Model for Study of Malware Propagation Dynamics in Wireless Sensor Network

Title	Model for Study of Malware Propagation Dynamics in Wireless Sensor Network
Publication Type	Conference Paper
Year of Publication	2019
Authors	Biswal, Satya Ranjan, Swain, Santosh Kumar
Conference Name	2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)
Date Published	apr
Keywords	Analytical models, composability, Computational modeling, computer viruses, critical security challenges, detection, early detection method, Epidemic model, epidemiology basic reproduction number, Equilibrium points, Grippers, Human Behavior, invasive software, malicious signals presence, Malware, malware propagation dynamics, malware spread, malware status, Metrics, neighboring sensor nodes, Propagation, pubcrawl, Resiliency, security mechanism, sensor security, Stability analysis, Susceptible-Exposed-Infectious-Recovered-Dead model, telecommunication security, Wireless Sensor Network, Wireless sensor networks, WSN
Abstract	Wireless Sensor Network (WSN) faces critical security challenges due to malware(worm, virus, malicious code etc.) attack. When a single node gets compromised by malware then start to spread in entire sensor network through neighboring sensor nodes. To understand the dynamics of malware propagation in WSN proposed a Susceptible-Exposed-Infectious-Recovered-Dead (SEIRD) model. This model used the concept of epidemiology. The model focused on early detection of malicious signals presence in the network and accordingly application of security mechanism for its removal. The early detection method helps in controlling of malware spread and reduce battery consumption of sensor nodes. In this paper study the dynamics of malware propagation and stability analysis of the system. In epidemiology basic reproduction number is a crucial parameter which is used for the determination of malware status in the system. The expression of basic reproduction number has been obtained. Analyze the propagation dynamics and compared with previous model. The proposed model provides improved security mechanism in comparison to previous one. The extensive simulation results conform the analytical investigation and accuracy of proposed model.
DOI	10.1109/ICOEI.2019.8862736

Citation Key biswal_model_2019

telecommunication security malware invasive software Resiliency Human behavior pubcrawl composability wireless sensor networks Computational modeling Metrics Analytical models detection sensor security Stability analysis security mechanism Wireless Sensor Network WSN computer viruses critical security challenges early detection method Epidemic model epidemiology basic reproduction number Equilibrium points Grippers malicious signals presence malware propagation dynamics malware spread malware status neighboring sensor nodes Propagation Susceptible-Exposed-Infectious-Recovered-Dead model