عنوان مقاله:
تشخیص و جداسازی عیب از حمله سایبری در سامانه SCADA با اتکا به پارامترهای شبکه

محل انتشار:
فصلنامه مهندسی برق دانشگاه تبریز, دوره 51, شماره 4 (سال: 1401)

تعداد صفحات اصل مقاله: 8

نویسندگان:
حسین مصفا - *فارغ التحصیل کارشناسی ارشد، گروه کنترل مهندسی برق، دانشگاه صنعتی خواجه نصیرالدین طوسی، تهران، ایران*

حمید حالوزاده - *استاد، دانشکده مهندسی برق، گروه کنترل، دانشگاه صنعتی خواجه نصیرالدین طوسی، تهران، ایران*

خلاصه مقاله:
سامانه SCADA سامانه ای حیاتی می باشد که فرایندهای صنعتی را نظارت و کنترل می کند. در این سامانه با نفوذ در راه های ارتباطی بین حسگرها، عملگرها و سرورها حمله سایبری رخ می دهد. در سال های اخیر حمله سایبری مشکلاتی را برای سامانه های کنترل صنعتی به بار آورده است. حمله سایبری از نظر اختلال در سامانه، عملکردی شبیه به وقوع عیب در آن دارد. در اختیار داشتن لحظه ای پارامترهای شبکه مانند تاخیر انتها به انتها، از دست رفتن بسته و ترافیک شبکه می‌تواند بین عیب و حمله سایبری تمایز ایجاد کند. هدف از این پژوهش ابتدا تشخیص و سپس جداسازی عیب از حمله سایبری در سامانه ی SCADA با استفاده از پارامترهای شبکه است. برای این‌کار یک سامانه ی عبور سیال به همراه یک کنترل کننده مدلسازی شده است. برای این سامانه فیلتر تشخیص عیب برد (BFDF) طراحی شده است که ناهنجاری های مختلف سامانه را مشخص می کند. اگر در زمان تشخیص ناهنجاری توسط فیلتر، پارامترهای شبکه نیز شرایط غیرعادی را نشان بدهد، حمله سایبری تشخیص داده می شود. شبیه سازی ها در نرم افزار Omnet++ انجام شد. نتایج پژوهش موثر بودن این روش در تفکیک عیب و حمله سایبری را نشان داد.

کلمات کلیدی:
تشخیص عیب, حمله سایبری, حمله داس, سیستم SCADA, فیلتر تشخیص عیب برد (BFDF), نرم افزار OMNET++