VOICE over IP (VoIP) is an economical alternative for telephone communication compared to traditional Public Switched Telephone Network (PSTN) communication. In VoIP communication the voice conversation data is sent using IP packets over Internet. A typical voice call communication involves two phases as signaling and data transmission. Signaling is used to establish and maintain the end to end VoIP call; the actual data transmission usually happens in a different session. VoIP can use a range of protocols (H.323, SIP) for signaling purposes. Session Initiation Protocol (SIP) is an application layer signaling protocol for VoIP communication and has almost become the defacto standard. It is used to establish, modify and terminate multimedia sessions between two VoIP clients also called user agents. It is also used to request and deliver client's presence; send and receive instant messages between clients.

Session Initiation Protocol is a text-based protocol and is vulnerable to a range of denial of service (DoS) attacks. These DoS attacks can render the SIP servers/SIP proxy servers unusable by depleting memory and CPU time. In this work, we consider two types of DoS attacks, namely, flooding attacks and coordinated attacks for detection. Flooding attacks affect both stateless and stateful SIP servers while coordinated attacks affect stateful SIP servers. We model the SIP operation as *discrete event system*(DES) and design a new state transition machine, which we name as *probabilistic counting deterministic timed automata* (PCDTA) to describe the behaviour of SIP operations.We also identify different types of anomalies that can occur in a DES model, which appear in the form of illegal transitions, violating timing constraints, and appear in number which is otherwise not seen. Subsequently, we map various DoS attacks in SIP to a type of anomaly in DES. PCDTA can learn probabilities of various transitions and timings delay from a set of known non-malicious training sequences. A trained PCDTA can detect anomalies, and hence various DoS attacks in SIP.