# CONCLUSION

Despite the necessary digitization of the healthcare ecosystem, the IoMT progression and mainly the insecure nature of the legacy healthcare systems increase the attack surface. In this article, we paid our attention to the IEC 60 870-5-104 protocol, which is widely adopted by the industrial systems in the healthcare sector. In particular, first, we introduced a quantitative threat model, which evaluates the severity of the possible cyber attacks with respect to the corresponding IEC 60 870-5-104 commands. Next, we provided an IDPS system, which combines ML and SDN in order to detect and mitigate the IEC 60 870-5-104 cyber attacks. The intrusion detection relies on a CART classifier that uses the TCP/IP network flow statistics and IEC 60 870-5-104 payload flow statistics. On the other side, the SDN-based mitigation is transformed into a MAB problem solved with the TS method. The evaluation results demonstrated the efficiency of the proposed IDPS. Our future plans related to this work are focused on enhancing the proposed IDPS so that it can detect multistep cyber attacks related to IEC 60 870-5-104 and other industrial and IOMT protocols utilized in the healthcare sector, such as Mod bus, MQTT, and Ether CAT. To this end, ML-based association rules techniques will be adopted.