**Wireless Security for Personalised and Mobile Healthcare Services**

Robert S. H. Istepanian  
*Mobile Information and Network Technologies Research Centre,  
Kingston University, London,  
Kingston-Upon-Thames, KT1 2EE, UK*  
E-mail: r.istepanian@kingston.ac.uk

**m-Health** is a new and evolving research discipline that is defined as emerging merging mobile communications and network technologies for healthcare. This new evolutionary research area will involve the provision of new paradigms in healthcare that will provide both the health care professionals and patients with an efficient, secure, ubiquitous and robust infrastructure coupled with tools for the assessment and management of patient health status and the support of preventive and patient empowerment programmes [1,2].

However, for such new services to be provided, in which patient confidential data will be routinely transferred between mobile devices having no prior knowledge of each other, robust new security services will be essential. These will have to be based on new security paradigms that, unlike today, cannot assume the presence of common trusted third parties, or require the patients to use cumbersome key or password management techniques. The assessment and the trustworthiness of “stranger” devices such as future wireless wearables and implantable devices will need to replace the former or some of the existing security methodologies. Issues such as context awareness and mobile ubiquitous computing systems will be the driving force for such development in existing security architectures and technologies that will be compatible with the requirement of such systems and services and the whole m-health security infrastructure will need to be autonomic and predictive with self-annealing so that it can determine when it is being attacked or not.

For example, some of the major features in current 3G security systems such IMS architectures, Link and higher levels security systems together with new confidentiality and integrity algorithms and authentication plans need to be revised and investigated further to address the compatibility and functionality issues of these technologies and architectures with the demanding and robust security and confidentiality requirement seamless mobile healthcare applications and service domains. It is also important that in order to achieve wireless global connectivity from the healthcare perspective a new standardisation procedures and protocols defining the specific security and privacy sensitive services such as mobile healthcare systems need also to be researched further and investigated to provide a visible standards for 3G based and beyond 3G based wireless healthcare systems and services.

**References**
