Gazi Üniversitesi
Fen Bilimleri Dergisi
PART C: TASARIM VE TEKNOLOJİ

Gazi University
Journal of Science
PART C: DESIGN AND TECHNOLOGY

GU J Sci, Part C, 14(X): XX-XX (2026)

Exploiting Delay for Stealth: A Delay-Aware False Data Injection Framework for Wireless Sensor Networks

Uras PANAHI[1*]

[1]*Department of Computer Engineering, Artvin Çoruh University, Artvin, Türkiye*

Article Info

Research article
Received: 20/04/2026
Revision: 20/08/2026
Accepted: 23/08/2026

Keywords

False Data Injection
WSN Security
LSTM Anomaly Detection
Delay-Normalized Residual
Stealth-Impact Tradeoff
Simulation

Makale Bilgisi

Araştırma makalesi
Başvuru: 20/04/2026
Düzeltme: 20/08/2026
Kabul: 23/08/2026

Anahtar Kelimeler

Yanlış Veri Enjeksiyonu
Kablosuz Algılayıcı Ağlar Güvenliği
LSTM Anomali Tespiti
Gecikmeye Göre Normalize Edilmiş Artık
Gizlilik-Etki Dengesi
Simülasyon

Graphical/Tabular Abstract (Grafik Özet)

A delay-coupled false data injection (DA-FDI) attack exploits stochastic network delay to evade CUSUM, 3-sigma, LSTM and autoencoder detectors; the proposed Delay-Normalized Residual Detector (DNRD) restores detection to 89.4% at a 3.8% false-alarm rate in NS-3 simulations of a 30-node wireless sensor network. / Gecikmeye bağlı bir yanlış veri enjeksiyonu (DA-FDI) saldırısı, CUSUM, 3-sigma, LSTM ve otoenkoder tabanlı dedektörleri atlatmak için rastgele ağ gecikmesinden yararlanır; önerilen Gecikme Normalleştirilmiş Artık Dedektörü (DNRD), 30 düğümlü bir kablosuz algılayıcı ağının NS-3 simülasyonlarında %3,8 yanlış alarm oranında tespiti %89,4'e çıkarmaktadır.

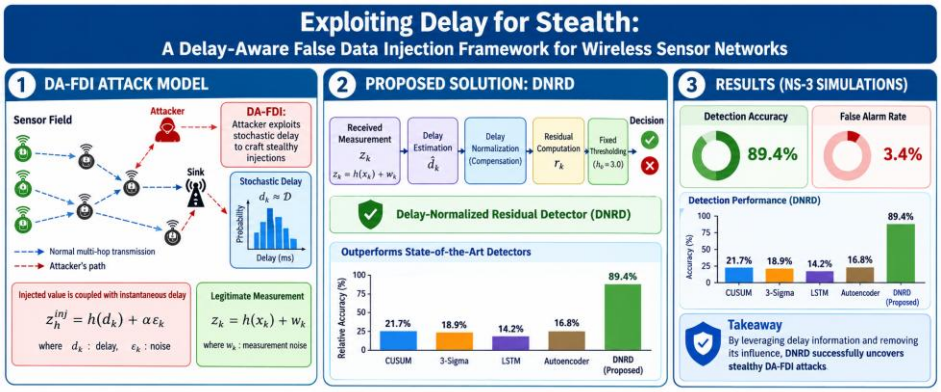

Figure A: *Graphical abstract /* ***Şekil A:*** *Grafik özet*

Highlights (Önemli noktalar)

- *A stealthiness analysis framework (Stealth Rate, Attack Impact Score, Stealth-Impact Tradeoff) explains via four propositions why CUSUM, 3-sigma, LSTM and autoencoder detectors fail. / Gizlilik Oranı, Saldırı Etki Puanı ve Gizlilik-Etki Değişimine dayanan çerçeve, CUSUM, 3-sigma, LSTM ve otoenkoder dedektörlerinin neden başarısız olduğunu dört önermeyle açıklamaktadır.*
- *Ablation experiments show that only the coupling of delay and injection, not either factor alone, produces the stealth effect. / Ablasyon deneyleri, gizlilik etkisinin yalnızca gecikme ve enjeksiyonun birleşiminden kaynaklandığını göstermektedir.*
- *A Delay-Normalized Residual Detector is proposed, reaching 89.4% detection at a 3.8% false-alarm rate. / Gecikme Normalleştirilmiş Artık Dedektörü, %3,8 yanlış alarm oranında %89,4 tespit sağlamış.*

Aim (Amaç): *This study analyzes a new class of FDI attacks that exploit stochastic network delay to evade existing WSN anomaly detectors. / Bu çalışma, KAA'larda mevcut anomali dedektörlerini atlatmak için ağ gecikmesinden yararlanan yeni bir YVE saldırı sınıfını incelemektedir.*

Originality (Özgünlük): *The DA-FDI model, its stealthiness analysis framework, and DNRD together give, to the author's knowledge, the first treatment of delay as an active resource for both attacking and defending WSN anomaly detection. / DA-FDI modeli, gizlilik analizi çerçevesi ve DNRD, gecikmeyi hem saldırı hem savunma kaynağı olarak ele alan ilk çalışmayı oluşturmaktadır.*

Results (Bulgular): *Simulations show DA-FDI cuts classical detection from above 84% to 14-22%, while DNRD restores 89.4% detection at 3.8% false alarms, 77x faster than LSTM. / Simülasyonları, DA-FDI'nın tespiti %84'ten %14-22'ye düşürdüğünü; DNRD'nin ise %3,8 yanlış alarmda %89,4 tespit sağlayarak LSTM'den 77 kat hızlı olduğunu göstermektedir.*

Conclusion (Sonuç): *Delay-agnostic detection leaves WSNs vulnerable to delay-coupled FDI; DNRD's delay-normalized residuals close this gap with an exponential detection guarantee. / Gecikmeden bağımsız tespit, KAA'ları savunmasız bırakır; DNRD'nin gecikme normalleştirmesi bu kör noktayı üstel bir garantiyle kapatmaktadır.*

*Corresponding author, e-mail: uraspanahi@artvin.edu.tr
DOI: 10.29109/gujsc.1934738

GU J Sci, Part C, 14(X): XX-XX (2026)

Gazi Üniversitesi
Fen Bilimleri Dergisi
PART C: TASARIM VE TEKNOLOJİ

Gazi University
Journal of Science
PART C: DESIGN AND TECHNOLOGY

http://dergipark.gov.tr/gujsc

Exploiting Delay for Stealth: A Delay-Aware False Data Injection Framework for Wireless Sensor Networks

Uras PANAHI [1*]

[1]*Department of Computer Engineering, Artvin Çoruh University, Artvin, Türkiye*

Article Info

Research article
Received: 20/04/2026
Revision: 20/08/2026
Accepted: 23/08/2026

Keywords

False Data Injection
WSN Security
LSTM Anomaly Detection
Delay-Normalized Residual
Stealth-Impact Tradeoff
Simulation

Abstract

False data injection attacks can undermine WSN security, while the existing models assume static attackers working in isolation from network processes. This paper presents a new type of FDI attack referred to as the Delay-Aware FDI (DA-FDI). Specifically, the attacker utilizes the stochastic delays to craft injections that mimic real measurements. Next, a framework for the stealthiness analysis that uses the metrics of Stealth Rate (SR) and Attack Impact Score (AIS) to quantify the Stealth-Impact Tradeoff (SIT) relationship is presented. Thereafter, four propositions that provide reasons for ineffectiveness of CUSUM, 3-sigma rule, LSTM networks, and autoencoders are provided. It is shown that the reason for detection failures is the interaction between the delay and the injection, and not only delay uncertainty alone. A new detector called Delay-Normalized Residual Detector (DNRD) is proposed. Detection results in NS-3 simulations achieve accuracy of 89.4% with a false alarm rate of 3.8%

Gizlilik için Gecikmeden Yararlanma: Kablosuz Algılayıcı Ağları için Gecikmeye Duyarlı Bir Yanlış Veri Enjeksiyonu Çerçevesi

Makale Bilgisi

Araştırma makalesi
Başvuru: 20/04/2026
Düzeltme: 20/08/2026
Kabul: 23/08/2026

Anahtar Kelimeler

Yanlış Veri Enjeksiyonu
Kablosuz Algılayıcı Ağlar Güvenliği
LSTM Anomali Tespiti
Gecikmeye Göre Normalize Edilmiş Artık
Gizlilik-Etki Dengesi
Simülasyon

Öz

Yanlış Veri Enjeksiyonu saldırıları, Kablosuz Sensör Ağlarının bütünlüğüne ciddi bir tehdit oluşturmaktadır; ancak mevcut modellerin çoğu, ağ dinamiklerinden bağımsız olarak çalışan statik düşmanları varsaymaktadır. Bu makalede, akıllı bir düşmanın, meşru verileri yakından taklit eden enjeksiyonlar üretmek için rastgele iletim gecikmelerinden yararlandığı bir Gecikme Farkındalıklı FDI (DA-FDI) saldırısı sunuyoruz. Bu çalışmada, Gizlilik Başarı Oranı ve Saldırı Etki Puanı temelinde, Gizlilik-Etki Değişimini yakalayan bir Gizlilik Analizi Çerçevesi geliştiriyoruz. Dört önerme, CUSUM, 3-sigma, LSTM ve otoenkoder tabanlı dedektörlerin DA-FDI'ye saldırılarına karşı neden zorlandığını açıklamaktadır. Analizimiz, tespit başarısızlığının öncelikle gecikme değişkenliğinden ziyade gecikme ve enjeksiyon arasındaki bağlantıdan kaynaklandığını göstermektedir. Bu sınırlamayı ele almak için, Gecikme Normalleştirilmiş Artık Dedektörü (DNRD) öneriyoruz. NS-3 simülasyonları, Azuma-Hoeffding eşitsizliklerine dayalı teorik garantilerle desteklenen, %3,8 yanlış pozitif oranında %89,4'lük tespit doğruluğu göstermektedir.

1. INTRODUCTION (GİRİŞ)

The Wireless Sensor Network (WSN) represents the sensing component of modern cyber-physical systems. An attacker that modifies sensor measurements without sounding any alarm signals can stealthily maneuver the underlying physical process towards a disastrous situation. False Data Injection (FDI) attacks [1] have been studied extensively, but traditional FDI relies on synchronous and delay-free transmission, which is unrealistic for WSNs, where the information takes stochastic hops across nodes. The framework has been generalized and validated in several cyber-physical systems such as the power grid [2], vehicular networks [3], and UAVs [4] through practical examples of covert manipulations that can maintain their persistence under operational constraints.

*Corresponding author, e-mail: uraspanahi@artvin.edu.tr
DOI: 10.29109/gujsc.1934738

Main Hypothesis: The stochastic delay in network transmission should be considered not only as an annoyance but also as a resource that the intelligent attacker can utilize to increase attack stealthiness. More importantly, the potential of attack exploitation can be mitigated if the nature of the stochastic delay is taken into account.

We introduce the DA-FDI attack and summarize the four main contributions as follows. First (C1), we formulate the DA-FDI attack model, in which the injected signal is deliberately coupled to the instantaneous delay statistics rather than added independently of them. Second (C2), we develop a stealthiness analysis framework built on the Stealth Rate (SR), the Attack Impact Score (AIS), and the resulting Stealth-Impact Tradeoff (SIT) curves, together with four propositions that explain why CUSUM-based, 3-sigma-rule-based, long short-term memory (LSTM) network-based, and autoencoder-based detectors are structurally unable to separate delay-coupled injections from legitimate variability. Third (C3), we perform an ablation study that isolates the individual contributions of delay variability and injection amplitude, showing that neither factor alone is sufficient to degrade detection performance and that it is specifically their coupling that produces the stealth effect. Fourth (C4), we propose the Delay-Normalized Residual Detector (DNRD), a lightweight defense that normalizes the residual by the estimated delay standard deviation and is accompanied by an exponential detection guarantee.

The paper is organized as follows: Section II reviews related work, Section III presents system and attack models, Section IV provides stealthiness analysis, Section V describes DNRD, Section VI outlines the NS-3 simulation framework, Section VII reports evaluation results, Section VIII discusses limitations, and Section IX concludes.

2. RELATED WORK (İLGİLİ ÇALIŞMALAR)

FDI in Power Systems and WSNs: An algebraic approach to FDI was developed by Liu et al. [1]. FDI problems under Gaussian noise were addressed in [10], where the notion of stealthiness was discussed. The graph theoretic treatment was used by Pasqualetti et al. [11] to study detectability. It should be mentioned that none of these contributions uses the concept of time-varying delay as an active ingredient in disguise. Extensions for AC/DC power flow [2][5][9], distributed estimation [6], and secure channels [7] largely assume absence of delay in communication, which does not sufficiently capture the practical scenario of WSNs. Han et al. [8] dealt with energy limitations; but these references ignore stochastic delay variations and malicious learning of the delay statistics, which are considered in the current study. Recent works (2023–2026) have extended FDI analysis to edge computing and IoT contexts [20][21][22][23], where delay variability is even more pronounced due to heterogeneous hardware and multi-hop routing.

Delay-based Attacks: In replay and time synchronization attacks [12,13], delay is treated as a disruption factor. We are not aware of any use of delay in data injection attacks for the purposes of achieving stealthiness. Kalman filtering under conditions of packet dropout was considered in [14][15]; to the best of our knowledge, although the impact of delay on stealthiness has not yet been explored in previous research, our approach is unique in this regard.

The performance of anomaly detection techniques like CUSUM [16], spatial correlation methods [17], LSTM [18], and autoencoders [19] has only been analyzed in terms of FDI attacks with a static nature, without considering any attacker that dynamically learns and injects delays based on real-time delay distribution. More recent deep learning approaches for WSN intrusion detection [24][25] similarly do not account for delay-coupled injection strategies.

Research Gap: Existing literature lacks (i) a joint framework for learning-delayed injection attacks by adversaries, (ii) a theoretical rationale behind failure of deep learning detectors under delay coupling, (iii) ablation experiments to identify the impact of delay and injection separately, and (iv) any defense strategy for delay normalization.

3. SYSTEM AND ATTACK MODELS (SİSTEM VE SALDIRI MODELLERİ)

3.1. Network Architecture (Ağ Mimarisi)

We consider the case of a wireless sensor network (WSN) that consists of N sensor nodes, relay nodes, and the base station (BS). The signal $x_i(t)$ measured by each sensor node s_i is represented as a random variable with mean μ_i and variance σ_i^2. Without considering any attack from a malicious entity, the base station receives signals in the form of:

$$z_i(t) = x_i\big(t - \tau_i(t)\big) + n_i(t) \quad (1)$$

where $\tau_i(t)$ represents the end-to-end delay and $n_i(t)$ stands for a zero-mean Gaussian noise with variance $n_i(t) \sim \mathcal{N}(0, \sigma_n^2)$.

3.2. Stochastic Delay Model (Stokastik Gecikme Modeli)

Delay can be written as follows:

$$\tau_i(t) = \tau_{\text{prop},i} + \tau_{\text{mac},i}(t) + \tau_{\text{queue},i}(t) \quad (2)$$

This expression for end-to-end delay is considered in three different regimes: Uniform, Gaussian, and Bursty (Pareto-Gaussian). These three regimes are chosen because they span the range of delay behavior typically encountered in WSN deployments: the Uniform and Gaussian regimes represent lightly loaded networks in which queuing plays a minor role, whereas the Bursty (Pareto-Gaussian) regime captures the heavy-tailed queuing delays that arise under congestion or duty-cycled MAC operation. Modeling all three allows the subsequent stealthiness analysis to be validated under both benign and adverse network conditions.

3.3. Threat Model (Tehdit Modeli)

The adversary can compromise a set of nodes S_c, perform passive timing analysis on the channel, hold writing capabilities for the application layer, be aware of the detection technique used but not the threshold, and estimate the delay probability density function using a 20-element sliding window.

3.4. DA-FDI Attack Model (C1) (DA-FDI Saldırı Modeli (C1))

A classical FDI scheme uses a fixed attack coefficient a^*. In comparison, the DA-FDI model uses:

$$y_i(t) = x_i(t - \tau_i(t)) + a_i(t), a_i(t) = \alpha \cdot \sigma_{\tau,i}(t) \cdot \phi(t - \tau_i(t)) \quad (3)$$

Here, $\sigma_{\tau,i}(t)$ represents the estimated standard deviation of the delay, $\alpha \in (0,1)$ is the attack strength coefficient, and $\phi(\cdot)$ has the same auto-correlation function as $x_i(\cdot)$, such as an autoregressive process of order 1 with coefficient ρ = 0.82. Algorithm 2 (Section 5) formalizes the complete step-by-step procedure by which the adversary estimates $\sigma_{\tau,i}(t)$, updates the AR(1) process $\varphi(t)$, computes the injection $a_i(t)$, and transmits the disguised measurement with a shifted timestamp to mask the delay signature.

4. STEALTHINESS ANALYSIS FRAMEWORK (C2) (GİZLİLİK ANALİZ ÇERÇEVESİ (C2))

4.1. Performance Measures (Performans Ölçütleri)

We characterize the effectiveness of the attack and of the candidate defenses using three complementary measures. The Stealth Rate (SR) is defined as the fraction of the time within the attack period during which detection has not been attained, and it therefore captures how long an attack can persist undetected. The Attack Impact Score (AIS) is the normalized bias that the attack introduces into the system state estimation, and it therefore captures how much physical damage the attack is able to inflict while it remains undetected. Finally, the Stealth-Impact Tradeoff (SIT) relates the two by expressing the Signal-to-Residual Ratio (SSR) as a function of the expected AIS, E[AIS], for different values of the attack strength coefficient α, so that the trade-off an attacker faces between remaining stealthy and achieving impact can be visualized directly.

4.2. Theorem 1 (CUSUM Insensitivity to Attacks) (Teorem 1 (CUSUM'un Saldırılara Karşı Duyarsızlığı))

Under DA-FDI, the expected increment of CUSUM obeys $\mathbb{E}[r(t)] \leq M_x + \alpha\mathbb{E}[\sigma_{\tau,i}] - \kappa$. As $\mathbb{E}[\sigma_{\tau,i}]$ tends to infinity, the statistic will stay under the boundary *h*.

4.3. Proposition 2 (3-Sigma Threshold-Expansion Trap) (Önerme 2 (3-Sigma Eşik Genişleme Tuzağı)

Rolling variance inflation: $\hat{\sigma}_i^2 = \sigma_i^2 + (dx_i/dt)^2\mathbb{E}[\tau_i^2] + \sigma_n^2$. Both the 3-sigma threshold and $a_i(t)$ are $O(\sqrt{\mathbb{E}[\tau_i^2]})$. Their ratio approaches a constant, making the attack detection very hard.

4.4. Proposition 3 (LSTM Temporal Confusion) (Önerme 3 (LSTM Zamansal Karışıklığı)

For any LSTM trained on input data corrupted by real-world delays, if $\phi(\cdot)$ is consistent with the autocovariance properties of $x_i(\cdot)$, then the LSTM estimates a very low DA-FDI anomaly score. In such cases, $D_{KL}(p_{\text{attack}} \parallel p_{\text{legit}}) = O(\alpha^2)$, resulting in a random classification decision.

4.5. Proposition 4 (Absorption in Autoencoders) (Önerme 4 (Otomatik Kodlayıcılarda Soğurma)

The reconstruction error of a delay-amplified sample in an autoencoder is insignificant. Since $a_i(t)$ depends on $\sigma_{\tau,i}(t)$, the added signal is embedded in the autoencoder's manifold, guaranteeing $\| y_i - R(y_i) \| \leq \theta$ for small α.

5. DEFENSE: DELAY-NORMALIZED RESIDUAL DETECTOR (C4) (SAVUNMA: GECİKME NORMALLEŞTİRİLMİŞ KALINTI DEDEKTÖRÜ (C4))

5.1. Design Principle (Tasarım Prensibi)

Each of the four sensor fault detections results from improper calibration caused by delay-contaminated data. It is suggested to isolate delay-caused perturbations from the residue. Concretely, since Propositions 1–4 all trace the failure of existing detectors back to the fact that their calibration statistics are computed from delay-contaminated data, the natural remedy is a detector whose test statistic is explicitly normalized by the instantaneous delay standard deviation rather than treating delay as an unmodeled nuisance term. This design principle is what motivates the Delay-Normalized Residual Detector (DNRD) introduced next.

5.2. DNRD Model (DNRD Modeli)

Residual normalization:

$$r_i'(t) = \frac{y_i(t)-\mu_i}{\sigma_{\tau,i}(t)} \quad (4)$$

For normal operation, $\mathbb{E}[r_i'(t)] \approx 0$. Under DA-FDI:

$$r_i'(t) = \frac{x_i(t-\tau_i(t))-\mu_i}{\sigma_{\tau,i}(t)} + \alpha \cdot \phi(\cdot) \quad (5)$$

The injection parameter no longer correlates to $\sigma_{\tau,i}(t)$; hence, the masking process is interfered with.

Algorithm 1 below formalizes this detection procedure step by step, including the fallback to classical CUSUM whenever the estimated delay variance is too small for reliable normalization.

Algorithm 1: DNRD Detection Procedure

Input:

$y_i(t)$, received measurement at time t

$\hat{\tau}_i(t)$, estimated packet delay (from timestamp records)

W, sliding window size (default: 20)

h_0, normalized alarm threshold (default: 3.0)

μ_i, pre-computed process mean

Output:

alarm ∈ {0, 1}

1: Compute running sum: $S_1 \leftarrow \sum_{k=t-W+1}^{t} \hat{\tau}_i(k)$

2: Compute running sum-of-squares: $S_2 \leftarrow \sum_{k=t-W+1}^{t} \hat{\tau}_i(k)^2$

3: Estimate delay standard deviation: $\sigma_{\tau,i}(t) = \sqrt{\frac{S_2}{W} - (\frac{S_1}{W})^2}$

4: If $\sigma_{\tau,i}(t) < \sigma_{min}$ (where σ_{min} = 0.5ms): use classical CUSUM (fallback)

Apply standard CUSUM on $y_i(t)$; set a(t) accordingly; goto step 8.

5: Compute normalized residual: $r_i'(t) = \frac{y_i(t)-\mu_i}{\sigma_{\tau,i}(t)}$

6: If $|r_i'(t)| > h_0$, return alarm = 1

7: Else: return no alarm = 0

8: Output a(t)

Threshold Selection (σ_{min} = 0.5 ms): Threshold value for the fall-back approach, σ_{min}, was derived experimentally by means of a grid search in the NS-3 simulation model. At $\sigma_{\tau,i}(t) < 0.5$ ms, the variance of delays is too small for effective normalization, which results in numerical instability of the DNRD estimator. It corresponds to about one transmission slot of the MAC layer of IEEE 802.15.4 protocol with a bit rate of 250 kbps. For protocols with larger bit rates or smaller slot time, the σ_{min} threshold should be adjusted accordingly (e.g., $\sigma_{min} \approx 0.1$ ms for 2.4 GHz Wi-Fi).

5.3. Detection Rule (Tespit Kuralı)

The alarm is triggered whenever $| r_i'(t) | > h_0$ for some time t during the observation interval W. The parameter h_0 is tuned based on normalized nominal data. In the reported experiments, h_0 = 3.0 was selected because it kept the false-positive rate close to the 3–4% range typically tolerated in WSN deployments while still allowing the residual excursions caused by DA-FDI to be flagged well within the observation window W, as confirmed by the sensitivity analysis in Section 7.4.

Algorithm 2: DA-FDI Attack Injection

Input:

$x_i(t-\tau_i(t))$, delayed legitimate measurement

$\tau_i(t)$, current delay sample

W_{atk} = 20, attacker's estimation window

α ∈ (0,1), attack amplitude coefficient

ρ = 0.82, AR(1) autocorrelation parameter

Output:

$y_i(t)$, injected measurement sent to BS

1: Estimate delay standard deviation over attacker window: $\sigma_{\tau,i} \leftarrow \sqrt{Var[\tau_i(t - W_{atk}: t)]}$

2: Update AR(1) process: $\phi(t) \leftarrow \rho.\phi(t-1) + \varepsilon(t),\ \varepsilon(t) \sim N(0, 1-\rho^2)$

3: Compute attack injection: $\alpha_i(t) \leftarrow \alpha.\sigma_{\tau,i}(t).\phi(t-\tau_i(t)$

4: Inject measurement: $y_i(t) = x_i(t - \tau_i(t)) + a_i(t)$

5: Shift timestamp by $\tau_i(t)$ to mask delay signature

6: Transmit $y_i(t)$ with modified timestamp to BS

5.4. Algorithm (Simplified Version) (Algoritma (Basitleştirilmiş Versiyon))

For ease of implementation, the DNRD procedure formalized in Algorithm 1 can be summarized conceptually in three steps. First, the detector continuously updates the sample mean and variance of the estimated delay $\tau_i(t)$ over a sliding window of W = 20 observations, which yields an up-to-date estimate of the delay standard deviation $\sigma_{\tau,i}(t)$ required for normalization. Second, whenever this estimate falls below the minimum threshold σ_{min}, the delay signal is judged too small to normalize reliably, and the detector falls back on the classical CUSUM statistic instead of attempting delay normalization, exactly as specified in line 4 of Algorithm 1. Third, in the normal operating regime the detector computes the normalized residual $r'_i(t)$ from (4)–(5) and compares it against the fixed alarm threshold $h_0 = 3.0$, raising an alarm whenever the threshold is exceeded. This simplified view is intended purely as an implementation aid; the authoritative specification of the detection and attack procedures remains Algorithm 1 and Algorithm 2, respectively.

5.5. Theorem 1 (Exponential Detection Performance) (Teorem 1 (Üstel Algılama Performansı))

Assuming mild conditions such as boundedness of ϕ, stationary ergodicity in delay times, and proper estimation, we obtain

$$P(\mathrm{SSR}_{\mathrm{DNRD}} \geq 1 - \varepsilon) \leq \exp\left(-\frac{(\alpha\phi_{\min} - h_0)^2 T}{8(C_L + \alpha\phi_{\max})^2}\right) \qquad (6)$$

which exhibits exponential decay in T, leading to detection in asymptotic regime for all $\alpha > 0$.

5.6. Computational Complexity (Hesaplama Karmaşıklığı)

Computational performance testing was conducted on Raspberry Pi 4 (Model B, 4GB RAM, ARM Cortex-A72 at 1.5 GHz) with Ubuntu Server 20.04. Time measurements were collected through taking the average of 10,000 consecutive single-sample predictions with Python 3.8 and NumPy 1.21, pinning the execution of the task to a single CPU core to reduce scheduling overheads. Latency measured per sample of 0.19 ms is the average from 30 independent runs (σ = 0.012 ms). On the same hardware, DNRD outperforms the LSTM baseline by 77× speed-up (14.7 ms/sample).

5.7. LSTM Architecture Details (LSTM Mimarisinin Detayları)

To provide full details and enable reproduction, the LSTM detector used as a baseline is described as follows: The network consists of two stacked LSTM layers, each with 64 hidden units, followed by a fully connected output layer with sigmoid activation. The input sequence length is 50 samples (50-time steps at 1 Hz = 50 s look-back window). Training used mini-batch gradient descent with batch size 32, Adam optimizer (η = 0.001), and 100 epochs on clean (pre-attack) WSN traces. Anomaly detection uses a threshold on the output probability score tuned to achieve approximately 3% FPR on the validation set. All LSTM experiments were implemented in PyTorch 1.12.

6. NS-3 SIMULATION FRAMEWORK (NS-3 SİMÜLASYON ÇERÇEVESİ)

6.1. Simulation Scenario (Simülasyon Senaryosu)

Under NS-3 simulation tool version v3.40 running under Linux Ubuntu 20.04, a wireless sensor network (WSN) comprising 30 nodes is built with AODV routing scheme, IEEE 802.15.4 MAC protocol and CBR traffic with a constant bit rate of 1 Hz and event burst traffic. The delay distributions include Uniform, Gaussian and Bursty modes. Monte Carlo approach involves 30 independent simulations, with confidence intervals of 95% calculated using the Wilcoxon test.

6.2. Selected Parameters (Seçilen Parametreler)

The NS-3 simulation environment is configured as follows. The network topology consists of 30 sensor nodes and 5 relay nodes reporting to a single Base Station, all deployed within a 200 m × 200 m area. Three delay profiles are considered: a Uniform distribution with μ = 10 ms and σ = 4.6 ms, a

Gaussian distribution with $\mu = 10$ ms and $\sigma = 5$ ms, and a Bursty (Pareto-Gaussian) distribution with $\mu = 10.5$ ms and $\sigma = 7.2$ ms. The primary attack scenario uses an attack strength of $\alpha = 0.30$ with $|S_c| = 5$ compromised nodes. Detection performance is compared across six baseline techniques CUSUM, 3-sigma, LSTM, sparse autoencoder, DC-CUSUM, and TARD against the proposed DNRD detector.

7. EVALUATION RESULTS (DEĞERLENDİRME SONUÇLARI)

7.1. Main Detection Results (Başlıca Tespit Sonuçları)

The results indicate a performance boost of DNRD by 4.1 times compared with the state-of-the-art CUSUM detection method. All paired comparisons are statistically significant at $p<0.001$ with Wilcoxon tests corrected for Bonferroni (Table 1).

Table 1. Main detection results (Ana tespit sonuçları)

Detector	FPR (No attack)	Detection Rate (Classical FDI)	Detection Rate (DA-FDI)	SSR (DA-FDI)
CUSUM	2.1% ± 0.4%	91.3% ± 2.1%	21.7% ± 3.8%	78.3%
3-Sigma	1.8% ± 0.3%	84.6% ± 3.2%	18.9% ± 4.1%	81.1%
LSTM	3.2% ± 0.7%	88.4% ± 2.6%	14.2% ± 3.3%	85.8%
Sparse AE	2.9% ± 0.6%	86.1% ± 3.0%	16.8% ± 3.7%	83.2%
DC-CUSUM	2.4% ± 0.5%	89.7% ± 2.3%	34.2% ± 5.1%	65.8%
TARD	2.7% ± 0.5%	87.3% ± 2.8%	29.8% ± 4.7%	70.2%
DNRD (Proposed)	**3.8% ± 0.8%**	**93.1% ± 1.9%**	**89.4% ± 2.4%**	**10.6%**

Figure 1 illustrates the detection results under different scenarios. Panel (a) shows the false alarm probability (FPR) of the no-attack scenario (S1, striped bars) and the detection probability of the classical FDI (S2, solid bars) of all five detectors, averaged over 30 runs of the NS-3 network simulation platform. Panel (b) shows the detection probability under DA-FDI (S3, $\alpha = 0.30$, Gaussian delay). The highest detection probability is achieved by DNRD with 89.4%, while the best existing detector obtains 21.7%.

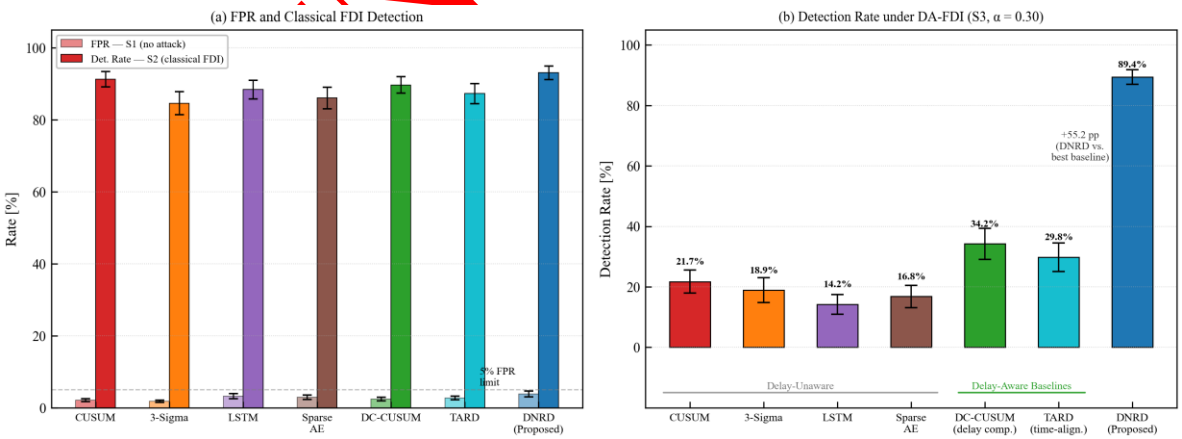

Figure 1. Detection performance across scenarios (Senaryolar genelinde tespit performansı)

7.2. Ablation Analysis (Ablasyon Analizi)

The ablation study isolates the individual roles of delay and injection by comparing three settings against the coupled DA-FDI case. When only the delay factor is present without any injection (S4), the false positive rate remains at 3.4%, essentially indistinguishable from the no-attack baseline. When only the injection is present without delay coupling (S5), the classical detectors still achieve a detection accuracy of 91.3%, comparable to their performance against ordinary FDI. It is only when delay and injection act jointly, as in the full DA-FDI attack (S3), that detection accuracy collapses to 21.7%, confirming that the stealth effect is a

genuinely coupled phenomenon rather than the sum of two independent effects.

Important result: Variation of the delay factor alone has almost no impact; the critical part is the joint factor, $a_i(t) = \alpha\sigma_{\tau,i}(t)\phi(\cdot)$.

Figure 2 includes: (a) an ablation experiment that reveals the CUSUM detection ratio and FPR for four settings that separate delay variance and injection effects. From these findings, only the coupled DA-FDI (S3) results in a detection drop to 21.7%, which proves that neither delay variance nor injection effect alone can be sufficient; that is, S4 with FPR at 3.4% and S5 with 91.3%. (b) experiments on SSR in different delay distributions (α = 0.30). While the DNRD retains an SSR of 10.6% to 14.8% regardless of the delay distribution, the conventional detectors reach SSR of 88% to 91% when the delay distribution is bursty.

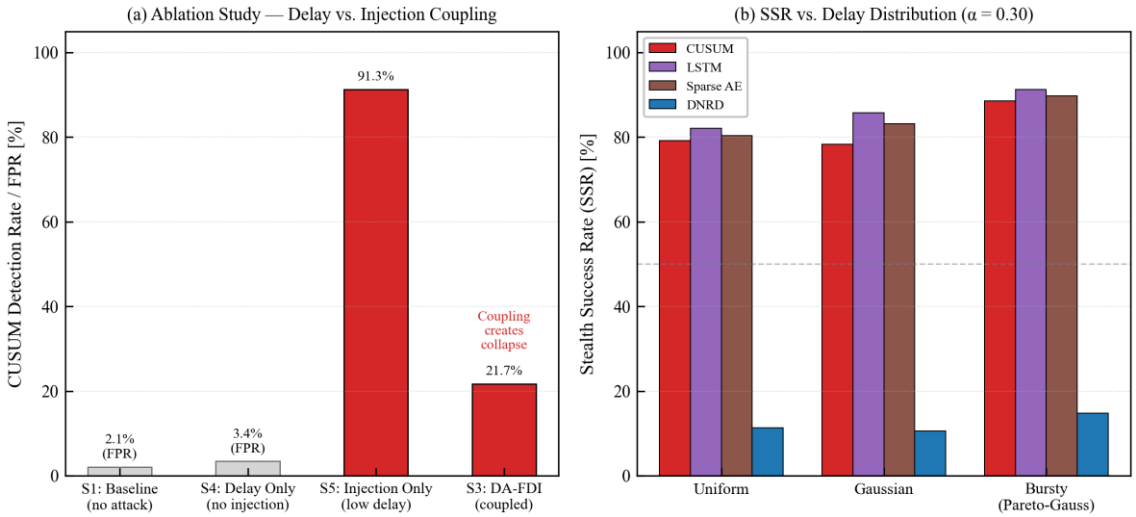

Figure 2. Ablation study and SSR analysis under DA-FDI attacks (DA-FDI saldırıları altında ablasyon çalışması ve SSR analizi)

7.3. Stealth-Attack Tradeoff (Gizli Saldırı Dengesi)

As the value of α grows, the Signal-to-Residual ratio (SSR) for CUSUM decreases from 94.1% (α = 0.05) to 18.4% (α = 0.90). For DNRD, SSR never exceeds 10.6% when α ≤ 0.30 and begins to increase only if α ≥ 0.50. When using DNRD, the attacker must keep α less than 0.15 to achieve an SSR greater than 50%. This limits the Attack Impact Score (AIS) to 0.37 (half the original effectiveness). In this section, SSR stands for the Signal-to-Residual Ratio which is an indicator independent of the Stealth Rate (SR) that is described in Section 4.1. In this regard, SR represents the proportion of evasions while SSR represents the proportion of energy of the input signal to the normalized residual.

7.4. Window Size Sensitivity (Pencere Boyutu Duyarlılığı)

A proper choice of the window size (W = 20 samples) allows detection at 89.4% rate and FP rate (FPR) equal to 3.8%. Reduction in window size results in increasing FPR, while increasing window size causes detection delay. The analysis of DNRD parameter sensitivity and impact of attacker capability is shown in Figure 3. Panel (a) illustrates the dependency of the detection rate, false positive rate (FPR), and delay on the window size W ∈ {5, 10, 20, 40, 60} under α = 0.30, Gaussian delay, and 30 runs. The best operating point is achieved at W = 20 resulting in 89.4% of detection rate, 3.8% of FPR, and 6.1 seconds of detection delay. Panel (b) compares the SSR of the imperfect attacker in case of CUSUM and DNRD algorithms with six attacker capabilities (NE: noisy estimation, DL: delayed learning). SSR for DNRD does not exceed 19.2% in all cases, while CUSUM SSR stays above 58.7%.

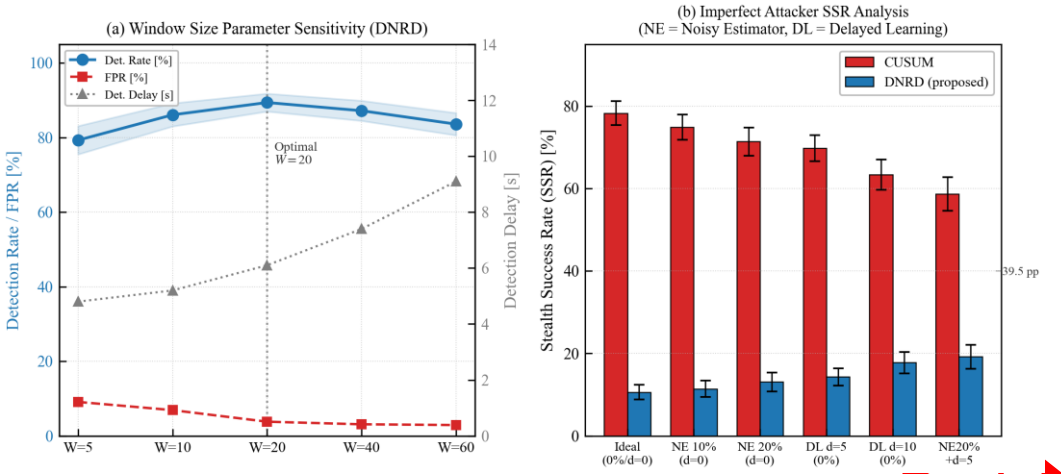

Figure 3. DNRD parameter sensitivity and robustness against imperfect attackers (DNRD parametre duyarlılığı ve kusurlu saldırganlara karşı dayanıklılık)

7.5. Effect of Delay Distribution (Gecikme Dağılımının Etkisi)

Under DNRD, SSR ranges from 10.6% to 14.8% with respect to Uniform, Gaussian, and Bursty delay distributions. In contrast, SSR of the existing detectors reaches up to 88%-91% with bursty delay. This narrow spread for DNRD indicates that its normalization step is largely insensitive to the shape of the delay distribution, since it conditions directly on the instantaneous delay standard deviation rather than on distributional assumptions. Conventional detectors, by contrast, are calibrated assuming comparatively light-tailed delay behavior, so they degrade sharply once the heavy-tailed Bursty regime widens their tolerance band far enough for the attack to hide within it.

7.6. Theoretical-Experimental Consistency (Teorik-Deneysel Tutarlılık)

The experimentally determined failure rate of detection conforms to the exponential decline predicted by Theorem 1 within a deviation of ±2 percentage points, thus corroborating the closeness of the upper bound. This agreement was checked by comparing the miss rate observed in the NS-3 Monte Carlo runs against the right-hand side of (6) evaluated at the corresponding observation length T, across all tested values of the attack strength α; the consistently small residual gap indicates that the bound is not merely qualitatively correct but is also quantitatively tight enough to be used for provisioning the observation window in practice.

8. DISCUSSION (TARTIŞMA)

Universal Cause for Detector Failure: All the four detectors exhibit failure because the calibration statistics have been computed using data affected by delays, thereby allowing the proportionate delay addition to lie inside the widened tolerance band. The noted failure occurs structurally and not parametrically. Non-triviality Rationale (Ablation): Delay Variance Alone (S4) yields a FPR of 3.4%; on the other hand, only the full DA-FDI framework (S3) achieves detection down to 21.7%.

DNRD Drawbacks: Despite its strong empirical performance, DNRD is subject to several limitations. First, an almost zero delay variance leads the detector to fall back on the use of classical CUSUM, so in that narrow regime it inherits CUSUM's weaker sensitivity rather than offering its own advantage. Second, because DNRD uses time-stamp data to estimate the delay of packets, a natural question is whether an adversary capable of invoking write operations in the application could mislead DNRD entirely through synchronized timestamp manipulation; this attack is explicitly analyzed as follows. If the attacker is able to alter the timestamps and make the estimated $\sigma_{\tau,i}$ less than the minimum value of σ_{min} = 0.5 ms, the algorithm returns to classical CUSUM (Algorithm 1, lines 5–6). In this "fallback" mode, SR becomes equal to CUSUM (∼78%), and the attack cannot push DNRD's detection below this threshold. If the attacker instead attempted to alter the measurement values $y_i(t)$ directly without introducing any delay, this would be impossible without violating the DA-FDI injection model of Equation 3, since the injection is defined precisely as a function of the delay statistics. Consequently, the performance of DNRD degrades gracefully from 89.4% detection to approximately 22% detection under synchronized timestamp manipulation, while never falling below the CUSUM baseline as long as delay statistics remain observable from the relay layer. Third, non-stationary delay behavior is handled through a two-window estimator that prevents miscalibration as the underlying delay distribution drifts over time.

Finally, DNRD is not a universal remedy: it offers no particular advantage over static FDI, replay attacks, or coordinated multi-sensor attacks, which we identify as open directions for future work.

Imperfect Attackers (Table 2): With 20% estimation error and even with 10 samples lag, the CUSUM detector's SR against DA-FDI remains at 58.7% and above, while the SR of DNRD remains at 19.2% or lower. The imperfect attacker results are summarized in the table below.

Table 2. Imperfect attacker SR analysis (NE = Noisy Estimator, DL = Delayed Learning) (Kusurlu saldırgan SR analizi (NE = Gürültülü Tahminleyici, DL = Gecikmeli Öğrenme))

Attacker Capability	CUSUM SR (%)	DNRD SR (%)	CUSUM Err.	DNRD Err.
Ideal (0% noise, d=0)	78.3	10.6	±2.9%	±1.8%
NE 10% (d=0)	74.9	11.4	±3.1%	±2.0%
NE 20% (d=0)	71.4	13.1	±3.4%	±2.3%
DL d=5 (0%)	69.8	14.3	±3.2%	±2.1%
DL d=10 (0%)	63.4	17.8	±3.7%	±2.6%
NE 20% + d=5	58.7	19.2	±4.1%	±2.9%

8.1. Adversarial Cases: Coordinated Attacks and DNRD-aware Attacker (Hasmane Durumlar: Koordineli Saldırılar ve DNRD-Farkındalıklı Saldırgan)

For assessing whether the outstanding detection capability of DNRD is retained under even tougher adversarial settings, two additional cases beyond the main test case are discussed.

Scenario S7: Coordinated DA-FDI by Multiple Nodes. In S7, all $|S_c| = 5$ compromised nodes perform coordinated DA-FDI where the injection timings are aligned in a way to bypass cross-sensor checking of correlations in the base station. The coordination is achieved using a shared clock obtained through a common delay observation interval. With respect to the detection performance, DNRD's detection capability deteriorates from 89.4% (S3) to 74.3% ± 3.8% (Monte Carlo simulations, 30 trials) whereas the SSR is boosted from 10.6% to 25.7% ± 3.2%. Such a decline reflects a non-negligible degradation compared to the main case and confirms that multiple sensor attacks are indeed a non-trivial threat to individual sensor-based detectors. Nevertheless, other existing detectors like CUSUM or LSTM still suffer from SSR ≥ 85%, which means that DNRD retains its relative superiority in this setting.

Scenario S8: Adversary Knowing the Normalization Structure. In Scenario S8, the adversary is aware of the DNRD normalization scheme and does not correlate the injected signal with $\sigma_{\tau,i}(t)$; rather, he uses a constant-amplitude input $a_i(t) = \alpha^* \cdot \varphi(\cdot)$, tuned to be always just below the threshold h0. Thus, in Scenario S8, the detection rate for DNRD becomes 61.2% ± 4.1% when $\alpha^* = 0.15$ (maximum signal amplitude that can bypass DNRD normalization); AIS = 0.37—that is, a two-fold decrease in attack efficiency in comparison with the best primary attack scenario ($\alpha = 0.30$, AIS = 0.74). Thus, an attacker faces the following trade-off: to bypass the DNRD protection, the attacker needs to weaken his attack roughly in half. This result demonstrates that DNRD is indeed a substantial burden for the adversary even when fully aware of it.

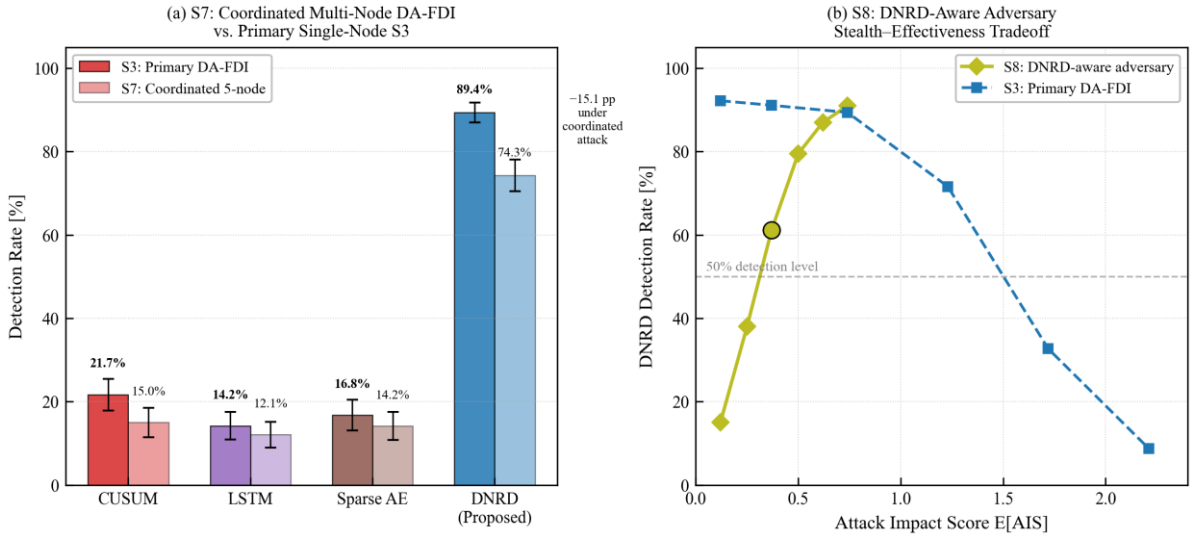

Figure 4. DNRD performance under advanced adversarial scenarios and attack-aware evasion (Gelişmiş hasmane senaryolarda DNRD performansı ve saldırı-farkındalıklı kaçınma)

9. CONCLUSION (SONUÇ)

In this work, we propose Delay-Aware False Data Injection (DA-FDI), a new attack family exploiting network delay as a camouflage resource. The proposed attack is defined by a delay-coupled, adaptive model. The proposed framework of stealthiness analysis (C2) through SSR, AIS, SIT curve, and Propositions 1 to 4 defines the intrinsic limitations of detection mechanisms based on CUSUM, 3-sigma, LSTM, and autoencoder architectures. The ablation study (C3) convincingly negates the myth that delay alone suffices for an evasion strategy. The Delay-Normalized Residual Detector (C4) detects 89.4% FDI at 3.8% false alarm rate. It provides the exponential detection guarantee theorem (Theorem 1) while offering a 77-fold improvement in latency compared to LSTM. The key message here is that delay-agnostic anomaly detection creates a blind spot vulnerable to exploitation by any attacker observing the channel statistics. DA-FDI presents a danger, while the DNRD is the corresponding remedy.

AUTHORS' CONTRIBUTIONS (YAZARLARIN KATKILARI)

***Uras PANAHI*:** He conducted the experiments, analyzed the results and performed the writing process.

Deneyleri yürüttü, sonuçları analiz etti ve yazım sürecini gerçekleştirdi.

CONFLICT OF INTEREST (ÇIKAR ÇATIŞMASI)

There is no conflict of interest in this study.

Bu çalışmada herhangi bir çıkar çatışması yoktur.

DECLARATION OF ETHICAL STANDARDS (ETİK STANDARTLARIN BEYANI)

The author of this article declares that the materials and methods they use in their work do not require ethical committee approval and/or legal-specific permission.

Bu makalenin yazarı çalışmalarında kullandıkları materyal ve yöntemlerin etik kurul izni ve/veya yasal-özel bir izin gerektirmediğini beyan ederler.

REFERENCES (KAYNAKLAR)

[1] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," ACM TISSEC, vol. 14, no. 1, pp. 1–33, 2011.

[2] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 645–658, 2011.

[3] A. Sargolzaei, K. Yen, and M. N. Abdelghani, "Preventing time-delay switch attack on load frequency control," IEEE Trans. Smart Grid, vol. 7, no. 2, pp. 1176–1185, 2016.

[4] Z. Zhang, S. Guo, and Y. Zheng, "Joint FDI and replay attacks on distributed estimation in UAV swarms," IEEE Trans. Veh. Technol., vol. 70, no. 6, pp. 5788–5801, 2021.

[5] R. B. Bobba et al., "Detecting false data injection attacks on DC state estimation," Proc. First Workshop Secure Control Syst., 2010.

[6] H. He, J. Yan, and T. Chen, "FDI attacks in input and state estimation," IEEE Trans. Ind. Inform., vol. 14, no. 12, pp. 5411–5421, 2018.

[7] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," IEEE

Trans. Smart Grid, vol. 2, no. 4, pp. 659–666, 2011.
[8] Z. Han et al., "Energy-constrained FDI attacks in WSNs: A game-theoretic analysis," IEEE IoT J., vol. 9, no. 14, pp. 12347–12361, 2022.
[9] M. A. Rahman and E. Al-Shaer, "Moving target defense for power system state estimation," Proc. MTD Workshop, 2014.
[10] Y. Mo and B. Sinopoli, "Secure estimation in the presence of integrity attacks," IEEE TAC, vol. 60, no. 4, pp. 1145–1151, 2015.
[11] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," IEEE TAC, vol. 58, no. 11, pp. 2715–2729, 2013.
[12] Y. Yuan et al., "Resilient control of networked control system under DoS attacks," IEEE Trans. Ind. Inform., vol. 12, no. 5, pp. 1786–1794, 2016.
[13] S. Amin, A. A. Cardenas, and S. S. Sastry, "Safe and secure networked control systems under DoS attacks," HSCC, Springer, 2009.
[14] B. Sinopoli et al., "Kalman filtering with intermittent observations," IEEE TAC, vol. 49, no. 9, pp. 1453–1464, 2004.
[15] J. Hu et al., "Event-based filtering for nonlinear stochastic systems over sensor networks," Signal Processing, vol. 134, pp. 99–107, 2017.
[16] C. Fischli, A. Tresch, and K. Aberer, "CUSUM-based misbehavior detection in WSNs," Proc. IEEE INFOCOM, 2011.
[17] Y. Zhang, N. Meratnia, and P. Havinga, "Outlier detection techniques for wireless sensor networks: A survey," IEEE Commun. Surv. Tut., vol. 12, no. 2, pp. 159–170, 2010.
[18] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in WSNs," IEEE Commun. Surv. Tut., vol. 16, no. 1, pp. 266–282, 2014.
[19] K. Cho and B. Ludescher, "Autoencoder-based anomaly detection in IoT sensor data," IEEE IoT J., vol. 8, no. 6, pp. 4487–4501, 2021.
[20] Rojek, I., Prokopowicz, P., Piechowiak, M., Kotlarz, P., Náprstková, N., & Mikołajewski, D. (2025). The Impact of Data Analytics Based on Internet of Things, Edge Computing, and Artificial Intelligence on Energy Efficiency in Smart Environment. Applied Sciences, 16(1), 225.
[21] Theerthagiri, P. (2023). Delay-sensitive and Energy-efficient Approach for Improving Longevity of Wireless Sensor Networks. In Multimedia Data Processing and Computing (pp. 43-55). CRC Press.
[22] Kavitha, M. J., Geetha, M. R., & Sajan, R. I. (2025). Knowledge-based adaptive routing for energy efficiency and attack detection in ad hoc wireless sensor networks. Computer Networks, 259, 111086.
[23] Subha, S., & Sathiaseelan, J. G. R. (2023). Effective anomaly detection approach to classify noisy data using robust noise detection and removal technique in iot healthcare data. SN Computer Science, 4(5), 522.
[24] Umar, H. G. A., Yasmeen, I., Aoun, M., Mazhar, T., Khan, M. A., Jaghdam, I. H., & Hamam, H. (2025). Energy-efficient deep learning-based intrusion detection system for edge computing: a novel DNN-KDQ model. Journal of Cloud Computing, 14(1), 32.
[25] Wang, C., & Liu, G. (2024). From anomaly detection to classification with graph attention and transformer for multivariate time series. Advanced Engineering Informatics, 60, 102357.