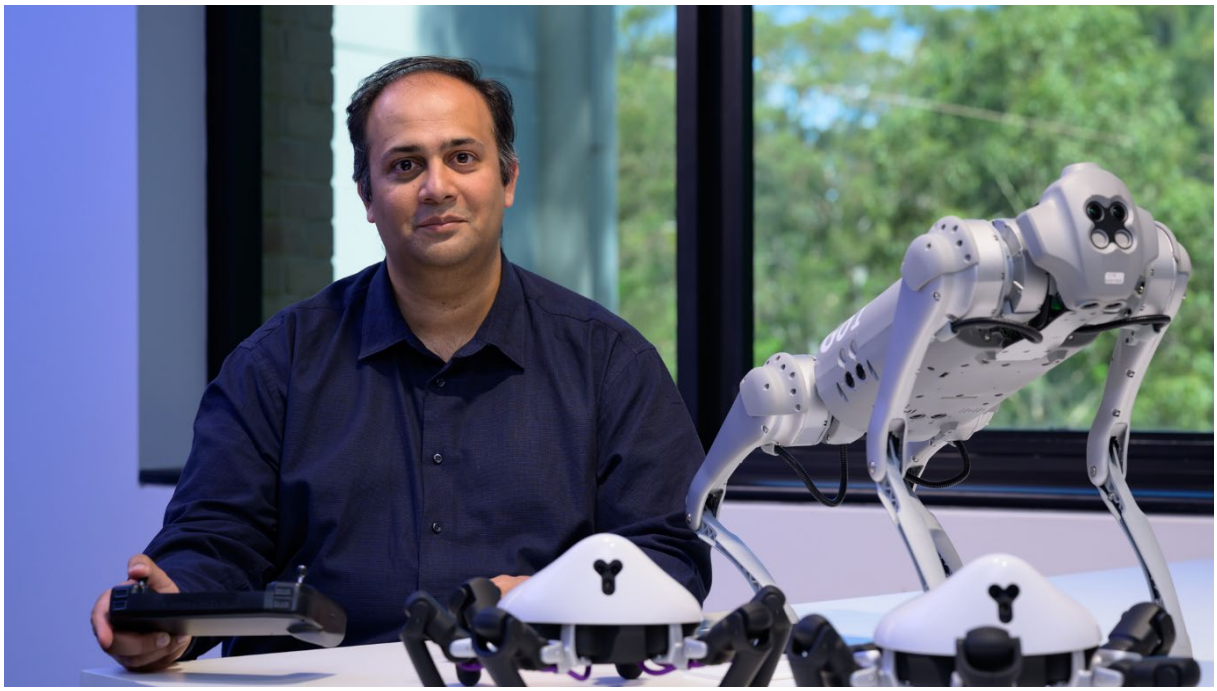
[MUICT-AST] MUICT x Macquarie University: Exploring World's Research Frontiers in Intelligent Autonomous Systems



Dr. Adnan Mahmood

Title	Trusting the Unknown – The Art of Trust Management in the Internet of Vehicles
Bio	Dr. Adnan Mahmood is a Lecturer in Computing – IoT and Networking at the School of Computing, Macquarie University, Sydney, Australia, and a member of the IEEE and ACM. Adnan's research interests include the Internet of Things (primarily, the Internet of Vehicles), Trust Management, Software Defined Networking, and Next Generation Heterogeneous Wireless Networks, among other topics. His extensive publication list includes refereed book chapters; journal articles published in prestigious venues, including but not limited to, ACM Computing Surveys, IEEE Transactions on Knowledge and Data Engineering, IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Network and Service Management, ACM Transactions on Sensor Networks,

	ACM Transactions on Cyber-Physical Systems, and Scientific Reports (Nature Portfolio); and conference papers. He is co-author of the books entitled, 'Trust Management in the Internet of Vehicles' (the first major publication in this fast-growing domain), 'Towards Resilient Social IoT Sensors and Networks: A Trust Management Approach', and 'Protecting Location Privacy in the Era of Big Data: A Technical Perspective', and supervises PhD and Master of Research students. Adnan, over the years, has given several invited talks and delivered tutorials at the International Conference on Intelligent Environments (IE) – 2023, IEEE International Conference on BigData (IEEE BigData) – 2021, and the International Conference on Cyber Security in Networking (CSNet) – 2021.
Abstract	Recent technological breakthroughs in vehicular ad hoc networks and the Internet of Things (IoT) have transformed vehicles into smart objects hence paving the way for the evolution of the promising paradigm of the Internet of Vehicles (IoV), which is an integral constituent of the modern intelligent transportation systems. Simply put, IoV attributes to IoT-on-wheels, wherein vehicles broadcast safety-critical information amongst one another (and their immediate ambiences) for guaranteeing highly reliable and efficacious traffic flows. This, therefore, necessitates the need to fully secure an IoV network since a malicious attacker, i.e., vehicle, is not only able to send counterfeited safety-critical messages to its nearby vehicles and the traffic management authorities but could further enable a compromised vehicle to broadcast both spoofed coordinates and speed-related information. It is, therefore, of the utmost importance that malicious entities (and their messages) be identified and subsequently eliminated from the network before they are able to manipulate the entire network for their malicious gains. This talk, therefore, delineates the

	convergence of the notion of trust with the IoV primarily in terms of its underlying rationale. It further highlights the opportunities which transpire as a result of this convergence for securing an IoV network. Issues pertinent to trust quantification and optimal threshold selection (for determining the trustworthiness) would be discussed. Finally, open research challenges, along with the recommendations for addressing the same, would be deliberated too.