2. To design a routing module for IoT routing protocols to address modification and manipulation attacks.

Methodology: To prevent modification and manipulation attacks on routing protocols, nodes in IoT network have to actively participate to secure the route selection process. RPL is the standardized IPV6 routing protocol for low-power lossy networks. The DIO and DAO messages of RPL protocol need to be secured to prevent illegitimate access and modification of the fields in these two messages. As the message fields need to acted upon by intermediate nodes, malicious nodes can exploit this vulnerability to manipulate routes or simplify modify message fields to prevent selection of optimal routes. To handle such attacks, a simple trust/reputation based approach may not be feasible and therefore a more active methodology is to applied. As the IoT nodes are energy constrained, traditional security mechanisms involving asymmetric cryptographic techniques cannot be applied. Therefore, we aim to employ simple hash based chaining mechanisms to validate the authenticity of messages. The proposed methodology aims to combines a the identity of a node with the Lamport’s keyed hash chain method. The nodes participating in the routing process authenticate a message M by using a key obtained from the root/gateway of the IoT network. This key is used as a seed to generate a chain of authentication tickets as with Lamport’s keyed hash chain scheme. We do not rely on any public key infrastructure and there is no need for public key certificates. The proposed scheme is particularly suitable for multiple and dynamic sources of broadcast traffic like in RPL.