Detection and isolation of fault from cyber attack in SCADA systems using network parameters

Hossein Mosaffa, Hamid Khaloozadeh*

Faculty of Electrical Engineering, K. N. Toosi University of Technology, Tehran, Iran
E-mails: h.mosaffa@email.kntu.ac.ir; h_khaloozadeh@eetd.kntu.ac.ir
Received: 09-01-2022, Accepted: 30-04-2022.

Short Abstract
The SCADA system is a vital system that monitors and controls industrial processes. In these systems, a cyber attack occurs by infiltrating the communication channels between sensors, actuators and servers. In recent years, cyber-attacks have created problems for industrial control systems. A cyber attack has a function similar to a fault in terms of system malfunction. Having instantaneous network parameters such as latency, packet loss, and network traffic can probably make the difference between a fault and a cyber attack. The purpose of this initial research is to detect and then isolate the fault from the cyber attack of the SCADA system using different networks. To do this, a fluid passage system with a controller is modeled. A fault detection filter (BFDF) was designed, which detects various anomalies of the system, If at the time of detection of the anomaly by the filter, the network parameters also show abnormal conditions, a cyber attack is detected. The simulations were performed in Omnet ++ software. The research results showed the effectiveness of this method in distinguishing between fault and cyber attack.

Keywords
Beard fault detection filter (BFDF), cyber attack, DoS attack, fault detection, OMNET++ software, SCADA system.

1- Short Introduction

The SCADA system is used in the vital infrastructure of countries. It collects and monitors real-time infrastructure's data. With the increasing number of cyber-attacks and the impact that these attacks have on society in terms of economics and health, research on the security of SCADA systems has increased. The source of the fault and the cyber attack are different, but they have almost the same effect on the system. A cyber attack is likely to have a significant impact on the network. Therefore, network parameters can also be examined to distinguish between a cyber attack and a fault. This article examines the conditions that the system experiences and distinguishes between a cyber attack and a fault by analyzing test data.

2- Proposed Work and Methodology (including comprision, simulation/experimental results and discusion)

In this paper, first the BFDF filter is introduced and its details are reviewed. A system is then modeled and a BFDF filter is designed for it. Also, four correlations are defined, which represent four different faults of the system. Then, by simulating the system in Omnet ++ software, network parameters are added besides physical data as available data to separate the fault and cyber attack. In Omnet ++ software, various faults and cyber attacks are created on the system, and with the obtained algorithm, a distinction is made between the fault and the cyber attack.

3- Conclusion

In this paper, a networked control system(NCS) was modeled in which the controller and the system were interconnected by Internet protocols. Then a BFDF filter was designed for this system. This filter detects and distinguishes various system anomalies, including anomalies in the actuators, sensors and parameters of the system. This system was simulated in Omnet ++ software and various faults and cyber attacks were applied on it. By having network parameters besides residual values and correlations, the isolation of faults and cyber attacks were effective and finally an algorithm was written for it.

4- References

- T.-Y. Zhang and D. Ye, "False data injection attacks with complete stealthiness in cyber–physical systems: A self-generated approach," *Automatica*, vol. 120, p. 109117, 2020.
- J. Rønneberg, "Reference Topologies and Scenarios for Cyber-Physical Systems in the Norwegian Cyber Range," NTNU, 2019.
- M. Taheri, K .Khorasani, I. Shames, and N. Meskin, "Cyber Attack and Machine Induced Fault Detection and Isolation Methodologies for Cyber-Physical Systems," arXiv preprint arXiv:2009.06196, 2020.
- W. Werth, "Towards distinguishing between cyber-attacks and faults in cyber-physical systems," 2014

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

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

حمید خالوزاده
استاد، دانشکده مهندسی برق، گروه کنترل، دانشگاه صنعتی خواجه نصیرالدین طوسی، تهران، ایران

چکیده
سامانه SCADA سامانه‌ای حیاتی می‌باشد که فرایندهای صنعتی را نظارت و کنترل می‌کند. در این سامانه با نفوذ در راه‌های ارتباطی بین حسگرها، عملگرها و سرورها حمله سایبری رخ می‌دهد. در سال‌های اخیر حمله سایبری مشکلاتی را برای سامانه‌های کنترل صنعتی به بار آورده است. حمله سایبری از نظر اختلال در سامانه، عملکردی شبیه به وقوع عیب در آن دارد. در اختیار داشتن لحظه‌ای 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 سامانه‌ی SCADA با استفاده از پارامترهای شبکه است. برای این‌کار یک سامانه‌ی عبور سیال به همراه یک کنترل کننده مدلسازی شده است. برای این سامانه فیلتر تشخیص عیب برد (BFDF) طراحی شده است که ناهنجاری‌های مختلف سامانه را مشخص می‌کند. اگر در زمان تشخیص ناهنجاری توسط فیلتر، پارامترهای شبکه نیز شرایط غیرعادی را نشان بدهد، حمله سایبری تشخیص داده می‌شود. شبیه سازی‌ها 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++.

نام نویسنده مسئول: دکتر حمید خالوزاده
ایمیل نویسنده مسئول: h_khaloozadeh@eetd.kntu.ac.ir

تاریخ ارسال مقاله: ۱۴۰۰-۱۰-۱۹
تاریخ پذیرش مقاله: ۱۴۰۱-۰۲-۱۰

۵- مقدمه

سامانه اسکادا (SCADA) نوعی سیستم سایبری-فیزیکی (CPS) است که در زیرساخت‌های حیاتی کشورها مانند شبکه برق، شبکه آبرسانی شهری، پالایشگاه‌های نفت و کارخانه‌های شیمیایی کاربرد دارد. استفاده از شبکه‌های ارتباطی در این سامانه‌ها باعث شده است که در برابر حمله‌های سایبری آسیب پذیر باشند. حملات سایبری احتمالی به این سیستم‌ها ممکن است تأثیر منفی بر اقتصاد، محیط زیست و امنیت ملی داشته باشد [۱, ۲]. در تازه‌ترین حمله سایبری به تاسیسات کشور می‌توان حمله به سامانه‌ی هوشمند سوخت در آبان ۱۴۰۰ را نام برد.

به طور کلی، بخش فیزیکی CPSها توسط لایه سایبری آن که شامل سنجش، محاسبات و ارتباطات است، نظارت یا کنترل می‌شود. با این حال، لایه سایبری در برابر حملات سایبری آسیب پذیر است و می‌تواند به طور غیر مستقیم بر سیستم فیزیکی تأثیر بگذارد. حمله سایبری را می‌توان به سه دسته اصلی دسته بندی کرد: حمله انکار سرویس (DoS)، حمله تکرار(Replay) و حمله تزریق داده‌های غلط(FDI). حمله DoS می‌تواند کانال‌های ارتباطی را مختل کند تا جلوی دریافت داده‌ها گرفته شود [۳-۵]. حمله Replay داده‌های ارتباطی را ضبط و پوشش می‌دهد تا عملکرد سیستم کاهش یابد [۶]. از بین حمله‌های فوق، حملات FDI که داده‌ها را در لایه سایبری تغییر می‌دهند، خطرناک‌تر و پیچیده‌تر هستند [۷]. بر اساس مکان وقوع حمله نیز حملات FDI را می‌توان به حمله‌ی عملگر [۸, ۹] و حمله‌ی حسگر [۱۰-۱۳] طبقه بندی کرد. تشخیص این حملات که اثری همانند بروز عیب در سیستم دارد، می‌تواند از بروز خسارت به آن جلوگیری کند.

توانایی تشخیص عیب و حمله سایبری می‌تواند اثر مفیدی برای پاسخ بهتر سامانه اسکادا به شرایط مختلف داشته باشد. منشأ عیب و حمله سایبری متفاوت است ولی آن‌ها تقریبا اثر یکسانی بر سامانه دارند؛ به عنوان مثال انحراف در یک حسگر می‌تواند در اثر بروز عیب در آن و یا وقوع حمله سایبری در کانال ارتباطی آن ایجاد شده باشد. بنابراین استفاده از داده‌های فیزیکی به تنهایی نمی‌تواند عیب و حمله سایبری را از یکدیگر تفکیک کند. حمله سایبری به احتمال زیاد تاثیر خاصی روی شبکه خواهد داشت. بنابراین منطقی است که پارامترهای شبکه نیز علاوه بر داده‌های فیزیکی سامانه مطالعه شود [۱۴-۱۶].

در شبکه‌های کامپیوتری، به هر دستگاه که در شبکه امکان ارسال و دریافت اطلاعات را داشته باشد، گره (Node) گفته می‌شود. همچنین برای تبادل اطلاعات، داده‌های بزرگ به قسمت‌های کوچکتر تقسیم می‌شوند و هر یک از این قسمت‌ها را بسته (Packet) می‌نامند. پارامترهای شبکه که تغییرات آن‌ها قابل بررسی است، تاخیر انتها به انتها (end to end delay)، جیتر (Jitter) و توان عملیاتی شبکه (Throughput) است. تاخیر انتها به انتها، مدت زمانی است که یک بسته در گره فرستنده ساخته می‌شود و با موفقیت به گره گیرنده می‌رسد. واریانس تاخیر انتها به انتها نیز جیتر نام دارد. توان عملیاتی شبکه، نرخ تحویل موفقیت آمیز پیام از طریق شبکه‌ی ارتباطی است و واحد آن بیت بر ثانیه(bps) می‌باشد [۱۴].

در این مقاله امکان تشخیص عیب و حمله سایبری و تفکیک آن‌ها بررسی می‌شود. بدین منظور برای تشخیص ناهنجاری‌هایی که در سیستم می‌تواند رخ دهد، از فیلتر تشخیص عیب برد (BFDF) استفاده شد. فیلتر BFDF یک مشاهده‌گر خطی است که بهره آن به گونه‌ای به دست می‌آید که در زمان رخ دادن یک عیب، مانده در جهت مشخص و ثابت پاسخ دهد. بنابراین در فضای مانده، هر عیب جهت منحصر به فرد خود را دارد و همراستا شدن مانده با آن جهت، نوع عیب را در سیستم مشخص خواهد کرد [۱۷, ۱۸]. تعدادی از پژوهشگران نیز از الگوریتم‌های استاندارد تشخیص عیبِ مبتنی بر مدل مانند مشاهده‌گر ورودی ناشناخته (UIO) برای تشخیص حملات سایبری استفاده کرده اند [۱۹-۲۱]. هُمایی در [۲۲] به مدلسازی حمله FDI در سیستم قدرت و تشخیص آن با استفاده از فیلتر کالمن و آشکارساز χ^2 پرداخته است.

بررسی پارامترهای شبکه در کنار خروجی فیلتر، به دلیل مستقل بودن این دو متغیر از هم، در حقیقت ابعادی را به فضای مانده‌ها اضافه می‌کند که در این فضای جدید، قابلیت تفکیک عیب و حمله سایبری میسر می‌شود.

ورث با استفاده از داده‌های فیزیکی و اطلاعات شبکه به تفکیک عیب و حمله سایبری با الگوریتم‌های یادگیری ماشین می‌پردازد. این کار را با شبیه سازی وضعیت‌های مختلف یک سامانه در نرم افزار Omnet++ انجام می‌دهد [۱۵]. Omnet++ یک نرم افزار قابل توسعه، با برنامه‌ریزی مجموعه‌ای و مبتنی بر اجزا است و برای ساخت شبیه‌سازی‌های شبکه در سیستم‌های فیزیکی-سایبری نیز استفاده می‌شود و شامل شبکه‌های ارتباطی بی‌سیم و سیمی و همچنین توپولوژی و پروتکل‌های مختلف شبکه است [۲۳, ۲۴]. رونبِرگ نیز اثر حمله‌ی سایبری بر پارامترهای شبکه را با شبیه سازی دو سامانه در نرم افزار Omnet++ و ایجاد حمله سایبری در آن‌ها بررسی کرد. او مشاهده کرد که پارامترهای شبکه مانند تاخیر انتها به انتها، جیتر و از دست رفتن بسته حین وقوع حمله‌ی سایبری افزایش یافته است [۱۴].

در این مقاله یک سیستم کنترل شبکه‌ای معرفی شده و برای آن فیلتر BFDF طراحی می‌شود. سپس سیستم در نرم افزار Omnet++ شبیه سازی می‌گردد تا دسترسی لحظه‌ای به پارامترهای شبکه نیز فراهم شود. در پایان بر اساس خروجی فیلتر و پارامترهای شبکه وقوع عیب یا حمله سایبری تشخیص داده می‌شود.

۶- مواد و روش

در این بخش ابتدا فیلتر BFDF معرفی و جزئیات آن بررسی می‌شود. سپس در بخش مطالعه‌ی موردی یک سیستم مدلسازی و برای آن فیلتر BFDF طراحی می‌شود. در ادامه نیز از پارامترهای شبکه برای تشخیص عیب و حمله سایبری از یکدیگر استفاده می‌شود.

۶-۱- فیلتر تشخیص عیب برد (BFDF)

فرم فضای حالت یک سیستم گسسته‌ی خطی تغییر ناپذیر با زمان به صورت معادله ۱ تعریف می‌شود.

$$\begin{aligned} x_{k+1} &= Ax_k + Bu_k + b_i\xi_{i_k} + \Delta A \propto (x_k) + \Delta B\beta(u_k) \\ y_k &= Cx_k + I_j\eta_{j_k} \end{aligned} \quad (۱)$$

عبارت $\Delta A \propto (x_k) + \Delta B\beta(u_k)$ عیب در سامانه (انحراف و آشفتگی در پارامترهای سامانه) را نشان می‌دهد. عبارت‌های $b_i\xi_{i_k}$ و $I_j\eta_{j_k}$ نیز به ترتیب نمایانگر ناهنجاری (عیب یا حمله‌ی سایبری) در عملگرها و حسگرهای سامانه است. $b_i \in \mathcal{R}^n$ نمایانگر ستون i ام ماتریس B می‌باشد و $I_j \in \mathcal{R}^m$ بردار واحد نشان‌دهنده‌ی ناهنجاری در حسگر j ام است.

با فرض رؤیت پذیر بودن سامانه، فیلتر BFDF مانند معادله ۲ برای آن قابل تعریف است. البته در صورت رؤیت ناپذیر بودن، فرایند طراحی فیلتر جزئیات بیشتری دارد که در پژوهش‌های [۲۵-۲۷] قابل بررسی است.

$$\begin{aligned} &z_{k+1} = Gz_k + Dy_k + Bu_k \\ &r_k = y_k - Cz_k \\ &G = A - DC \;\rightarrow\; D = (A-G)C^{-1} \\ &G = \sigma_f I\,, |\sigma_f| < 1 \end{aligned} \quad (۲)$$

ماتریس D بهره مشاهده‌گر می‌باشد و باید به گونه‌ای طراحی شود که مانده در حضور هر ناهنجاری خاص، خاصیت تک جهتی داشته باشد. خطای تخمین حالت $\epsilon_k = x_k - z_k$ است. حال اگر ناهنجاری در عملگرها ایجاد شود، معادله‌ی خطای تخمین حالت و مانده به صورت معادله ۳ می‌شود.

$$\begin{aligned} \varepsilon_{k+1} &= (A-DC)\varepsilon_k + b_i\xi_{i_k} \\ r_k &= C\varepsilon_k \end{aligned} \quad (۳)$$

بنابراین مانده در فضای خروجی در راستای Cb_i تغییر می‌کند. اگر عیب در سامانه رخ دهد، به صورت ترکیب خطی ΔA و ΔB در فضای خروجی ظاهر می‌شود.

$$\begin{aligned} \varepsilon_{k+1} &= (A-DC)\varepsilon_k + \Delta A \propto (x_k) + \Delta B\beta(u_k) \\ r_k &= C\varepsilon_k \end{aligned} \quad (۴)$$

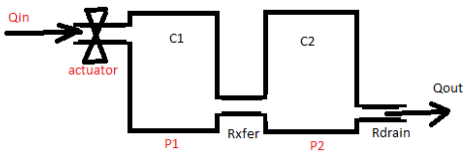
همچنین اگر انحراف در حسگرها رخ دهد، تغییرات مانده مانند معادله ۵ می‌شود. در معادله ۵، d_j ستون j ام ماتریس D می‌باشد.

$$\begin{aligned} \varepsilon_{k+1} &= (A-DC)\varepsilon_k - d_j\eta_{j_k} \\ r_k &= C\varepsilon_k + I_j\eta_{j_k} \end{aligned} \quad (۵)$$

ناهنجاری در حسگرها و عملگرها می‌تواند ناشی از عیب در آن‌ها و یا وقوع حمله‌ی سایبری باشد. فیلتر BFDF فقط وقوع ناهنجاری و مکان آن را تشخیص می‌دهد. در ادامه پارامترهای شبکه به عنوان پارامترهای مستقل از داده‌های فیزیکی، بُعدی را به این فضای مانده اضافه می‌کنند که در آن فضا تفکیک عیب و حمله سایبری تحقق می‌یابد.

۶-۲- مطالعه‌ی موردی

در این مقاله سامانه‌ی عبور سیال با دو مخزن مورد بررسی قرار گرفت. این سامانه دو حسگر فشار و یک عملگر (شیر کنترلی) دارد. با مدل‌سازی آن و جایگذاری مقدار پارامترها [۱۵]، فرم فضای حالت آن مانند معادله ۶ شد.



شکل ۱- شکل شماتیک سامانه‌ی سیال با دو مخزن

$$\begin{aligned} p_{k+1} &= \begin{bmatrix} 0.9999 & 8.69e-5 \\ 8.69e-5 & 0.9999 \end{bmatrix} p_k + \begin{bmatrix} 6366 \\ 0.2769 \end{bmatrix} u_k \\ y_k &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} p_k \end{aligned} \quad (۶)$$

اگر لوله اتصال مخزن‌ها شکسته شود، مدل سیستم تغییر می‌کند. با وقوع این عیب، فشار مخزن‌ها از یکدیگر مستقل می‌شوند و ورودی فقط روی مخزن۱ اثر خواهد داشت و فرم فضای حالت سیستم مانند معادله ۷ می‌شود.

$$\begin{bmatrix} p_{1_{k+1}} \\ p_{2_{k+1}} \end{bmatrix} = \begin{bmatrix} 0.9999 & 0 \\ 0 & 0.9999 \end{bmatrix} \begin{bmatrix} p_{1_k} \\ p_{2_k} \end{bmatrix} + \begin{bmatrix} 6366 \\ 0 \end{bmatrix} F_{in} \quad (۷)$$

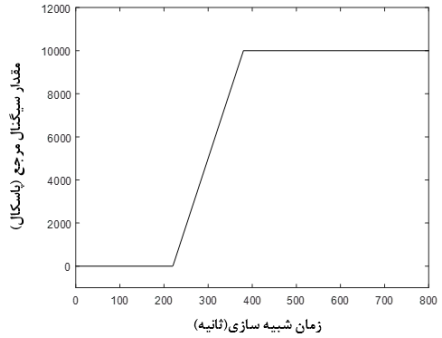
بنابراین فرم فضای حالت این سامانه در حضور ناهنجاری در عملگرها (f_a)، حسگرها (f_s) و عیب در پارامترهای سامانه (f_p) به صورت زیر می‌شود.

$$p_{k+1}=\begin{bmatrix}0.9999 & 8.69e-5\\ 8.69e-5 & 0.9999\end{bmatrix}p_k+\begin{bmatrix}6366\\ 0.2769\end{bmatrix}u_k+\begin{bmatrix}6366\\ 0.2769\end{bmatrix}f_{a_k}+\begin{bmatrix}0 & -8.69e-5\\ -8.69e-5 & 0\end{bmatrix}p_k f_{p_k}+\begin{bmatrix}0\\ -0.2769\end{bmatrix}u_k f_{p_k}$$
$$y_k=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}p+\begin{bmatrix}1\\ 0\end{bmatrix}f_{s1_k}+\begin{bmatrix}0\\ 1\end{bmatrix}f_{s2_k} \quad (۸)$$

در معادله ۸ مقدار f_{p_k} صفر است. اگر عیب در پارامترهای سیستم رخ دهد، مقدارش یک و سیستم مانند معادله ۷ می‌شود. f_{a_k} و f_{s1_k} و f_{s2_k} نیز در شرایط عادی صفر هستند و به ترتیب در زمان بروز ناهنجاری در عملگر و حسگر ۱و۲ مقداری مخالف صفر دارند.

برای این سامانه، یک کنترل کننده PI طراحی شد. هدف کنترلی، کنترل فشار مخزن۲ بود که سیگنال مرجع (شکل ۲) را دنبال کند.

برای این سامانه فیلتری همانند معادله ۲ طراحی شد. اگر ناهنجاری در عملگر رخ دهد، مانده همانند معادله ۳ در فضای خروجی در راستای CB تغییر می‌کند.



شکل ۲- مقدار سیگنال مرجع برای کنترل فشار مخزن۲

$$\sigma_f=0.8\rightarrow G=\begin{bmatrix}0.8 & 0\\ 0 & 0.8\end{bmatrix}$$
$$A=\begin{bmatrix}0.9999 & 8.69e-5\\ 8.69e-5 & 0.9999\end{bmatrix} \quad (۹)$$
$$D=(A-G)C^{-1}\xrightarrow{\square=\square}\square=\begin{bmatrix}0.1999 & 8.69e-5\\ 8.69e-5 & 0.1999\end{bmatrix}$$

$$C=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix},\ CB=\begin{bmatrix}6366\\ 0.2769\end{bmatrix}\approx\begin{bmatrix}1\\ 0\end{bmatrix} \quad (۱۰)$$

در معادله ۲ σ_f مقداری دلخواه و کمتر از یک دارد و در معادله ۹ مقدار آن ۰٫۸ در نظر گرفته شد. وقوع عیب در پارامترهای سامانه (شکسته شدن لوله اتصال مخزن‌ها) مانند معادله ۴ در فضای خروجی ظاهر می‌شود و طبق معادله ۸ مقدارهای ΔA و ΔB مانند معادله ۱۱ به دست می‌آید.

$$\Delta A=\begin{bmatrix}0 & -8.69e-5\\ -8.69e-5 & 0\end{bmatrix}$$
$$\Delta B=\begin{bmatrix}0\\ -0.2769\end{bmatrix} \quad (۱۱)$$

با توجه به اینکه هم ΔB و هم u_k مقدارشان کوچک است، $\Delta B\beta(u_k)$ (در معادله۲) تاثیر زیادی در تغییرات مانده‌ها ندارد. در زمان وقوع عیب به دلیل افزایش خطای کنترل‌کننده، مقدار سیگنال کنترلی بزرگی ایجاد می‌شود و همین باعث افزایش زیاد مقدار p_{1_k} می‌گردد. p_{1_k} هم روی r_{2_k} اثر دارد. بنابراین تغییرات خروجی در زمان وقوع این عیب در راستای $\begin{bmatrix}0\\ 1\end{bmatrix}$است.

برای به دست آوردن رابطه‌ی جهت بین بردار مانده $r_k=\begin{bmatrix}r_{1_k}\\ r_{2_k}\end{bmatrix}$ و بردار امضای ناهنجاری‌ها (f)، مانند معادله ۱۲ از همبستگی بین آن‌ها استفاده می‌کنیم [۲۸].

$$CORR_k=\frac{f^T r_k}{\|f\|_2\|r_k\|_2} \quad (۱۲)$$

هرچه همبستگی به +۱ نزدیک‌تر باشد، یعنی مانده و بردار امضای عیب در یک جهت اند و اگر در خلاف جهت هم باشند این رابطه به -۱ نزدیک‌تر است. به هرحال نزدیک بودن به -۱ یا +۱ به معنی هم راستا بودن بردار مانده با بردار امضای ناهنجاری است. از آنجا که راستا برای ما اهمیت دارد از قدرمطلق آن استفاده می‌کنیم. دو همبستگی را با توجه به امضاها تعریف کردیم؛ یکی در راستای r_{1_k} یا $\begin{bmatrix}1\\ .\end{bmatrix}$ و دیگری در راستای r_{2_k} یا $\begin{bmatrix}.\\ 1\end{bmatrix}$.

$$CORR_{1_k}=\frac{|r_{1_k}|}{\|r_k\|_2}\ ,\ CORR_{2_k}=\frac{|r_{2_k}|}{\|r_k\|_2} \quad (۱۳)$$

برای تشخیص ناهنجاری در حسگرها دو همبستگی جدید را نیز تعریف می‌کنیم. اگر فرض کنیم که ناهنجاری در هر دو حسگر به طور همزمان رخ دهد، معادله‌ی خطای تخمین حالت‌ها مانند معادله ۱۴ می‌شود. با جایگذاری مقادیر، معادله‌ی خروجی مانده مانند معادله ۱۵ می‌شود. در معادله ۱۶ ماتریس Q را به گونه‌ای به دست می‌آوریم تا پس از ضرب کردن آن در r_k اثر f_1 و f_2 در راستای $\begin{bmatrix}1\\ 0.1\end{bmatrix}$ و $\begin{bmatrix}0.1\\ 1\end{bmatrix}$ ایجاد شود. Q طبق معادله ۱۶ به دست آمد.

$$\xrightarrow{(۵)} e_{1_{k+1}}=\sigma_f e_{1_k}-d_{11}f_1-d_{12}f_2\rightarrow e_{1_k}\approx\frac{-d_{11}f_1-d_{12}f_2}{1-\sigma_f}$$
$$\xrightarrow{(۵)} e_{2_{k+1}}=\sigma_f e_{2_k}-d_{21}f_1-d_{22}f_2\rightarrow e_{2_k}\approx\frac{-d_{21}f_1-d_{22}f_2}{1-\sigma_f} \quad (۱۴)$$
$$\xrightarrow{(۵)} r_{1k}=\frac{-d_{11}f_1-d_{12}f_2}{1-\sigma_f}+f_1=\frac{(1-\sigma_f-d_{11})f_1-d_{12}f_2}{1-\sigma_f}$$

$$\xrightarrow{(۵)} r_{2k}=\frac{-d_{21}f_1-d_{22}f_2}{1-\sigma_f}+f_2=\frac{(1-\sigma_f-d_{11})f_2-d_{21}f_1}{1-\sigma_f}$$

$$r_k=\begin{bmatrix}r_{1k}\\ r_{2k}\end{bmatrix}=\begin{bmatrix}0.0005 & -0.0004\\ -0.0004 & 0.0005\end{bmatrix}\begin{bmatrix}f_1\\ f_2\end{bmatrix} \quad (۱۵)$$

$$\begin{bmatrix}0.0005 & -0.0004\\ -0.0004 & 0.0005\end{bmatrix}\begin{bmatrix}q_1\\ q_2\end{bmatrix}=\begin{bmatrix}1\\ 0.1\end{bmatrix}$$
$$\begin{bmatrix}0.0005 & -0.0004\\ -0.0004 & 0.0005\end{bmatrix}\begin{bmatrix}q_3\\ q_4\end{bmatrix}=\begin{bmatrix}0.1\\ 1\end{bmatrix} \quad (۱۶)$$

$$Q=\begin{bmatrix}q_1 & q_2\\ q_3 & q_4\end{bmatrix}\rightarrow \boldsymbol{Q}=\begin{bmatrix}\mathbf{4.4682} & \mathbf{3.9869}\\ \mathbf{3.9869} & \mathbf{4.4682}\end{bmatrix}$$

ماتریس Q را در r_k ضرب می‌کنیم و مانند معادله ۱۷ دو همبستگی بر اساس $m_k=Qr_k$ به دست می‌آید.

$$CORR_4(k)=\frac{|m_2(k)|}{\|m(k)\|_2}\ ,\ CORR_3(k)=\frac{|m_1(k)|}{\|m(k)\|_2} \quad (۱۷)$$

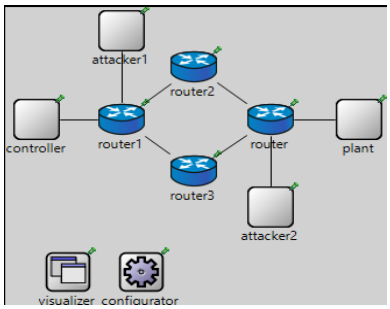
۶-۳- افزودن پارامترهای شبکه به داده‌های فیلتر BFDF

همبستگی‌های تعریف شده در بخش قبل، بروز ناهنجاری در بخش‌های مختلف سامانه را مشخص می‌کند. این ناهنجاری‌ها می‌تواند ناشی از عیب و یا حمله سایبری باشد. حال در اینجا اطلاعات شبکه را نیز در کنار مقدار همبستگی‌ها و مانده بررسی می‌کنیم.

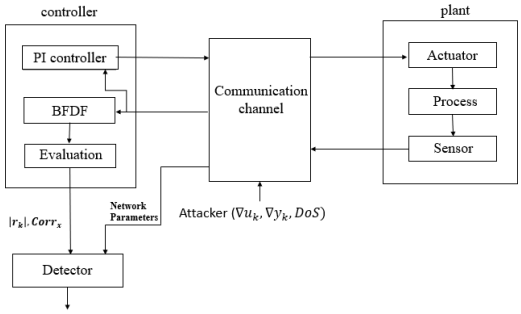
پارامتر شبکه‌ای که در این مقاله بیشتر به آن توجه شد، ترافیک شبکه است. با توجه به بسته بودن سامانه و نداشتن ترافیک ورودی و مشخص بودن تعداد اتصالات بین گره‌ها و میزان ترافیک عادی هر گره، بیشتر شدن ترافیک شبکه از حدی معین نسبت به مقدار معلوم هر گره می‌تواند نشان دهنده‌ی نفوذ به

شبکه و حمله سایبری باشد. سامانه معرفی شده در بخش قبل در نرم افزار Omnet++ و با استفاده از کتابخانه INET شبیه سازی شد.

فرم فضای حالت سامانه با زبان c++ نوشته شد و مانند شکل ۳ در قسمت plant قرار داده شد. کد کنترل کننده و فیلتر تشخیص عیب نیز در بلوک controller قرار داده شد. بخشی از کدها در پیوست قرار داده شده است. توپولوژی ارتباط بین plant و controller نیز مانند شکل ۳ انتخاب شد. در یک مسیر مقدار حسگرها برای controller و در مسیر دیگر مقدار سیگنال کنترلی برای plant ارسال می‌شود. بلوک دیاگرام سیستم برای مشخص‌تر شدن بخش‌های داخل گره‌های plant و controller در شکل ۴ نمایش داده شده است.

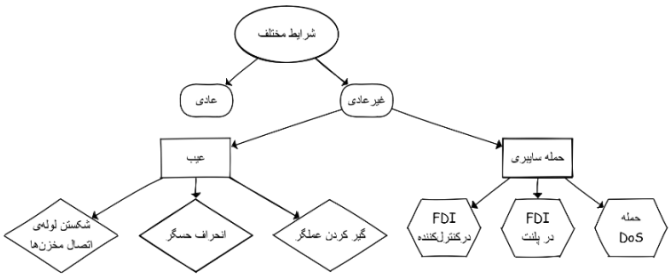


شکل ۳- ساختار شبکه‌ی طراحی شده در Omnet++



شکل ۴- بلوک دیاگرام و ساختار سیستم

در سناریوهای حمله فرض می‌شود که مهاجم از قبل به نقاط تحریک قابل کنترل لازم برای ارسال بسته‌ها از طریق شبکه دسترسی دارد. در زمان حمله، گره‌های attacker مانند شکل ۳ شروع به سیل بسته‌ها در شبکه‌ی ارتباطی کرده و نقاط دسترسی، سوئیچ ها و روتر را با بسته‌ها پر می‌کنند. در زمان حمله تزریق داده غلط نیز مقدار داده‌های ارسالی، در مسیر رسیدن به مقصد تغییر می‌کند. وضعیت‌های گوناگون ناهنجاری و وضعیت عادی همانند شکل ۵ برای سامانه در شبیه سازی اعمال شد.



شکل ۵- نمودار وضعیت‌های مختلف سیستم

۷- نتایج شبیه سازی

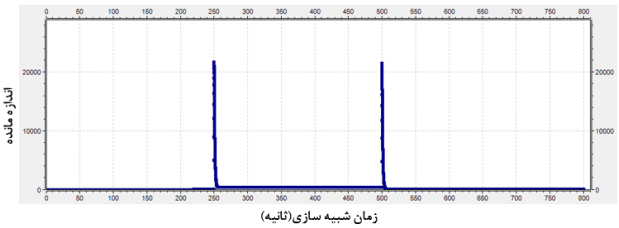
برای مشاهده‌ی کدهای کامل شبیه سازی در Omnet++ می‌توانید به آدرس مراجعه نمایید.

کنترل‌کننده بر اساس مقدار سیگنال مرجع و مقدار حسگر ۲، یک سیگنال کنترلی تولید و برای سامانه ارسال می‌کند. سامانه نیز مقدار حسگرها را هر از ۰,۰۱ ثانیه برای کنترل‌کننده با پروتکل UDP می‌فرستد. طول هر بسته‌ی ارسالی بین گره‌ها ۲۰ بایت است. بنابراین با توجه به بسته بودن سامانه و مشخص بودن تعداد اتصالات بین گره‌ها، میزان ترافیک حدودی دریافتی هر گره معلوم است. در اینجا ترافیک دریافتی هر گره در حالت عادی حدود ۱۶۰۰۰ بیت بر ثانیه می‌شود، زیرا هر گره هر از ۰,۰۱ ثانیه ۲۰ بایت داده دریافت می‌کند.

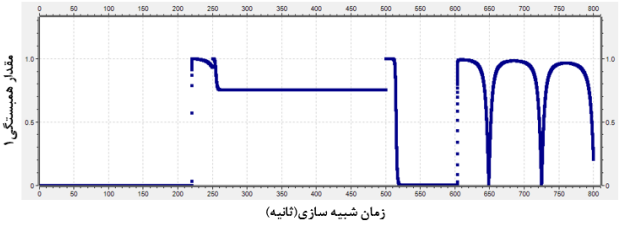
چهار همبستگی به دست آمده در بخش قبل را معیاری برای تفکیک ناهنجاری‌ها در نظر می‌گیریم. بیشینه این چهار همبستگی، نوع ناهنجاری را به ما می‌دهد. زمان کل شبیه سازی ۸۰۰ ثانیه است. در بازه زمانی ۲۵۰ تا ۵۰۰ ناهنجاری‌های مطرح شده در شکل ۵ در چند شبیه سازی جداگانه ایجاد شد. نتایج این شبیه سازی‌ها در جدول ۱ آورده شده است.

به عنوان نمونه، هنگام وقوع حمله سایبری در کانال ارتباطی حسگر۱ اندازه مانده و همبستگی‌ها و پارامترهای شبکه همانند شکل‌های۶ تا ۱۲ شد. در شکل‌ها همبستگی ۳ از بقیه‌ی همبستگی‌ها بیشتر بوده و مقدارش یک شده است. بنابراین ناهنجاری در حسگر۱ تشخیص داده شده است و با توجه به ترافیک شبکه و بیشتر بودن آن از مقدار قابل انتظار، وقوع حمله سایبری در کانال حسگر۱ تشخیص داده می‌شود.

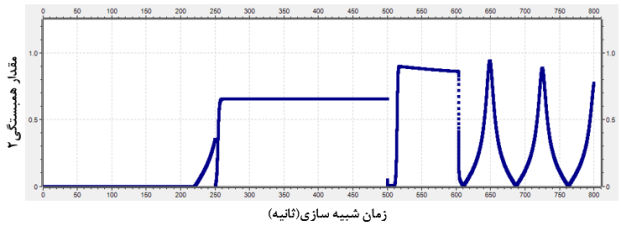
واضح است که مقدار همبستگی در زمان‌های دیگر اهمیتی ندارد؛ زیرا در آن زمان‌ها مانده مقداری نزدیک به صفر داشته و ناهنجاری تشخیص داده نشده است. اندازه مانده در زمان وقوع ناهنجاری حدود ۳۳۰ شد و در زمان‌های دیگر نزدیک صفر است.



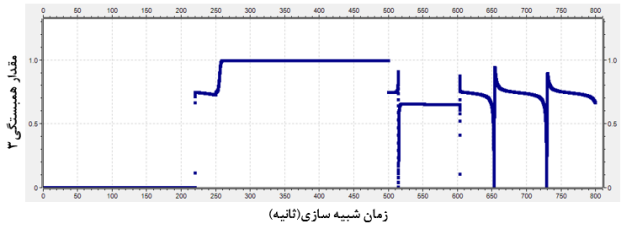
شکل ۶- اندازه مانده در زمان حمله به حسگر۱ در مدت زمان شبیه سازی(ثانیه)



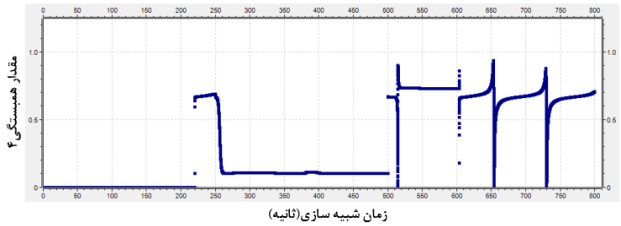
شکل ۷- مقدار همبستگی۱: امضای ناهنجاری در عملگر نسبت به زمان شبیه سازی(ثانیه)



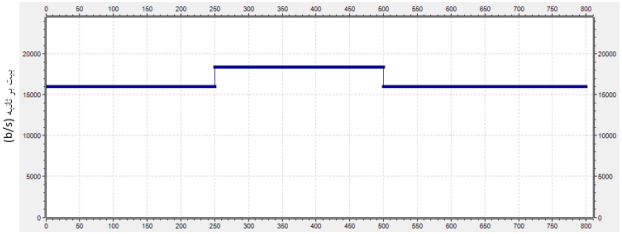
شکل ۸- مقدار همبستگی۲: امضای عیب در پارامترهای سامانه نسبت به زمان شبیه سازی(ثانیه)



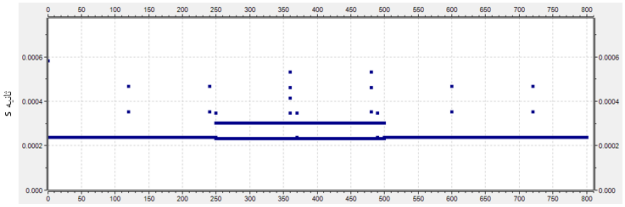
شکل ۹- مقدار همبستگی۳: امضای ناهنجاری در حسگر۱ نسبت به زمان شبیه سازی(ثانیه)



شکل ۱۰- مقدار همبستگی۴: امضای ناهنجاری در حسگر۲ نسبت به زمان شبیه سازی(ثانیه)



شکل ۱۱- ترافیک شبکه(بیت بر ثانیه) نسبت به زمان شبیه سازی(ثانیه)



شکل ۱۲- تاخیر انتها به انتها نسبت به زمان شبیه سازی(ثانیه)

در جدول ۱ f_u، f_{s_1} و f_{s_2} به ترتیب ناهنجاری(حمله یا عیب) در عملگر، حسگر۱ و حسگر۲ است و f_u عیب در سامانه می‌باشد. مقدار همبستگی‌ها در زمان وقوع این ناهنجاری‌ها در جلوی آن‌ها نوشته شده است.

اگر انحراف در حسگرها و یا عملگر رخ دهد، می‌تواند ناشی از عیب در آن‌ها و یا وقوع حمله سایبری در کانال آن‌ها باشد. در هر دو، همبستگی‌ها مکان وقوع ناهنجاری و پارامترهای شبکه، نوع ناهنجاری را مشخص می‌کند.

جدول ۱- مقدار همبستگی‌ها در زمان وقوع هر ناهنجاری

	$Corr_1$	$Corr_2$	$Corr_3$	$Corr_4$
f_u	۱	۰.۰۲	۰.۷۴	۰.۶۶
f_p	۰	۱	۰.۶۶	۰.۷۴
f_{s1}	۰.۷۵	۰.۶۵	۱	۰.۱
f_{s2}	۰.۶۵	۰.۷۵	۰.۱	۱

اگر حمله داس در کانال ارتباطی عملگر رخ دهد، مقدار سیگنال کنترلی ثابت می‌ماند و همانند عیب در عملگر ظاهر می‌شود. اگر در کانال ارتباطی حسگرها رخ دهد، مقدار آن‌ها ثابت می‌ماند و با تغییرات سیگنال کنترلی نیز تغییر نمی‌کند. ترافیک شبکه در زمان وقوع حمله داس به حدی می‌شود که داده‌ی جدید به مقصد نمی‌رسد و یا با فاصله‌ی زمانی زیادی می‌رسد.

یک راه برای تشخیص حمله داس بررسی ترافیک شبکه است. اگر مقدار شبکه مثلا دو برابر مقدار عادی آن شد، حمله داس تشخیص داده می‌شود.

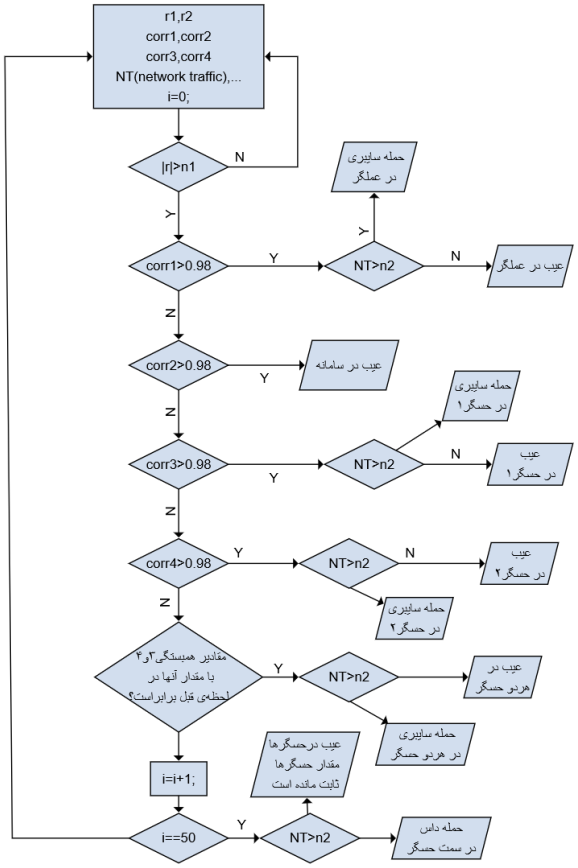
یک راه دیگر نیز برای تشخیص حمله داس در کانال حسگرها در نظر گرفته شد. یک متغیر با مقدار صفر را تعریف می‌کنیم. در هر نمونه، مقدار فعلی و قبلی سیگنال کنترلی و همینطور حسگرها را با هم مقایسه کنیم. اگر مقدار سیگنال کنترلی تغییر کند ولی مقدار حسگرها ثابت بماند، مقدار متغیر را یکی اضافه می‌کنیم. اگر مثلا پس از ۵۰ نمونه پشت سرهم این اتفاق افتاد و آن متغیر مقدارش به ۵۰ رسید، حمله داس تشخیص داده می‌شود. چون زمان ارسال و دریافت بسته ۰،۰۱ ثانیه در نظر گرفته شده است، ۵۰ نمونه حدود ۰،۵ ثانیه طول می‌کشد که زمان تشخیص مناسبی است.

اگر همزمان در هر دو حسگر انحراف ایجاد شود، اثر آن در اندازه مانده نمایان می‌شود اما هیچکدام از همبستگی‌ها ۱ نمی‌شود. برای فهمیدن اینکه چه مقدار انحراف در هر حسگر وجود دارد، می‌توان نسبت همبستگی‌های ۳ و۴ را به دست آورد. به این صورت می‌توان فهمید که انحراف در کدام حسگر بیشتر بوده و چند برابر دیگری است.

بنابراین طبق نتایجی که به دست آمد، الگوریتمی همانند شکل ۱۳ برای تشخیص و جداسازی عیب و حمله سایبری قابل ارائه است. عدد ۵۰ در فلوچارت، مربوط به تشخیص حمله داس است که توضیح داده شد. از آنجایی که در صورت وقوع ناهنجاری، همبستگی مربوط به آن مقداری نزدیک به ۱ خواهد داشت، برای تشخیص داده شدن هر ناهنجاری مقدار بزرگتر از ۰،۹۸ در فلوچارت در نظر گرفته شد.

۸- نتیجه‌گیری

هدف اصلی این مقاله بررسی برخی از حملات سایبری معروف بود و ارزیابی اینکه چگونه می‌توان آن‌ها را از عیب‌های رایج قابل وقوع در سیستم متمایز کرد. در این مقاله برای درک بهتر وضعیت یک سیستم کنترل شبکه‌ای علاوه بر داده‌های فیزیکی، از پارامترهای شبکه نیز استفاده شد. بدین منظور یک سامانه کنترل شبکه‌ای مدل شد که کنترل کننده و سامانه با پروتکل‌های اینترنت با هم در ارتباط بودند. برای تشخیص ناهنجاری‌های سامانه اعم از عیب یا حمله سایبری، برای سامانه یک روش بر مبتنی بر مدل که فیلتر BFDFاست، طراحی شد.



شکل ۱۳- الگوریتم برای تشخیص عیب و حمله‌ی سایبری با فرض داشتن پارامترهای شبکه با استفاده از فیلتر تشخیص عیب برد

هر ناهنجاری در فضای مانده تولید شده توسط فیلتر جهت منحصر به فرد خود را دارد و از یکدیگر قابل تفکیک است. در ادامه برای تشخیص اینکه این ناهنجاری ناشی از عیب و یا حمله سایبری است، استفاده از پارامترهای شبکه پیشنهاد شد. سیستم در نرم افزار Omnet++ شبیه سازی شد و عیب‌ها و حمله‌های سایبری مختلف روی آن اعمال شد. در پایان بر اساس نتایج به دست آمده یک الگوریتم برای تشخیص عیب و حمله سایبری برای سامانه نوشته شد.

پیشنهادات

برای کارهای آینده می‌توان به طراحی نوع جدیدی از سیستم تشخیص نفوذ اشاره کرد که بیشتر مختص سیستم‌های SCADA است. همچنین برای تفکیک عیب از حمله سایبری می‌توان از سایر روش‌های مبتنی بر مدل و شبیه سازی عیب‌ها و حملات سایبری پیچیده‌تر و کمک گرفتن از پارامترهای شبکه برای تشخیص بهتر آن‌ها بهره برد. همچنین می‌توان از روش‌های کلاس‌بندی یادگیری ماشین استفاده نمود که داده‌های پارامتر شبکه نیز به دیتاست اضافه شده باشد.

پیوست‌ها

کد c++ سامانه به صورت زیر است.

```
void Plant::RealPlant(double u)
 {
   p1 = A[0][0] * p1 + A[0][1] * p2 + B[0] * u;
   p2 = A[1][0] * p1 + A[1][1] * p2 + B[1] * u;
 }
```

کد مربوط به کنترل کننده PI نیز به صورت زیر است.

```
void Controller::PI_Controller(double y)
 {
   referenceValue = ReferenceSignal();
   controlError = referenceValue - y;
   Integral = Integral + Ts * controlError;
   controlSignal = Kp * controlError + Ki * Integral;

   if (controlSignal < 0) controlSignal = 0;

   emit(referenceValueSignal, referenceValue);
   emit(errorValueSignal, controlError);
 }
```

کد c++ قسمت فیلتر تشخیص عیب برد و همینطور محاسبه‌ی همبستگی‌ها نیز به صورت زیر نوشته شد.

```
const double G[2][2] = {{0.8, 0},
          {0, 0.8}};
const double D[2][2] = {{0.1999, 8.69e - 5},
          {8.69e - 5, 0.1999}};
const double Q[2][2] = {{4.4682, 3.9869},
          {3.9869, 4.4682}};

void Controller::Plant_Model()
 {

   R1 = (p1 - z1);
   R2 = (p2 - z2);

   m1 = (Q[0][0] * R1 + Q[0][1] * R2);
   m2 = (Q[1][1] * R2 + Q[1][0] * R1);

   z1 = G[0][0] * z1 + G[0][1] * z2 + D[0][0] * p1 + D[0][1]
                * p2 + Bb[0] * u[0];
   z2 = G[1][0] * z1 + G[1][1] * z2 + D[1][0] * p1 + D[1][1]
                * p2 + Bb[1] * u[0];

 }

void Controller::Evaluation()
 {
   norm_R = sqrt(R1 * R1 + R2 * R2);
   norm_m = sqrt(m1 * m1 + m2 * m2);

   corr1 = abs(R1)/(norm_R + 0.001);
   corr2 = abs(R2)/(norm_R + 0.001);
   corr3 = abs(m1)/(norm_m + 0.001);
   corr4 = abs(m2)/(norm_m + 0.001);
 }
```

مراجع

[۱] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, and N. Meskin, "Cybersecurity for industrial control systems: A survey," computers & security, vol. 89, p. 101677, 2020.

[۲] Y. Cherdantseva et al., "A review of cyber security risk assessment methods for SCADA systems," Computers & security, vol. 56, pp. 1-27, 2016.

[۳] S. Feng and P. Tesi, "Resilient control under denial-of-service: Robust design," Automatica, vol. 79, pp. 42-51, 2017.

[۴] A.-Y. Lu and G.-H. Yang, "Input-to-state stabilizing control for cyber-physical systems with multiple transmission channels under denial of service," IEEE Transactions on Automatic Control, vol. 63, no. 6, pp. 1813-1820, 2017.

[۵] T.-Y. Zhang and D. Ye, "Distributed secure control against denial-of-service attacks in cyber-physical systems based on K-connected communication topology," IEEE transactions on cybernetics, vol. 50, no. 7, pp. 3094-3103, 2020.

[۶] D. Ye, T.-Y. Zhang, and G. Guo, "Stochastic coding detection scheme in cyber-physical systems against replay attack," Information Sciences, vol. 481, pp. 432-444, 2019.

[۷] Y. Li, D. Shi, and T. Chen, "False data injection attacks on networked control systems: A Stackelberg game analysis," IEEE Transactions on Automatic Control, vol. 63, no. 10, pp. 3503-35.۲۰۱۸ ,۰۹

[۸] C.-Z. Bai, F. Pasqualetti, and V. Gupta, "Data-injection attacks in stochastic control systems: Detectability and performance tradeoffs," Automatica, vol. 82, pp. 251-260, 2017.

[۹] G. Park, C. Lee, H. Shim, Y. Eun, and K. H. Johansson, "Stealthy adversaries against uncertain cyber-physical systems: Threat of robust zero-dynamics attack," IEEE Transactions on Automatic Control, vol. 64, no. 12, pp. 4907-4919, 2019.

[۱۰] C.-Z. Bai, V. Gupta, and F. Pasqualetti, "On Kalman filtering with compromised sensors: Attack stealthiness and performance bounds," IEEE Transactions on Automatic Control, vol. 62, no. 12, pp. 6641-6648, 2017.

[۱۱] Z. Guo, D. Shi, K. H. Johansson, and L. Shi, "Worst-case stealthy innovation-based linear attack on remote state estimation," Automatica, vol. 89, pp. 117-124, 2018.

[۱۲] L. Hu, Z. Wang, Q.-L. Han, and X. Liu, "State estimation under false data injection attacks: Security analysis and system protection," Automatica, vol. 87, pp. 176-183, 2018.

[۱۳] T.-Y. Zhang and D. Ye, "False data injection attacks with complete stealthiness in cyber–physical systems: A self-generated approach," Automatica, vol. 120, p. 109117, 2020.

[۱۴] J. Rønneberg, "Reference Topologies and Scenarios for Cyber-Physical Systems in the Norwegian Cyber Range," NTNU, 2019 .

[۱۵] A. W. Werth, "Towards distinguishing between cyber-attacks and faults in cyber-physical systems," 2014 .

[۱۶] مرضیه نجار، سید محمدحسین معطر، «تشخیص نفوذ شبکه با استفاده از رویکرد ترکیبی مدل مخفی مارکوف و یادگیری ماشین مفرط»، مجله مهندسی برق دانشگاه تبریز، جلد ۴۸،شماره ۴، صفحات ۱۸۰۷-۱۸۱۷، ۱۳۹۷.

[۱۷] D. Du, "Fault detection for discrete-time linear systems based on descriptor observer approach," Applied Mathematics and Computation, vol. 293, pp. 575-585, 2017.

[۱۸] Z. Gao, "Fault estimation and fault-tolerant control for discrete-time dynamic systems," IEEE Transactions on Industrial Electronics, vol. 62, no. 6, pp. 3874-3884, 2015.

[۱۹] F. Miao, Q. Zhu, M. Pajic, and G. J. Pappas, "Coding schemes for securing cyber-physical systems against stealthy data injection attacks," IEEE Transactions on Control of Network Systems, vol. 4, no. 1, pp. 106-117, 2016.

[۲۰] A. Barboni, H. Rezaee, F. Boem, and T. Parisini, "Distributed detection of covert attacks for interconnected systems," in 2019 18th European Control Conference (ECC), 2019: IEEE, pp. 2240-2245 .

[۲۱] M. Taheri, K. Khorasani, I. Shames, and N. Meskin, "Cyber Attack and Machine Induced Fault Detection and Isolation Methodologies for Cyber-Physical Systems," arXiv preprint arXiv:2009.06196, 2020.

[۲۲] بهنام همایی، سعید اباذری، مجتبی برخورداری یزدی، «تشخیص حمله‌ی سایبری تزریق داده‌ی غلط در شبکه‌ی برق مبتنی‌بر PMU با استفاده از فیلتر کالمن»، مجله مهندسی برق دانشگاه تبریز، جلد ۴۹، شماره ۴، صفحات ۱۸۹۵-۱۹۰۳، ۱۳۹۸.

[۲۳] A. Varga and R. Hornig, "An overview of the OMNeT++ simulation environment," in Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops, 2008, pp. 1-10 .

[۲۴] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, "A survey on SCADA systems :secure protocols, incidents, threats and tactics," IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1942-1976, 2020.

[۲۵] H. H. Alhelou, M. H. Golshan, and J. Askari-Marnani, "Robust sensor fault detection and isolation scheme for interconnected smart power systems in presence of RER and EVs using unknown input observer," International Journal of Electrical Power & Energy Systems, vol. 99, pp. 682-694, 2018.

[۲۶] J. Chen, R. J. Patton, and H.-Y. Zhang, "Design of unknown input observers and robust fault detection filters," International Journal of control, vol. 63, no. 1, pp. 85-105, 1996.

[۲۷] C. Shang, S. X. Ding, and H. Ye, "Distributionally robust fault detection design and assessment for dynamical systems," Automatica, vol. 125, p. 10943.۲۰۲۱ ,۴

[۲۸] J. J. Gertler, Fault detection and diagnosis in engineering systems. CRC press, 2017.