Chapter 9
Conclusion and Future Scope

9.1 Conclusion

In this thesis we have discussed how communication is integral part of every life on planet and the progress in the communication system. Digitization of communication has brought great revolution in communication field and succeeded in bringing the world close to each other, communication has broken geographical boundary of planet. We have concentrated our work on VoIP system and its signaling protocol. During study we have identified that most of VoIP systems support SIP but due to its text based nature and poor authentication it makes VoIP system vulnerable to various threats. Our thesis work is focused on analysis and deterrence of SIP threats. During analysis of the SIP vulnerability more VoIP threats are identified, which are classified into confidentiality, integrity, availability and social threats.

We have confined our work on Force Teardown, Billing attack and DoS attack because these attacks cause economical and reputational damages to VoIP system. During literature survey we have identified few researchers have attempted to address force teardown and billing attack but their solution does not address major security goals.

Initially, Force Teardown attack is analyzed and an attempt has been made to deter it by providing secrecy to all signaling messages which carry credential information. We have proposed a symmetric encryption technique to provide secrecy to all signaling message and its performance is compared with well known symmetric encryption technique. Proposed encryption technique supports better CPU utilization and memory allocation compared to well known technique. Integrity of signaling message is maintained by using non breakable hashing technique. Security analysis of proposed encryption is carried out using Cryptool based on factor Entropy, Histogram, Digram and Trigram. Result of crypto analysis shows that 3DES gives slightly better result as compare to Proposed encryption technique.

After Force Teardown attack, Billing attack is analyzed and an attempt has been made to mitigate them by implementing well known security protocol which provides confidentiality, integrity and authentication to all signaling messages. After implementing secured protocol, we have identified that it added extra overhead on VoIP system. A secured session initiation protocol (SIPs) is designed with objective to minimize the communication overhead observed in SSL/TLS.
To evaluate a performance of SIPs security testing tool AVISPA is use. AVISPA has thoroughly tested security property of SIP as well as SIPs. AS a result of AVISPA has brought joy on our face because no attack has been traced out in proposed protocol (SIPs), while in SIP protocol attack has been traced out.

In this thesis an attempt has been made to identify abnormal activity in VoIP system, initially we have analyzed DoS attack such as Invite flooding, Cancel, Bye attack on SIP proxy and detected them by using intelligent IDS. Proposed IDS is a combination of neural network and fuzzy logic. After result analysis it has been clear that average detection, average false positive is better in BYE attack while average false negative is better in CANCEL attack. Proposed IDS technique uses fuzzy system to decide severity of DoS attacks. According to severity of attacks appropriate steps could be taken to protect them.

9.2 Future Scope

Security strength analysis of proposed encryption algorithm with 3DES shows that, there is a further scope of improvement in security strength of proposed encryption technique.

In proposed solution, we have not attempted to mitigate BYE delay and BYE drop billing attack and testing of SSL/TLS on a VoIP infrastructure where communicating parties are on different network, in addition to this evolution of SSL/TLS under different call rate will be future scope. We could further strengthen SIPs by improving symmetric key generation by maintaining and using timestamp mechanism, mutual authenticating technique and changing cipher suit in SIPs. During testing of SIPs, only security properties are considered, QoS testing of SIPs will be a future scope. In Adaptive IDS, threats detection ratio, false positive and false negative need to be checked under bulk traffic generated from various zombies, further research and testing is required to select the initial weight and no of hidden layer, neuron of FFNN (Feed forward neural network) to obtain better result. New IPS systems need to be designed to protect VoIP infrastructure from known as well as unknown DoS attack.

Providing security to RTP (Real Time Transport) protocol by maintaining better QoS of real time traffic could be a future scope.