Detection of Man-in-the-Middle Attacks on

Industrial Control Networks

*Abstract*—In this paper we present a method to detect

Man-in-the-Middle attacks on industrial control systems. The approach uses anomaly detection by developing a model of normal behavior of the industrial control system network.

To come as close as possible to reality a simple industrial System, a conveyor belt with sensors and actuators, was set up with controllers widely used in industry. A machine learning approach based on the k-Nearest Neighbors algorithm with Bregman divergence was used to define a model of normal (valid) behavior. Afterwards Man-in-the-Middle attacks were launched against the system and its behavior during the attack was compared to the valid behavior model. The results show that the approach taken was able to detect such attacks with satisfactory accuracy.

# چکیده

 رادر سیستم ها ی کنترل صنعتی ارایه می دهیم.روشی که مااز آن استفاده کردیم Man in middleدر این مقاله ما تشخیص حمله ی
تشخیص ناهنجاری از طریق مدل رفتار نرمال شبکه های کنترل صنعتی است.به منظور نزدیک شدن به واقعیت سیستم ها ی صنعتی ما یه تسمه نقاله با سنسور ها و محرک ها را به کنترلر هایی که به طور گسترده در صنعت استفاده میشود را پیاده سازی کردیم.
 نزدیک ترین همسایه واگرایی برگمن است .از این الگوریتم درتعریف k روش یادگیری ماشین مبتنی بر الگوریتم
را روانه چنین سیستمی کردیم و رفتار حاصل man in middle تعریف مدل نرمال (معتبر )استفاده کردیم حملات از نوع
را با رفتار عادی مقایسه کردیم نتایج بیان گر این حقیقت بود که این روش قادر به شناسایی حمله با دقت قابل قبولی است