

فهرست مطالب

صفحه	عنوان
۱	فهرست مطالب
۲	فهرست تصاویر
۱	مقدمه

فهرست تصاویر

عنوان

صفحه

فصل ۱

مقدمه

پیشرفت‌های اخیر در سیستم‌های کنترل و مانیتورینگ شبکه هوشمند^۱ مانند قابلیت ارتباط دو طرفه، به طور چشمگیری امنیت و کارایی شبکه را افزایش داده است [۴]. هرچند که در کنار این مزایا، به دلایلی مانند گسترده بودن و پراکندگی از نظر جغرافیایی، استفاده از زیرساخت‌های پیچیده مخابراتی، تبادل اطلاعات از طریق شبکه‌هایی مانند شبکه‌های کامپیوتری و ... موجب مشکلات و چالش‌هایی نظیر آسیب‌پذیری سیستم در برابر حمله‌های سایبری و به وجود آمدن تاخیرهای اضافی در سیستم شده است.

حمله‌های سایبری عموماً با هدف ایجاد اختلال در، در دسترس بودن^۲، یکپارچگی^۳ و قابلیت اطمینان شبکه^۴ انجام می‌شود [۴]. یک دسته‌ی جدید و مهم از حمله‌های سایبری با نام حمله‌ی تزریق داده‌ی غلط^۵ در سال‌های اخیر معرفی شده‌اند که یکپارچگی شبکه را تحت تاثیر قرار می‌دهند. در حمله‌ی تزریق داده‌ی غلط حمله‌کننده داده‌های دریافتی از سنسورها و واحدهای اندازه‌گیری فازور را به منظور فریب دادن مرکز کنترل دستکاری می‌کند^۶ و در نتیجه‌ی این تغییرات مرکز کنترل تصمیمات اشتباهی را اتخاذ می‌کند که می‌تواند نتایج فاجعه‌باری را به دنبال داشته باشد. به عنوان مثال^۷ یکی از نمونه‌های حمله سایبری به شبکه برق، دسامبر سال ۲۰۱۵ در اوکراین اتفاق افتاد که موجب خاموشی برق ۲۲۵ هزار مشتری از جمله مراکز درمانی مانند بیمارستان‌ها^۸ به مدت حدوداً سه ساعت شد [۴]. از این رو، بررسی دقیق حملات سایبری اهمیت ویژه‌ای پیدا کرده و شمار زیادی از مقالات سال‌های اخیر را به خود اختصاص داده است که این نوع حملات را از جهات مختلف مانند نحوه ایجاد حمله، مکانیزم‌های دفاع و پیشگیری و تشخیص هر چه سریع‌تر حمله در صورت اتفاق افتادن

¹Smart grid

²Availability

³Integrity

⁴Confidentiality

⁵False Data Injection Attack(FDIA)

⁶Hack

⁷example

⁸HospitALS

بررسی کرده‌اند.

مقالاتی که حمله‌های سایبری از نوع تزریق داده‌ی غلط را مورد بررسی قرار داده‌اند از یک دیدگاه می‌توانند به سه دسته‌ی کلی تقسیم شوند. دسته‌ی اول مقالاتی هستند که نحوه ایجاد حمله و استراتژی‌هایی را که هکر^۱ جهت ایجاد حمله به کار می‌برد، مورد بررسی قرار می‌دهند. دسته‌ی دوم به اثرات حمله تزریق داده غلط (FDIA)^۲ بر روی شبکه‌ی برق هوشمند می‌پردازد. آخرین دسته از مقالات مربوط به این حوزه با توجه به استراتژی‌های هکر جهت تزریق داده غلط، راهکارهایی برای دفاع و پیشگیری از وقوع حمله و آشکارسازی^۳ در صورت وجود حمله ارائه می‌دهد. در ادامه ابتدا پیشینه‌ی مختصری از مقالات دسته‌ی اول و دوم آورده می‌شود و سپس به دلیل تمرکز پایان‌نامه بر روی تشخیص حملات شرح مبسوطی از مقالاتی که به راهکارهای تشخیص حمله در شبکه‌های WAMS^۴ پرداخته‌اند، بیان می‌شود و مزایا و معایب روش‌های پیشنهاد شده مورد بررسی قرار می‌گیرند.

در بخش بعد با در نظر گرفتن تاخیر ناشی از شبکه‌های ارتباطی که یک ویژگی مهم و چالش برانگیز شبکه‌های WAMS محسوب می‌شود و نتیجه‌گیری از مقالاتی که در زمینه تشخیص حمله در شبکه‌های WAMS مورد بررسی قرار گرفته‌اند، هدف از انجام پایان‌نامه و روش استفاده شده در این تحقیق^۵ به منظور تشخیص حمله بیان می‌شود. سپس با توجه به هدف پایان‌نامه، مقاله‌هایی که به مسئله‌ی تاخیر پرداخته‌اند نیز بررسی می‌شوند.

در پایان^۶ نیز بخش‌بندی پایان‌نامه^۱ با توجه به مطالب قبلی گفته شده در این فصل^۲ انجام می‌شود.

^۱Hacker

^۲False data injection attack

^۳Detection

^۴Wide Area Measurement System

^۵Research

^۶end

^۱Thesis

^۲chapter