# ABSTRACT

Computer security is defined as the protection of computing systems against threats to confidentiality, integrity and availability. The threats to security in computing are interception, interruption, modification and fabrication. The controls available to address the threats to security in computing include encryption, network controls, programming controls and operating system controls.

The traditional methods of controls to threats in security which is the center of focus in this thesis are beset with drawbacks justifying a compelling need to look for better / efficient solutions. The work in the thesis centers around investigating computational intelligence based approaches such as Genetic Algorithms (GA) and the two paradigms of swarm intelligence viz Ant Colony Optimization (ACO) and Particle Swarm Optimization (PSO) to overcome the drawbacks existing in the traditional methods of controls available to combat threats in security in computing. The computational intelligence based approaches are applied to issues in security in computing such as Group rekeying for secure multicast, Leaker identification in secure multicast, Text and image encryption, Message authentication and Packet filtering firewall.

Group rekeying for secure multicast is achieved using an ACO/GA based Boolean Function Minimization Technique (BFMT) when the users join in or leave a group. Some of the group rekeying methods proposed in the

literature require a large number of keys to be stored and distributed to the users in the group. Of these, the group rekeying methods employing BFMT approaches stores and distributes minimum number of keys. However, the group rekeying methods employing BFMT approaches are not without drawbacks too. Therefore, to overcome these drawbacks, the computational intelligence based approaches viz, Genetic Algorithm and Ant Colony Optimization are proposed to obtain a minimized boolean expression for group rekeying in secure multicast. The genetic algorithm based approach termed Boolean Expression Evolver (BXE) is proposed to obtain a minimized boolean expression. However the drawback of the genetic algorithm approach is the increase in the time taken to obtain a minimized boolean expression, since all the chromosomes in each generation need to be considered. To overcome this drawback, an Ant Colony Optimization (ACO) based approach termed Ant Colony Optimization Boolean Expression Evolver (ABXE) is proposed to obtain a minimized boolean expression. The minimized boolean expression represents the minimum number of messages required to distribute minimum number of keys to the users in the secure multicast group.

Leaker identification in secure multicast applications such as commercial pay-per-view video multicast and pay-per view digital library should prevent users from leaking any information. Termed Ant Colony Optimization Leaker Identification Algorithm (ACOLIA), the novel technique serves to efficiently identify the leaker. The significant improvement in ACOLIA is that the number of comparisons is less when compared to the existing sequential search method for leaker identification.

Text and image encryption enhances the security of data traffic while transmitting messages over open network. A stream cipher method using swarm intelligence approach (ACO/PSO) of keystream generation is proposed. Termed Ant Colony Optimization Key Generation Algorithm (AKGA) / Particle swarm Optimization Key Generation Algorithm (PKGA) to generate the keystream, the stream cipher method employs a character code table for encoding the keys in the keystream and the plain text. The novelty of this approach is that it reduces the number of keys to be distributed when compared to Fast and Secure stream cipher, Key pooled RC4, Vernam cipher and RC4 algorithm. Also the time taken to encrypt using PKGA is less when compared to that of AKGA.

Encryption of images is done using a stream cipher method. The image is encoded in the form of a plain text. An Ant Colony Optimization Key Generation Image Encryption (AKGIE) Algorithm is proposed to generate the keystream for encrypting the image. The stream cipher method employs a character code table for encoding the keys in the keystream and the plain text denoting the encoded image. The novelty of the proposed stream cipher method is that it reduces the storage and distribution of keys compared to that of Vernam cipher considered to be the perfect cipher. It overcomes the drawback of boolean cellular automaton method for binary image encryption and scan pattern method of binary image encryption in terms of the storage and distribution of keys. The length of the key in AKGIE algorithm is lesser when compared to those of ELKNZ & DWT and chaos based image encryption method.

Message authentication plays an important role in preventing DoS attacks caused by injecting forged packets. Termed Ant Colony Optimization Boolean Expression Evolver Mark Generation (ABXEM) algorithm is proposed to authenticate the messages by generating a mark for each packet. The ABXE algorithm to obtain a minimized boolean expression is judiciously employed to efficiently generate marks for each packet. The novelty of this approach is that it calls for only (log n) keys and n signatures to be sent to the receiver which serve to reduce its communication overhead. In comparison, the Merkle tree packet filtering approach requires (n log n) hashes and n signatures to be sent to the receiver where n is the number of packets.

A firewall is a security guard placed at the point of entry between a private network and the outside network. An Ant Colony Optimization (ACO) based approach is proposed for packet filtering in the firewall rule set. Termed Ant Colony Optimization Packet Filtering (ACO-PF) algorithm, the scheme unlike its predecessors, considers all multiple occurrences of the same IP address or ports in the firewall rule set during its search process. The other parameters of the rule matching with the compared IP address or ports in the firewall ruleset are retrieved and the firewall decides whether the packet has to be accepted or rejected. The novelty is this scheme has a search space lesser than that of sequential search and binary search. It also strictly filters the packets according to the filter rules in the firewall rule set. It is shown that ACO-PF performs well when compared to other existing packet filtering methods.