Evolving Intelligent Systems – Concept, Applications and Opportunities for Security Systems of the Future

P Angelov, G Markarian, A Tarter. R Koeller, A Ali

Research into innovative computational intelligence methods to deal with data streams in *real time* will be presented. By using fuzzy rule based systems to capture knowledge from the data streams by on-line learning of both their parameters and structure a series of powerful computational engines were pioneered at Lancaster – evolving clustering (eClustering), classifiers (eClass family), predictors (eTS family), controllers (eControl). They can be seen as fuzzy blends of locally valid Gaussian filters and also as self-developing neuro-fuzzy systems. They possess a high level of adpativity to unknown environments and have been applied to a range of practical problems: a) intelligent sensors in oil refining (CEPSA Total) and chemical industry (Dow Chemical); b) on-line machine health monitoring and prognostics (Ford); c) autonomous systems for passive sense and avoid algorithm (BAE Systems); d) landmark recognition and self-localisation of robots (QinetiQ); e) cyber security (hacker attacks and intruders detection, user behaviour modelling); f) surveillance: object detection and tracking. This approach possesses significant potential to be used in the security systems of the future for the following reasons: a) evolving intelligent systems are convenient and rigorous tool for integration of expert knowledge and learning from data and experience; b) they can integrate the behavioural and psychological aspects of a security system and technological (engineering, mathematical, statistical); c) they can deal with uncertainties and linguistic variables such as *Anxiety*, *Fear*, *Hesitation* which are hard to be quantified otherwise; d) they tolerate imprecision. Interest to this original methodology for designing innovative in-flight security systems has been expressed by companies such as ULTRA and Thales. Such research can be a building block in the new Centre on BEhavioural Security Technologies (CBEST) that combines the efforts across the Faculty (it involves Communication Systems, Computing, and Engineering Departments).