ABSTRACT

23/09/20222

CYBERATTACK DETECTION FOR ELECTRIC VEHICLES USING PHYSICS-GUIDED MACHINE LEARNING

With the development of IoT and connectivity in the automotive industry, cyber security concerns are affecting every element of electric vehicles, including the battery, motors, and steering. Security threats to power electronics systems are growing dramatically every day. M alicious hackers attempt to get data from vehicle systems and deploy it . High level tampering of current and voltage signals is seen in the motor drive. For cybersecurity solutions, hardware- and software-based detection techniques are employed. In actual applications, the system is taught offline before being used to detect cyberattacks in real time. Attention on cyberattack detection that is adaptive can be modified by online driving data and more detailed Electric Vehicle physical parameters. Performance may get decline after a cyberattack. As a result, virus attack detection on EVs is done using machine learning in efficient way.

References

[1] J.C Balda, A. Mantooyh,R. Blum and P.Tenti,". *A "Cybersecurity and power electronics: Addresing the security vulnerabilities of the Internet of Things".* IEEE Power Electron Mag vol 4

[2] Lulu Guo ,Jin Ye, Bowen Yang IEEE Transaction on Transportation Electrification 3 sept 2021

Guide,
Prof. D. M. Padulkar
Deptt. of AIDS. Engg.

Student,
Yashraj Deepak Devrat
TE(AIDS. Engg.) Roll No. 2237031