УДК 621.39

INFORMATION TRANSMISSION PROBLEMS IN DUAL-PURPOSE IOT SOLUTIONS

Klishchuk V., Osypchuk S.
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"
E-mail: serg.osypchuk@gmail.com, vklishchuk@gmail.com

ПРОБЛЕМИ ПЕРЕДАВАННЯ ІНФОРМАЦІЇ В РІШЕННЯХ IOT ПОДВІЙНОГО ПРИЗНАЧЕННЯ

Our research delves into the crucial realm of IoT dual-purpose systems (DPS). We meticulously analyse the information transmission problems (ITP) in IoT DPS and provide a comprehensive list of techniques to mitigate them. We also present a high-level design of wearable health monitoring devices and a network diagram, showcasing one of the many applications of IoT DPS.

Internet of Things (IoT) refers to the network of physical objects or "things" embedded with sensors, software, and other technologies that enable them to connect and exchange data with other devices and systems over the Internet without human intervention.

The dual-purpose system (DPS) is designed to serve two distinct functions or purposes simultaneously.

IoT DPS, which can serve personal, industrial, or enterprise applications, is crucial in various fields, including engineering, healthcare, or military applications. By combining multiple capabilities of IoT applications into a single solution, IoT DPSs enhance efficiency and flexibility, thereby optimising resources and functionality. This is particularly significant in the face of increasing risks of conflicts and threats, underscoring the importance of IoT DPS research and development. *Table 1* showcases examples of IoT DPS designed explicitly for civil and military applications, emphasising their relevance.

Information transmission problem (ITP) refers to any issue or challenge that hinders the effective and reliable transfer of information from one point to another within a system or network. ITP can arise due to various factors, such as *technical limitations, environmental conditions, security concerns, or protocol inefficiencies*.

The *relevance of IoT DPS research and development* is the increased risks of conflicts and threats nowadays. Thus, proper attention must be paid to addressing the ITPs in IoT DPSs. *Table 2* shows critical ITPs in IoT DPSs.

Addressing ITP often requires developing and implementing appropriate technologies, protocols, and strategies tailored to the specific requirements and constraints of the communication system or network.

Task statement. The objective is to address the urgent need to reduce risks in military and civilian cases that could lead to lethal results: review the *wearable health monitoring devices (WHMD)* scenario [1-3]. This will be achieved by applying techniques for addressing ITPs in the IoT DPS listed in Table 2.

Table 1. Examples of the IoT DPS.

№	Dual-purpose system (DPS)	Civil Application	Military Application
1	Wearable health monitoring devices	Monitoring of vital signs, activity levels, sleep, patterns for patients with chronic conditions, fitness, tracking for wellness purposes	Remote health monitoring of soldiers in the field, tracking physiological indicators during missions, assessing fatigue and stress levels
2	Unmanned aerial vehicles (UAVs) or Drones	Aerial photography, mapping, surveillance, monitoring of infrastructure, agriculture, environmental conditions	Intelligence, surveillance, reconnaissance, target acquisition, battlefield situational awareness
3	Smart city infrastructure	Urban management, traffic control, public safety, environmental monitoring, energy efficiency	Critical infrastructure protection, emergency response coordination, support for military installations
4	Border surveillance systems	Border security, customs enforcement, monitoring of immigration, cross-border movements	Border control, intelligence gathering, detection of illicit activities, prevention of unauthorised incursions
5	Emergency response and disaster management	Early warning systems, disaster preparedness, search and rescue operations, humanitarian assistance	Rapid deployment of forces for disaster relief, coordination of emergency response efforts

Table 2. Information transmission problems (ITP) in the IoT DPS.

№	ITP	Challenges	Techniques for addressing ITP
1	Communication channel noise and signal interference, reliability, and error correction	External factors that distort or corrupt the transmitted signals, leading to errors in data reception, reliable data transmission	Channel coding, error detection and correction, modulation techniques and multiposition keying (MPK), antenna diversity, frequency hopping spread spectrum (FHSS), adaptive filtering, cyclic redundancy check (CRC), OFDM, dynamic spectrum access, automatic/selective/hybrid repeat request (ARQ), LDPC codes, interleaving, concatenated coding, soft decision decoding, iterative decoding, and combinations of these techniques
2	Security threats	Unauthorised access to the data, confidentiality breach of the transmitted data, data integrity or availability	Data encryption (AES, RSA, ECC), authentication and authorisation, keys management, secure protocols (TLS, IPSec, SSH, HTTPS), firewalls, intrusion detection systems (IDS), packet filtering, traffic analysis, virtual private networks (VPN), secure network design (segmentation, least privilege access)
3	Reliable design	Lack of shockproof, waterproof, autonomous power for long-lasting work	Shock-absorbing materials, vibration-dampening mounts, solder joints and connectors, sealed enclosures, energy harvesting, energy-efficient components, economic power-management system, battery backup to allow communication to continue

The WHMD solution involves attaching IoT sensors to human individuals to collect telemetry data, encrypting and transmitting that information to storage facilities and to authorised personnel. Advances in Microelectromechanical Systems (*MEMS*) technology have resulted in the development of small and robust sensors that can monitor various parameters such as human movement, temperature, and others. The modern concept of Wireless Body Area Sensor Networks (*WBASN*) allows the integration of different networks and devices for remote monitoring. The WBASN structure consists of three *key stages* (Figure 1):

1. Data gathering about and around the human body.

2. Communication between humans and the command centre via ZigBee, Bluetooth, UWB, IEEE 802.11 a/b/g/n/ah WLAN, and 3G/4G cellular technologies at different steps of network design.

3. The overall WHMD communication scenario is managed by appropriately reacting to the gathered data.

All the ITP problems in Table 2 are applicable to this IoT DPS WHMD use case, and proper techniques for addressing ITP can be used.

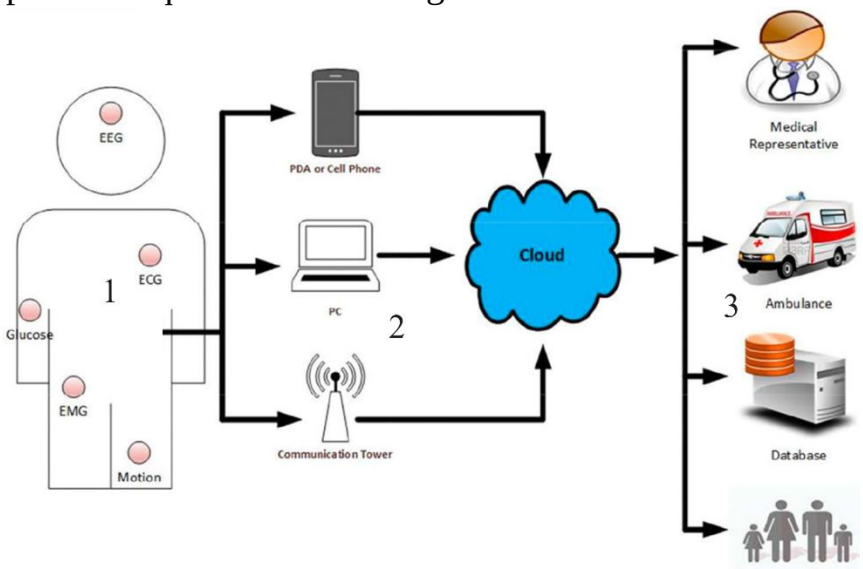

Figure 1. WBASN communication scheme.

In conclusion, our research has shown that IoT dual-purpose systems must be appropriately designed considering existing threats worldwide. By doing so, we can create reliable solutions with cost savings, eliminating the need to develop different systems. Our research provides techniques for addressing common information transmission problems.

References

1. Al Ameen, M., Liu, J. & Kwak, K. Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications. *J Med Syst* 36, 93–101 (2012). https://doi.org/10.1007/s10916-010-9449-4.

2. Khan RA, Pathan A-SK. The state-of-the-art wireless body area sensor networks: A survey. *International Journal of Distributed Sensor Networks*. 2018; 14(4). https://journals.sagepub.com/doi/10.1177/1550147718768994.

3. Bin Ahmad, M., Asif, M., Masood, K., Al Ghamdi, M. A., Almotiri, S. H., & Nagra, A. A. (2022). A Reliable Framework for Secure Communication and Health Assessment of Soldiers in the Battlefield. Sage Open, 12 (4). https://doi.org/10.1177/21582440221130300.