Research:

Research Interests:

- **Network Security**
- **Authentication mechanisms**
- **Formal languages: CSP, FDR**
- **Authentication verification and analysis**
- **Wireless sensor networks**
- **Performance evaluation and performability of Authentication protocols.**
- **Application of Image Processing Techniques on Network security**

RESEARCH INTEREST AND ACTIVITIES:

Authentication is the primary function used to reduce the risk of illegitimate access to IT services of any organisation. Kerberos is a widely used authentication protocol for authentication and access control mechanisms.

The development of security strategies using Kerberos authentication protocol in wireless networks, Kerberos-Key Exchange protocol, Kerberos with timed-delay, Kerberos with timed-delay and delayed decryption, Kerberos with timed-delay, delayed decryption and password encryption properties are main research interests.

Also a number of other research works such as, frequently key renewal under pseudo-secure conditions and shut down of the authentication server to external access temporarily to allow for secure key exchange are studied and published.

A general approach for the analysis and verification of authentication properties as well as Kerberos authentication protocol are searched and studied. Existing authentication mechanisms coupled with strong encryption techniques are considered, investigated and analysed in detail. IEEE 802.1x standard, IEEE 802.11 wireless communication networks are also considered one of the main parts of my research.

An authentication protocol has been developed to improve the three way authentication mechanism for Kerberos. Dynamically renewing keys under pseudo-secure situations involves a temporary interruption to link/server access. After describing and analysing a protocol to achieve improved security for authentication, an analytical method is used to evaluate the cost in terms of the degradation of system performability.

Formal methods for verifying cryptographic protocols are created to assist in ensuring that authentication protocols meet their specifications. Model checking techniques such as Communicating Sequential Processes (CSP) and Failure Divergence Refinement (FDR) checker, are widely acknowledged for effectively and efficiently revealing flaws in protocols faster than most other contemporaries. Essentially, model checking involves a detailed search of all the states reachable by the components of a protocol model. In the models that describe authentication protocols, the components, regarded as processes, are the principals including intruder (attacker) and parameters for authentication such as keys, nonces, tickets, and certificates. In my research, an automated generation tool, CASPER is used to produce CSP descriptions. Proposed protocol models rely on trusted third parties in authentication transactions while intruder capabilities are based on possible inductions and deductions.

My research attempts to combine the two methods in model checking in order to realise an abstract description of intruder with enhanced capabilities. A target protocol of interest is that of Kerberos authentication protocol.

The process of increasing the strength of security mechanisms usually impacts on performance thresholds. In recognition of this fact, the research adopts an analytical method known as spectral expansion to ascertain the level of impact, and which resulting protocol amendments will have on performance. Spectral expansion is based on state exploration. This implies that it is subject, as model checking, to the state explosion problem. The performance characteristics of amended protocols are examined relative to the existing protocols.

A number of publications are presented for all models developed.

Authentication mechanisms coupled with strong encryption techniques are used for network security purposes; however, given sufficient time, well-equipped intruders are successful for compromising system security. The authentication protocols often fail when they are analysed critically. Formal approaches have emerged to analyse protocol failures. In this study, Communicating Sequential Processes (CSP) which is an abstract language designed especially for the description of communication patterns is employed. Rank functions are also used for verification and analysis which are helpful to establish that some critical information is not available to the intruder. In order to establish this, by assigning a value or rank to each critical information, it is shown that all the critical information that can be generated within the network have a particular characterizing property. This research presents an application of rank functions approach to an authentication protocol that combines delaying the decryption process with timed authentication while keys are dynamically renewed under pseudo-secure situations.

Wireless local area networks (WLANs) which are based on IEEE 802.11 standard are used widely in existing local area network configurations. IEEE 802.11 offers multiple nonoverlapping channels to increase the capacity of the network. There are strong evidences that WLANs are prone to impairments. In order to improve the quality of service (QoS) and to evaluate the performance of WLANs realistically, the availability of the systems should be considered. In this work, we study performability evaluation of a multichannel WLAN using analytical modelling approach. Unlike the existing studies, the failures of the overall system, where a critical function unit fails making all the channels unavailable are considered. A new term is introduced as global failures. It is possible to solve the models considered using matrix geometric methodwhere system parameters and minimal non negative solution R is computed by an iterative method. However spectral expansion method is a wellknown alternative where the iterative calculations for solving R is avoided using eigenvalues and eigenvectors. The exact spectral expansion method is employed to obtain performability measures such as mean queue length and blocking probability. Iterative refinements are employed in solution of simultaneous equations.

Most wireless communication and mobile computing systems are expected to be operational 24 hours a day, 7 days a week. However, wireless communication systems encounter failures. Performability modelling and evaluation of wireless and mobile systems have been of interest for recent research work. Especially, because of the complexity of the next generation wireless and mobile systems, modelling and performance evaluation is essential to improve the architecture according to the quality of service (QoS) requirements and performance characteristics. This research presents a performability evaluation framework for wireless cellular networks in wireless environments using analytical modelling approaches. The availability and mobility issues are also considered in the proposed models. Well-known approximate Markov reward model solution and the exact Spectral expansion solution approaches are considered. Performability measures of proposed models, such as blocking probability and mean queue length are presented.

This research presents a preliminary framework using back propagation neural networks for modelling approach of performability evaluation of Kerberos servers which dynamically renew keys under pseudo- secure conditions. The proposed security approach involves temporary interruption to link/server access, which has implications on performance degradation. An analytical method is used to evaluate the cost in terms of system's performance degradation. The model presented considers the system for exact performability evaluation. Numerical results are provided in order to analyse the effects of renewal times, times between renewals and failures of the server. Additionally, artificial neural networks propose a quite different approach to problem solving and known as the sixth generation of computing. In this study, two phases are proposed. For first phase, image pre-processing techniques in detail. In second phase, an intelligent image processing system using back propagation neural networks is applied to detect performability modelling.

A number of publications are presented for all models developed.