**IMPLEMENTATION**

**MODULES:**

* Network Configuration
* Homomorphic Linear Authenticator
* Setup Phase and Packet Transmission Phase
* Audit Phase and Detection Phase

**MODULES DESCRIPTION:**

**Network Configuration**

In this project we are using Wireless Adhoc Network. Here we mainly focus on static or quasi-static network. In wireless network we need to send the packet through the node. System is represented as a node. Here every node has communication range. By using this range only we can transmit over packet. If source and destination node exists within the communication range, source can directly transmit the packet. Otherwise, we need to select the intermediate node based on the transmission range for transmit the packets.

**Homomorphic Linear Authenticator**

To correctly calculate the correlation between lost packets, it is critical to enforce a truthful packet-loss bitmap report by each node. We use HLA cryptographic primitive for this purpose. The basic idea of our method is as follows. An HLA scheme allows the source, which has knowledge of the HLA secret key, to generate HLA signatures s1, . . , sMfor M independent messages r1, . . . , rM, respectively. The HLA signatures are made in such a way that they can be used as the basis to construct a valid HLA signature for any arbitrary linear combination of the messages, , without the use of the HLA secret key, where *ci*’s are randomly chosen coefficients. A valid HLA signature for , can be constructed by a node that does not have knowledge of the secret HLA key if and only if the node has full knowledge of *s*1*, . . . , sM*. So, if a node with no knowledge of the HLA secret key provides a valid signature for ,, it implies that this node must have received all the signatures *s*1*, . . . , sM*.

**Setup Phase and Packet Transmission Phase**

This phase takes place right after route PSD is established, but before any data packets are transmitted over the route. In this phase, S decides on a symmetric-key crypto-system (encrypt key, decrypt key) and K symmetric keys key1, . . . , keyK, where encrypt key and decrypt key are the keyed encryption and decryption functions, respectively. S securely distributes decrypt key and a symmetric key keyj to node nj on PSD, for j = 1, . . . ,K. Key distribution may be based on the public-key crypto-system such as RSA: S encrypts keyj using the public key of node nj and sends the cipher text to nj . nj decrypts the cipher text using its private key to obtain keyj .

After completing the setup phase, *S* enters the packet transmission phase. Before sending out a packet *Pi*, where *i* is a sequence number that uniquely identifies *Pi*, *S* computes *ri* = *H*1(*Pi*) and generates the HLA signatures of *ri* for node *nj* , as follows

sji = [H2(i||j)uri ]x, for j = 1, . . . ,K

where || denotes concatenation. These signatures are then sent together with Pi to the route by using a one-way chained encryption that prevents an upstream node from deciphering the signatures intended for downstream nodes.

**Audit Phase and Detecting Phase**

This phase is triggered when the public auditor Ad receives an ADR message from S. The ADR message includes the id of the nodes on PSD, ordered in the downstream direction, i.e., n1, . . . , nK, S’s HLA public key information pk = (v, g, u), the sequence numbers of the most recent M packets sent by S, and the sequence numbers of the subset of these M packets that were received by D. Recall that we assume the information sent by S and D is truthful, because detecting attacks is in their interest.

The public auditor Ad enters the detection phase after receiving and auditing the reply to its challenge from all nodes on PSD. The main tasks of Ad in this phase include the following: detecting any overstatement of packet loss at each node, constructing a packet-loss bitmap for each hop, calculating the autocorrelation function for the packet loss on each hop, and deciding whether malicious behavior is present.