ABSTRACT

The communication channels are now being managed generally by autonomous agents and the generated data is converted into experience by machine learning. The attack surface of the future generation networks is increasing many-fold and any system can be attacked, vandalized or collapsed via the network route. The future of digital world is thus highly dependent on its continuous analysis and evolving security.

The learning based systems are highly dependent on the type of corpus on which it has been trained. Existing pieces of literature indicate use of datsets generated from simulated networks, lab environments, or datasets released for data competitions. However, literature with experimentation based on actual networks, that too in a country-scale and being utilized for various network enabled services, are scarce. Video conference is a bandwidth hungry application running on this network which calls for a minimum assured bandwidth, even in case the quality of service of the network is not defined. The network management system (NMS) monitoring the network keeps polling it at frequent and regular intervals to update its awareness about it. The feed from the NMS is used by various intrusion detection and prevention systems for anomaly detection. We also identify and study portability issues with regard to pubic key infrastructure (PKI) for its use over low-power wireless networks, specifically ZigBee and 6LoWPAN, as PKI is primarily designed for wired networks.

Motivated by these problems, in this dissertation, we train different classifiers on a video conference call corpus from actual network to learn and predict the bandwidth of call setup and the source-destination pair, between which a call has been setup. This can help predict the quality of the video conference before initiation, so that necessary resource allocation can be made a priori, if required. As a spinoff, this set of experiments indicates a set of attributes that can be used for learning various critical parameters, which can also be used for anomaly detection. Thus, we conducted experimentation on a NMS dataset from the same network and executed machine learning using four different classifiers to detect normal behavior, so that any deviation from it could indicate an intrusion. The results of our learning experiments indicate poor performance of the classifiers in the detection of normal network profiles, thereby raising concerns for enhanced security of current and future networks. Further, the future networks have smart objects and agents that would provide services and do transactions and hence should be third-party acceptable. This led us to adopt PKI across various types of networks.

We started our PKI-based security enhancement by first devising a replay attack resilient system for authentication in channel-response mode for securing channel connectivity, followed by timestamped secure signing mechanism to ensure non-repudiation. Thereafter, we propose a PKI enabled secured communication schema for ZigBee networks. Protocols for interconnection between network entities are proposed, followed by analysis of network adaptation in different scenarios. Based on the success of secured inter-network communication in ZigBee, we attempt internal network communication in another low power network, i.e 6LoWPAN. We integrate PKI with 6LoWPAN without proposing any changes in PKI, but integrating it with 6LoWPAN in an efficient manner. Finally, we propose a security model for an application oriented wireless sensor network (WSN) setup in the area of surveillance network. The proposed scheme is based on a unique chemical-process inspired security paradigm, wherein the concept of a ‘Chelating Node’ is defined and its effectiveness in providing n-modular security scheme in detection of breach in surveillance sensor network is presented.

Keywords: Machine learning, Video conference dataset, Anomaly detection, Public key infrastructure, ZigBee network, 6LoWPAN security, Chemical process inspired security, Chelating node