Mark Demore

485 Article Summaries

Dr. York

**Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges**

The Internet is continuously changing and evolving. The main communication form of present Internet is human-human. The Internet of Things (IoT) can be considered as the future evaluation of the Internet that realizes machine-to-machine (M2M) learning. Thus, IoT provides connectivity for everyone and everything. The IoT embeds some intelligence in Internet connected objects to communicate, exchange information, take decisions, invoke actions and provide amazing services. This paper addresses the existing development trends, the generic architecture of IoT, its distinguishing features and possible future applications. This paper also forecast the key challenges associated with the development of IoT. The IoT is getting increasing popularity for academia, industry as well as government that has the potential to bring significant personal, professional and economic benefits.

**Internet of Things: Architecture, Security Challenges and Solutions**

Internet of things (IoT) is a large distributed network in which billion of devices are interconnected. It is considered to be the largest wave of resolution as it does not require human to machine interaction. However, with the rapid growth of IoT, challenges in terms of security have evolved as well. Since IoT consists of three layers perception layer, network layer and application layer, this paper will provide an analysis for various security problems at each layer including the cross-layer heterogeneous integration security issues and suggest some promising solutions.

**Envisioning an Information Assurance and Performance Infrastructure for the Internet of Things**

The Internet of Things (IoT), in which sensing and actuation is embedded in everyday objects connected via the Internet, has the potential to support an increased level of intelligent, dynamic decision making cross a wide array of domains, such as smart cities, intelligent agriculture, and emergency response management. However, IoT systems are vulnerable to security threats, which limits their widespread adoption. In addition, in the future, systems will be challenged by the large amounts of IoT data communicated over the network and stored in cloud-based data centers. In this vision paper, outline a roadmap for innovative research on IoT security and performance, including the creation of secure communication protocols, IoT network threat detection, elastic computing algorithms, and computational offloading in IoT systems.

**Overview of Communication Protocols in Internet of Things: Architecture, Development and Future Trends**

The Internet of Things (IoT) transmits data between devices and users with the help of communication protocols. IoT communication protocols can be classified into 3 architecture kinds from different aspects: OSI model hierarchy, IEEE 802 protocol standard or network types. Designed for diverse situation and with growing technique, the protocols show different features in technology roadmap, communication distance, and signal frequency spectrum rang. The future trends of the IoT communication protocols might locate in their optimization, integration and information security.