Workshop: Internet of Things (IoT) for Intelligent Mobility and Dynamics: Interconnecting Air, Ground and Human

Yun Jia Wang, Kegen Yu
China University of Mining and Technology
Xuzhou, China
wyj4139@cumt.edu.cn,
kegen.yu@cumt.edu.cn

Chee Kiat Seow, Henrik Hesse
University of Glasgow
Glasgow, United Kingdom
cheekiat.seow@glasgow.ac.uk,
henrik.hesse@glasgow.ac.uk

Victor Wang
Singapore Institute of Technology
Singapore
victor.wang@singaporetech.edu.sg

2022 IEEE 8th World Forum on Internet of Things (WF-IoT) | 978-1-6654-9153-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/WF-IOT54382.2022.10152131

***Abstract* — This paper summarizes the workshop session on the pivoting interconnection between various Internet of Things (IoT) services in the air, ground, and human applications. Global Navigation Satellite System (GNSS) has been intelligently applied in space-to-ground, IoT-based remote sensing and imaging land applications for earth sustainability. The integrity and reliability of these GNSS services has been ensured with the digital signatures among the ground GNSS and edge IoT devices through the mobile terrestrial infrastructure. Edge IoT devices such as drones have traditionally suffered from unsustainable power consumption during mission critical operation such as hovering surveillance. These have been addressed by the introduction of perching drones that will reduce power consumption of the flying drones. Its critical safety aspect that will impact various human operations on the ground has been cleverly investigated through the design of dynamic design rules for flight operation.**

Keywords — GNSS, Remote Sensing, Cryptographic Digital Signature, Perching Drone, Internet of Drones, Drone Safety

Figure 1 illustrates the four session talks that demonstrate the interconnectivity of IoT spanning the various operating domains of air, ground, and human. Professor Kegen Yu, from China University of Mining Technology (CUMT) gave an invited talk on the land application of Global Navigation Satellite System reflectometry (GNSS-R) [1] which is an emerging remote sensing technology. Although it has been widely investigated, especially over the past two decades with many examples of spaceborne missions, airborne and ground-based experiments, there are still many research opportunities in earth observation and sustainability applications. Based on the image theory of the GNSS-R, Professor Yu has shared two specific land applications, namely snow depth and soil moisture measurement. With the detailed fundamental theory of GNSS-R covered, including the methodology in the retrieval of the associated parameters related to these two measurements, the demonstration of the experimental results has led to the discussion in the possibility of extending the application of both measurement of snow depth and soil moisture content to various humanitarian rescue operation and earth conservation for sustainability. For example, any victim trapped in the snowstorm can be detected if there is some means of effective environment scanning, potentially by leveraging on the deployment of drones as compared to the current form of receiver tripod or GNSS base station installation. With the good result shown in measurement of soil moisture content, the quality of the soil can be effectively measured to perform predictive analysis in the degradation of the earth conditions, for example, to preempt potential earthquake arrival. The maturity and advance in GNSS-R research have opened many research avenues for useful applications such as detection of hurricane, tsunami, and even cyber threats.

The success of any GNSS application and services relies heavily on the integrity and reliability of the Position, Velocity and Timing (PVT) information provided by the ranging and navigation message (NM) of the GNSS signal. It has been shown that potential vulnerability of GNSS has been uncovered in many circumstances, especially in defense related situations where drones have been spoofed and hijacked. Dr. Chee Kiat Seow, from the University of Glasgow, UK, has shared his invited talk on GNSS vulnerability [2]. The fundamental principle on the GNSS ranging and positioning, and spoofing vulnerability have been articulated with the emphasis on the importance in protecting GNSS integrity and reliability. Many essential critical infrastructures and modern applications rely heavily on the GNSS PVT information. For example, power grid synchronization, finance banking and timely transactions, communication signaling backbone (4G, 5G), and

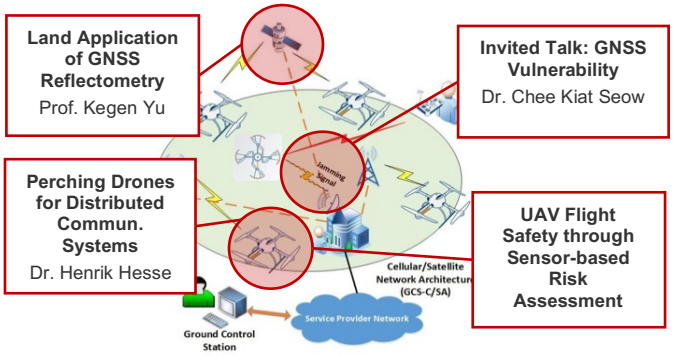

Fig. 1. Four workshop sessions on various IoT applications interconnecting the different domains of air, ground, and human. Figure adapted from [8].

transportation reliability and efficiency especially for autonomous vehicles. The operational region of GNSS attackers on the two main scenarios in spoofing has exposed the integrity protection weakness of existing GNSS signal [3]. Firstly, the technical analysis on spoofing of one victim and multiple coordinated victims has shown that it is impossible to offer protection against spoofing on one GNSS victim as the region of operation (ROC) is unlimitedly subjected to the constraint of the transmitting power of the GNSS attacker. Secondly, the vulnerability of GNSS has been further demonstrated if multiple GNSS has been spoofed. Various GNSS anti-spoofing protection mechanisms have been discussed. Notably, pseudo-range [4] and NM digital signature protection are more feasible and resilient solutions. For example, anti-spoofing using Gaussian Mixture Model machine learning [4] on abnormality detection in the pseudo-ranging from different satellites of the GNSS offers an effective unsupervised machine learning mechanism without any long training process. Providing a digital signature on authentic GNSS signal and relaying this signature to the IoT edge devices to verify the received GNSS signal have genuinely proved to be reliable. The demonstrated experimental campaign illustrates its effectiveness for integrity check under the dynamic mobility of IoT edge devices. However, there is room for research and development for resource-limited IoT devices. Both machine learning inference and the frequent dynamic digital signature requests between the client and server will put a demanding energy consumption on the power limited IoT edge devices especially if deployed on drones.

The usage of IoT edge devices such as drones have been prevalent not only in military domain but also in many recent commercial applications such as façade inspection and surveillance operation. However, the Achilles heel for drone applications is the short operation duration due to limited battery capacity. Dr. Henrik Hesse, from the University of Glasgow, UK, shares his research outcome on the development of perching drones for distributed communication in IoT applications [5]. The perching concept reduces the power consumption of drones which overcomes the shortcoming of drones by extending their operating time. This enables the use of drones as reliable IoT edge devices using drones to transport and deploy IoT sensors as desired locations [6]. The novel perching concept pivots on the use of electromagnetic perching compared to traditional mechanical perching to attach to vertical or horizontal surfaces. The novel use of electro-permanent magnets (EPMs) allows the attachment of drones on any ferromagnetic metal surface even when the operating current is being switched off. This capability provides substantial saving in the energy consumption of drones and allows it to focus on mission-critical operations. A small residual current is only needed to reverse the polarity of the EPM under the hysteresis loop to allow detachment from the surface. Experimental demonstration has shown the feasibility of this new concept for electromagnetic perching in different attachment angles between the drone and the surface. Discussion has ensued on the viability of the perching drones on non-ferromagnetic surface. Although in modern smart cities, numerous buildings have surfaces that are made of ferromagnetic materials. These buildings will easily allow the electromagnetic perching drone to rest securely on these surfaces. However, the discussion has created many research opportunities to venture into future solutions that allow perching on non-ferromagnetic surfaces. Such solutions will facilitate the unconstrained operation of drones and offer an energy-saving mechanism to extend the operational time of drones without compromising safety during flight operation.

The importance of safety of drones, also referred to as Unmanned Aerial Vehicle (UAV), is critical, especially if there is possibility of endangering human during flight operation, such as crashes during the building facade inspection in outdoor environments. Xin Xin, principal engineer from TUV SUD, a well-known German company in quality inspection and certification, shares how the company is enhancing UAV flight safety through sensor-based runtime risk assessment [7]. The proposed assessment is contrary to traditional passive risk assessment where the likelihood of safety risks and severity of their consequences are established before any flight operation can begin. The novel approach proposed by TUV SUD provides an active assessment by incorporating real-time data from Inertial Measurement Unit (IMU) onboard the UAV to actively provide real-time estimates of potential hazard for the current operation. This allows the operator to obtain predictive analysis of the UAV flight health status during flight and before any potential catastrophe can occur. However, there is some discussion evolving the instability and drift of the IMU to be addressed before implementation and experimental setup can be meaningfully carried out. This leads to research pivoting towards predictive algorithms for health monitoring such as Kalman filtering to observe the drift phenomena or understanding the effective operational duration of IMUs. In the context of Internet of Drones [8] online risk assessment will provide a reliable approach for operating drone swarms autonomously around cities.

REFERENCES

[1] K.G. Yu, “Land Application of GNSS Reflectometry,” *IEEE World Forum on Internet of Things, Invited Speaker, Workshop 5*, Nov. 2022, Japan.

[2] C.K. Seow, “GNSS Vulnerability,” *IEEE World Forum on Internet of Things, Invited Speaker, Workshop Session 5*, Nov. 2022, Japan.

[3] R.Y. Zhang, C.K. Seow, K.Wen and H. Zhang, “Spoofing Attack of Drone,” *2018 IEEE 4th International Conference on Computer and Communications (ICCC)*, pp. 1239–1246, 2018, Chengdu, China

[4] Z.J. Feng, C.K. Seow and Q. Cao, “GNSS Anti-Spoofing Detection on Gaussian Mixture Model Machine Learning,” *IEEE 25th Int. Conf. Intelli. Transportation Syst. (ITSC)*, pp. 3334–3339, 2022, Macau, China

[5] J.M. Liu, W. Yik, B. Saw and H. Hesse, “Perching Drones for Distributed Communication Systems in IoT Applications,” *IEEE World Forum on Internet of Things, Workshop Session 5*, Nov. 2022, Japan.

[6] P. N. Beuchat, H. Hesse, A. Domahidi and J. Lygeros, "Enabling Optimization-Based Localization for IoT Devices," in *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5639-5650, Jun 2019.

[7] Y.Z. Lim, X. Xin and T. P. Khoo “Enhancing UAV Flight Safety through Sensor-based Runtime Risk Assessment,” *IEEE World Forum on Internet of Things, Invited Speaker, Workshop Session 5*, Nov. 2022, Japan.

[8] Z. Kaleem and M. H. Rehmani, "Amateur drone monitoring: State-of-the-art architectures key enabling technologies and future research directions", *IEEE Wireless Commun.*, vol. 25, no. 2, pp. 150-159, Apr. 2018