An Efficient Secured Scheme for Detecting Source of Packet Drop and Forgery Attack in WSN

Nirupama. Sheelwant  
Department of IT, SNIST, Hyderabad, Telangana, India.  
Email: nirupama.sheelwant@gmail.com

Sandeep.SD  
Department of EEE, SNIST, Hyderabad, Telangana, India.  
Email:sandeep.sheelwant@gmail.com

Abstract
In huge sensor network are organized in various fields of applications where resources of data come from multiple sources by sensor nodes which lead to critical in decision making. Data collected since to make data aggregation and forwarded in a network through intermediate nodes. So malicious nodes injects traffic, add unnecessary data to compromise existing network. For that reason giving trust on a network is crucial. Data travels in untrusted environment to overcome this we are proposing a lightweight scheme that reduce overhead of storage space, detect packet drop and forgery attacks while transmit data along with data provenance in bloom filter.

In accumulation we are adding provenance encoding and decoding at source and rebuilding at base station to be effectiveness of network. The provenance module is bringing the low energy, bandwidth utilization, resourceful storage, secure transmission and high efficiency in a sensor network.

1. INTRODUCTION
A wireless sensor network (WSN) is a collection of generalized transducer with messages transportation for observing and storing conditions at different localities. In wireless sensor network nodes are originated at random places. WSN is a type of network which is wireless, the nodes are connected by sensor method [4]. It’s an independent sensor which used to monitor objective and ecological state. The performance of wireless network is obtained when security is good enough for user.
When larger packets arrives the smaller cost and avoidance should occurs. When nodes are contacting each other response time should perfect and throughput.

Sensor nodes vary from small size to gigantic sizes as application needs and hundred or more than that of nodes are be in network. Different types of sensor nodes are deployed in home, medical science, traffic control in air and monitoring system etc..

We proposed the secured authentication routing protocol by using an iBF (in packet Bloom Filter). The encoding and decoding used at source node and can rebuild at base station to get original data. Here the lightweight technique used to transmit data faster and secure manner with less overhead and storage efficiency. In addition to this it can detect malicious attacker by observing behaviour of nodes which information are stored in routing table with node address, sequence number, key factor, importance of data and provenance. It evaluates the performance of proposed scheme by presenting different performance results.

2. RELATED WORK

Network security and failure nodes analysis is important for protect network management. In the paper [1] signify the snoopy module in a wireless sensor network. Snoopy explains about routing table why it is used and collection routing in a network path. Operator can follow the each information of nodes activated and keep track of all the faulty nodes occurs. Snoopy used in map reduce program as parent node receive data from its different child, it collects all the data as stored in map. K. Muniswamy-Reddy, D. Holland [2] proposed the storage system in a provenance network. Messages are arrived from various multi hops to its origin which have more information’s that leads to a storage, energy and bandwidth. The limitations of this paper is it works on untrusted sensor network which is not protected to data so malicious may effects to network to obtain data. Elisa Bertino, Hyo-Sang Lim [5] represented SCADA (Supervisory Control and Data Acquisition) method. In this paper author explained how data becoming crucial when decision making condition exists. The data collected from many different servers, sites, nodes, etc to make decision of trusted data has more critical. To overcome this data likeness and provenance resemblance is used.

The other papers focused on the secure network provenance [3] and packet with provenance [4] to the network environment but they are not optimized for sensor networks.

3. PROPOSED SYSTEM

3.1. System architecture

System architecture defines the systematic approach of system tools, structure, properties, relationship, behaviour, principles, frameworks etc of product.

In simple provenance sensor network as shown figure 1 its taking information from a single leaf node and forwarding to next node. There’s no aggregation method is
processing so it’s simple and fast effective transmission. As shown in figure 2, it’s representing in a tree from that parent node accepting packets from different applications as children, those data are aggregated and with a bloom filter scheme forwarding data to its neighbouring nodes. When data wants to forward first it checks its neighbouring node which have shortest path distance from other nodes to reach destination.

3.2. Implementation

There are four methods in implementation.

A. Network

In this module to setup the multi hop wireless sensor network by representing sensor node and antenna setup with multi hops where nodes are distributed data to base station.

Figure 1. Simple provenance Network
Suppose that many sensor nodes are send data to the single node (parent node) and that aggregates all the information and forward to other intermediate node again that node will add its own data then aggregate it and forward to next node until it reach the base station like hierarchy.

Each data packet contains separate sequence number for each packet with data number and provenance to the data for security. Each packet contains sequence number and its run till the network is on and so the sequence number used same.

B. Provenance

In implementation, there are organised provenance encoding and decoding by combining bloom filter stream.

Data provenance used which holds the information of data and address of all the sensor nodes which present in infrastructure. The data is encodes in Bloom filter while transmitting the packets from one to one node.
C. Provenance Verification and Collection

Provenance verification organise sequence packets with iBF value for producing verification id’s using hash function. They produce verification id’s compare with a bloom filter value for ensuring the node trust level.

Provenance collection collect the set of nodes distributed data by verifying the node identification level on each subset of nodes where determined node verification status on different levels to distribute the trusted node data to base station by forming trusted node routing path. By using decoding function the base station retrieves the data for future process.

Base station keeps all records of nodes vertex id, sequence number, path distance in routing table. When base station receives packet it verify all the accepted information with its records to confirm whether original data is altered. Due to node failure path direction changes that are not known to destination so it considered as untrust nodes are interacted. Base station make sure that path followed is truthful or not through routing table. So the base station comes to know if any alteration is done to data and indicates secure data.

The provenance collection process executes when base station receives all data from node. One single node accepts data from its child or leaf nodes then aggregate its all the information to forward next node until it reach its destination all data are combined by bloom filter. When provenance verification method fails the provenance collection process is used to verify at base station.

D. Detecting Packet Drop Attacks

It detects every packet crash show aggressions to make out malicious nodes in a network. So where malicious nodes presented on the existed path by using secure scheme network verifies node identity in corresponding path level based on the verification level the malicious nodes in a network have a different id’s based on this information the propose scheme can detect a malicious. Each node contains a node ID with a verification acknowledgement to each packet and the base station sends the generated key and node ID with sequence number by using AODV (Ad hoc on demand routing protocol) routing protocol. The packet transmission from source node to base station with the intermediate nodes data is forwarded from one node to another in that lastly seen is added in acknowledgement in packets is included in data.

If there is an acknowledgement mismatch that shows paths are changes by attacker. So by observing these all circumstances us to find there is a packet drop attacks.

4. EXPERIMENT SETUP AND RESULT ANALYSIS

To evaluate the performance of proposed system to calculating neighbour nodes and enter source nodeID.
The above Figure 3 broadcast data in this source ID (43) node determines the location and calculates pathway distances of all the neighbour nodes from routing table in a network.

The above Figure 4 transmission of the packets from selected source node ID i.e. 43 to its intermediate nodes which is near and shortest distance path i.e. parent node 24. Packet contains data value, sequence number and provenance by using hash function.
the key (using symmetric key method) is distributed for secure transmission. The 23rd node forward data to its neighbour node of 29th parent node with lastly seen acknowledgement to make clear that there is no alteration in packet or malicious not attacked its secured the original data and accept data.

Figure 5. Packet Loss.

Figure 6. VFR.

In the above Figure 5 packet drop graph explain that fraction of packets are dropped along with number of hops in a networks.

The above Figure 6 shows VFR (verification failure rate) along with different number of hops. Verification failure occurs when the base station compare received data with original data but it fails. It happens due to changes of path or adding traffic in network and changes the packets information.
5. CONCLUSION AND FUTURE WORK

In this paper we concentrate on transmitting data with provenance in secure way in sensor network. We suggest using encoding and decoding process in lightweight scheme with bloom filter. Here we are binding data in provenance along with symmetric key pair generation, sequence number and node id’s information in routing table. The knowledge of information stored with data can help to detect malicious attack in sensor network by doing cross check.

We are enhancing this project by deceitful a new secure provenance scheme for recovering the packet failure detection accuracy for several uninterrupted malicious sensor nodes. We enhance this project for improving detection rate for multiple malicious on typical sensitive sectors. The secure provenance scheme provides protected zone communications to handle trusted nodes.

REFERENCES


