic networking task like routing. In this each node sensed the data and forwards it to sink node which looks for available neighbor. So, this makes network to get exposed to privacy attack that ultimately disturb the network operation. As this network operate in multihop routing, is exposed to attacks identity deception through replaying routing information. Due to the identity deception, attacker may interfere with nodes and cause damage, drop or misdirect messages, create traffic collision or jam the communication channel. In a poor network connection distinguishing between an attacker and an honest node causes much difficulty.

Obtaining a trusted relation among nodes is an important goal. WSNs which provide number of opportunities at same time it is exposed to dreadful challenges such as energy. So, it is important to consider energy use for sensor node at same time to consider security as one of the important goal.

Related Work

Here mainly we have considered routing in the following three protocols.

- **TARF**

  This framework is developed for secure routing in wireless sensor network. In this two parameters run on every sensor node to keep track of their trustworthiness and energy. As these parameter run on every sensor node it may increase the considerable overhead and it is developed on TinyOs.
- **FBSR**

  current states of neighbor nodes. This protocol consists of local independent forwarding decisions based on current feedback information and prediction of future conditions.

- **TARP**

  It is a trust-based routing scheme responsible for routing messages from the different nodes to the base station. It is based on idea of node cooperation which forwards the neighbor messages.

  It uses the concept of cooperation in terms of routing reputation. TARP achieves significant improvements in terms of energy consumption and scalability.

  The main problem in the above is the Networking and the security. So, we come up with the proposed system.

### Proposed System

To enhance the security of WSN in this a fuzzy based technique is used while making a routing decision. Trust model is used to enables a node to keep track of the trustworthiness of its neighbours and fuzzy rules are used to select a reliable route path. With this a key management architecture is used while grouping sensors. This will be applied while selecting the cluster headers so the compromised node should not be selected as a cluster header. This trust Model based on Fuzzy Logic provide better security and survival of wireless sensor network under harsh and hostile environment.

**Step 1**: Initial sensor network.

**Step 2**: A node with a highest energy will be elected as a cluster header. This cluster head has responsibility to route a data from cluster to cluster header or base station and perform the operation like data aggregation. Here if the energy of current cluster header gets fall below the predefined threshold value then it has to transfer its responsibility to a node in a group by re-election method.
Step 3: Trust based clustering will be performed so the compromised or malicious node should not be selected (elected) as a cluster header. Because a compromised node always shows the highest energy in order to select that node as a group head.

Step 4: For that trust monitor and energy supervisor parameter run on cluster header only.

Step 5: Through this a node's trust level and energy can be found out by considering other parameters like packet delivery ratio, packet transmission rate, packet received rate, packet drop etc.

Step 6: On the basis of above parameters a cluster header can be checked out. Then key management method is applied to cluster header where it maintains a master key.

Step 7: Then apply the fuzzy rules to cluster header to decide which node should be selected as a next hop node to forward data to the base station.

Methodologies

Here the main important modules supporting are:

- Base station
- Trusted authority
- Fire sensor
- Bomb sensor
- Earthquake sensor

Base station:

Data center is responsible for receiving the sensed data from sensor, storing it in database. According to the protocol it will verify signature which is sent from the sensor.
Trusted authority:

Responsible for generating the keys and distributing the keys to the sensor nodes.

Fire sensor:

It is responsible for detecting fire in the forest.

After detecting the signal it will send the sensed data to the data center.

Bomb sensor:

It is responsible for detecting bomb blast in the city.

After detecting the signal it will send the sensed data to the data center.

Earthquake sensor:

It is responsible for detecting earthquake in the city.

After detecting the signal it will send the sensed data to the data center.

RESULTS SNAPSHOT

User Interface

![User Interface Image]
Trusted Authority

Base Station

Earthquake Sensor
Bomb Sensor

![Bomb Sensor Image]

Fire Sensor

![Fire Sensor Image]

Fire sensor after sensing data

![Fire Sensor after sensing image]
Bomb sensor after sensing data

Earthquake sensor after sensing data

Displaying received data
Changing protocol

![Routing in Wireless Sensor Network using Fuzzy rules
Status history
Place
Protocol initialized successfully
OK
Initialize protocol
exit]

Conclusion

In this, trust based routing protocols are discussed. To enhance the routing security a fuzzy based approach is introduced. This trust model enables a node to keep track of the trustworthiness of its neighbours which provides reliable and secure routing in wireless sensor network.

BIBILOGRAPHY