MODEL FOR MITIGATING PASSIVE EAVESDROPPING ATTACK IN IOT

P.Shorubiga* and T.Kartheeswaran

Department of Physical Science, Vavuniya Campus of the University of Jaffna

*shorubiha@gmail.com

The passive eavesdropping attack on the Internet of Things has serious risks on the user's data privacy. The security of IoT is still an unresolved question. Soon the people all over the world adopt IoT as smart home applications, wearables, and Industrial automation too. The risks in the confidentiality of private data are raising the number of devices and data exchanged. Even though the data having various light-weight encryption practices, the attackers still have a way to invade the confidentiality of the data. Metadata information in the packet header such as the size of the packet, protocol type, MAC address of source and destination, and state of the device can be exploited in a way that the attacker can be able to understand the user activities in a particular device. Application of deep packet inspection method and machine learning to huge data packets of a targeted user can reveal a lot of personal information. In this study, we propose a model to protect the header information. Speck, a lightweight encryption algorithm is used to encrypting the metadata such as MAC addresses of the source and destination. Because the MAC address reveals the device type and services to the attacker. The Software-Defined Network is chosen to be the central control for packets transmission to overcome the anonymity of packet flow. The decoupling mechanism of the control plane and the forwarding plane, the controller directs the encrypted packets to the routers and switches as a secured third party. The model was simulated using the RYU controller and tested in the Mininet SDN emulation platform using 4 nodes and respective connecting Ovsk switches with the central controller. The model has been validated using the packet capturing process with Wireshark.

Keywords: information privacy, Eavesdropping attack, internet of things, confidentiality, packet header, software defined networking, MAC address