Modern Adaptable Zero Day Attack Detection in Network Traffic: Using Feature Identification and Tree Based Classifiers

Sivasankari K., M.E, (Ph.D)
Assistant Professor
The Department of Computer Science Engineering
SRM Institute of Science and Technology
Chennai, India

Alika Rizvi
The Department of Computer Science Engineering
SRM Institute of Science and Technology
Chennai, India

Adira Nair
The Department of Computer Science Engineering
SRM Institute of Science and Technology
Chennai, India

Anupama Mahata
The Department of Computer Science Engineering
SRM Institute of Science and Technology
Chennai, India

Abstract- **Zero-day attacks are sophisticated harms that take advantage of undisclosed weaknesses in software, making them exceedingly difficult to detect and prevent. Recently, attackers have been anxiously anticipating the discovery of previously unknown vulnerabilities that have not yet been patched or defended against. It is critical to detect and respond to these assaults in a timely way in order to prevent data breaches and secure sensitive information. By analysing network data and identifying aberrant activity, this research provides a machine learning-based solution to detecting zero-day attacks. The suggested system analyses network traffic with machine learning techniques to detect irregularities that might signal a zero-day assault. The NTA is critical for the network intrusion detection system (NIDS) since it monitors and extracts important data from network traffic data. The data is made up of several sorts of attributes that describe network packets, but not all of them are suitable for NIDS. It is critical to choose just those characteristics that have a substantial influence on our system. So, in order to identify the needed features, we apply Benford's Law to the numerical components of the data, such as IP addresses or packet sizes, and Zipf's Law to the non-numerical components, such as protocol headers or payload content. Finally, using ideally chosen features, we employ a semi-supervised ML technique that is successful for identifying zero-day attacks. The system is intended to be adaptable and scalable, with the ability to handle vast volumes of data and react to new attack patterns that keep developing. This project's ultimate purpose is to improve computer system security by identifying and blocking zero-day threats before they do harm.**

Keywords **— Zero-Day Attack, NTA, NIDS, Benford's law, Zipf's law**

I INTRODUCTION

Malicious actors can utilise zero-day attacks to infiltrate computer systems and obtain unauthorised access to sensitive data, making them an increasingly severe concern in modern times. These attacks are especially harmful because they target vulnerabilities in software or hardware that the program developer or vendor is unaware of and for which no patch or update has been published. Furthermore, since cybercriminals and nation-states have invested in the creation of these sorts of attacks, their usage has become more prevalent and sophisticated in recent years. As a result, organizations

ability to defend against these sorts of attacks has grown increasingly challenging, as there may be no established defence or mitigation plan. In March 2021, an organised gang of hackers launched a zero-day attack using a zero-day vulnerability in Microsoft Exchange Server. The flaw, later designated as CVE-2021-26855, allowed attackers to get access to email accounts and other sensitive data on susceptible computers. By exploiting weaknesses in Microsoft's Exchange Server email software, the hackers obtained access to critical data. The attackers gained access to email accounts, stole data, and installed malware on infected devices. Thousands of organisations worldwide were affected by this attack, including government bodies, corporations, and other groups. Microsoft issued emergency fixes to remedy the vulnerability, but by the time the patches were issued, the attackers had obtained access to numerous systems. This is only one example of how zero-day attacks may be used to exploit flaws in software and devices and obtain access to sensitive data. As technology advances, we should expect to see increasingly complex and targeted zero-day assaults in the future, emphasising the significance of good defences and incident response procedures. With the growth of technologies such as the Internet of Everything (IoE), wireless networks have become increasingly significant thus they have become vulnerable to zero-day attacks. As wireless networks are broadcast over the air, attackers can intercept and alter wireless communications without physically being present on the network. This enables eavesdropping, packet sniffing, DDoS, and man-in-the-middle assaults easier for attackers to carry out. To address these vulnerabilities, organisations must keep their wireless devices and protocols up to date with the latest security patches and upgrades, as well as utilise network intrusion detection systems (NIDS) that can identify and respond to zero-day attacks in real time. It examines network data for anomalous or harmful behaviour that might indicate a cyber attack attempt. In December 2020, NIDS aided in detecting the SolarWinds supply chain assault. In this instance, attackers gained access to SolarWinds' software development process, allowing them to include harmful malware into Orion software updates. We have focused on ML-NIDS, a sort of Network Intrusion Detection System that analyses network data and identifies potential security risks using machine learning methods. ML-NIDS, as opposed to typical rule-based intrusion detection systems, can learn from massive volumes of network traffic data to discover patterns and anomalies that may signal a security issue. ML-NIDS may detect previously undiscovered threats and react to changes in network traffic patterns by employing machine learning algorithms to recognise patterns and abnormalities. Additionally, ML-NIDS can assist minimise the amount of false positives and false negatives. In this study, we must discover the key features that can have an effect on the ML model. There are many properties in network traffic statistics, but we only want the important ones.The features of network traffic statistics are numerous, but we only need the most relevant ones. Techniques like singular value decomposition (SVD) are challenging to implement in a real-time NIDS setting due to their great complexity. High-dimensional feature space, data imbalance, data heterogeneity, dynamic nature of traffic, limited labeled data, and network traffic data complexity are some of the issues related with feature selection in network traffic data for NIDS. Given its great complexity and susceptibility to outliers, SVD can influence the selection process.To solve this sort of challenge, we combined Benford's law with Zipf's law, where Benford's Law concentrates on the leading digits of numerical data and Zipf's Law examines the rank-frequency distribution of data. The strategy is to first analyse the distribution of numerical data inside network traffic using Benford's Law, and then use Zipf's Law to analyse the distribution of traffic flows or packet sizes. A thorough examination of the network traffic pattern is achieved by studying both the leading digits and the rank-frequency distribution of the data, allowing for improved identification of aberrant behaviour. This increases the robustness of the feature selection process against noise and outliers in data while decreasing complexity. These two rules are used in tandem to acquire a more complete comprehension of the data. The obtained data serves as input for a semi-supervised ML learning strategy to train and test the models since it enhances the capacity to use vast amounts of unlabeled data while lowering dependency on labeled data. It enhances generalisation by learning from a bigger set of data, promotes flexibility by assisting the NIDS in adapting to changes in network traffic patterns, and decreases the processing resources required to train and maintain the model. It is claimed to be a successful strategy for NIDS since it may enhance system accuracy while decreasing reliance on labeled data and processing resources.

In our study, we categorise the data set as labeled or unlabeled once the characteristics have been correctly picked. The labeled data is utilised to train the ML model using the random forest algorithm (RFA), a more traditional and frequently used machine learning approach for classification tasks. It can identify known threats and handle a wide range of input attributes. The unlabeled data is then utilised to train the model with the isolation forest algorithm (IFA), a newer and less widely used approach for detecting anomalies and outliers in high-dimensional datasets. It's good for detecting new or unique assaults that don't fit any of the established patterns. The addition of RFA and IFA results in a more robust and effective ML-NIDS. RFA can detect known assaults and typical traffic patterns, whereas IFA can detect abnormal traffic patterns that do not adhere to the normal pattern. The outputs of these two algorithms may be combined to generate a more accurate and comprehensive ML-NIDS.

II EXISTING SYSTEM

According to the current system, a zero-dynamics attack (ZDA) is a model-based cyber assault. It is stealthy in nature as the presence of an attack signal cannot be identified by monitoring system output, and it is effective to the one utilising the generalised hold (GH), which is studied in the current system. The GH is a generalised variant of the zero-order hold, which is widely employed in digital control systems. In this study, the lethality of

ZDA and the efficacy of GH as a countermeasure are demonstrated utilising a control system that incorporates a DC-DC converter. The generalised hold transformer (GHT) may be used to discover new or unexpected attack patterns in the context of the attack detection by comparing them to a known collection of attack templates. The GHT may be trained to recognise similar patterns in network traffic by employing a set of known attack patterns. It is worth mentioning that the GHT technique may be ineffective at identifying zero-day attacks because it is based on a pre-defined collection of attack templates. By definition, zero-day attacks are previously unknown and do not match any current attack patterns.It was discovered that the current system had an arduous message update procedure. The real time complexity was significantly high, as was the likelihood of inaccuracy and insufficiency. It was not a simple system to use, and it took a lot of resources. There was a high amount of communication and computation overhead noticed.

III RELATED WORK

Many research publications have employed various approaches to identify and prevent ZDA. It was discovered in one of the studies [7], that Cyber-Physical Systems (CPS) are sophisticated systems which integrate cyber components, including sensors, actuators, and controllers, to track and regulate physical processes. In relation to zero-day attacks, CPS can be critical in recognising and reacting to these assaults. CPS may offer various advantages, including faster detection, improved situational awareness, and flexible security responses. It can assist organisations in more efficiently detecting and responding to zero-day threats, lowering the risk of harm and downtime. However, it is critical that CPS are built and deployed with sufficient security measures to avoid being an attractive target for intruders. As a result, auxiliary filters and systems were incorporated into the system to enhance the overall design of the CPS. Security Information and Event Management (SIEM) systems are meant to gather and analyse security-related data from numerous sources, including intrusion detection systems (IDS) and anomaly detection systems (ADS), in order to identify possible security risks. The generalised sampler, which takes a weighted average of numerous samples collected during one sampling interval, is used to develop a novel technique for detection of intrusions and defence against zero-dynamics attacks. The nulls of the sampled-data may be set at random positions by using the generalised sampler instead of the basic sampler, and if all of the zeros are positioned inside a given circle, the attack signal is no longer effective. The nulls of the sampled-data may be set at random positions by using the generalised sampler instead of the basic sampler, and if all of the zeros are positioned inside a given circle, the attack signal is no longer effective.This approach continues to operate even if all of the information is revealed to hackers, and it is extremely immune to the shifting of intrinsic zeros. Another research [22] describes an organic mix of Semantically Linked Network (SLN) and dynamic semantic graph creation for on-the-fly detection of zero-day threats utilising the Spark Streaming platform. A SLN is an application of ML that analyses text data to detect links between distinct ideas or entities. It may be used to detect and avoid zero-day attacks as part of a larger security plan. These networks, for example, may be used to analyse network traffic patterns and discover aberrant behaviour that may be suggestive of a zero-day assault. Security teams can analyse possible risks and take measures to limit any harm caused by the attack by spotting patterns of behaviour that depart from typical. SLN may also be used to detect flaws in systems or software that could be accessed by zero-day attacks. In addition, a minimal redundancy maximum relevance (MRMR) feature selection process is used to discover the dataset's most discriminating characteristics. The MRMR method computes a relevance and a redundant score per every attribute in the set of data. The relevance score assesses how closely a characteristic is connected to the desired variable or outcome, in this example, the occurrence of network intrusions. The redundancy score quantifies how closely a feature is connected to other characteristics in the dataset. The MRMR algorithm chooses a subset of characteristics that maximises relevance while minimising redundancy. The NIDS model is then trained using this selection of characteristics. A study [17] was utilised Quantized zero dynamics hacks against sampled data control systems are a form of cyber attack that focuses on the zero dynamics of an automation system that employs or discretized sampled data observations. The zero dynamics of a system in control theory relate to the behaviour of the system as a whole when the signal it receives is zero, i.e. when there is no external stimulus to the system. The system's inputs as well as its outputs are monitored at periodic time intervals in a collected data control system, and the resulting measurements are subsequently quantized into separate numbers. A quantized zero dynamics attack attempts to disturb the system's behaviour when the supplied signal is zero by changing the system's quantized measurements. The idea of universal zero dynamics in control theory refers to a property of a system in which the zero dynamics of the system are same for all potential stable disturbances. This indicates that the zero dynamics of a single-input single-output (SISO) system are the same for all conceivable stable inputs to the system. A SISO system exhibits universal zero dynamic if, independent of the exact choice of input, its result reaches zero approaching infinity for any consistent input . In other words, at the zero set, the system's dynamics are independent of the particular entry signal and only rely on the framework's internal behaviour. A research project [12] has also utilised Autonomous and Multi-Source Zero-Trust Authentication .It is a sort of system of authorization that uses numerous sources that contain data to authenticate an individual's legitimacy and authorise access to resources. The study demonstrated how it may be used to fight against ZDA assaults, which target previously discovered flaws in systems. The authentication

mechanism can offer an extra layer of defence against zero-day attacks by leveraging several sources of data to validate a user's identity. For example, if a ZDA steals an individual's login information or token, a multi-source authentication system can utilise additional criteria such as biometric data or user behavior to recognise that the user's identity has been compromised and block access to the system.

IV PROPOSED SYSTEM

In our system, we applied two unique feature selection mechanisms, Benford's law and Zipf's law, on the kdd dataset to generate a more precise form of data subgroup with featured properties, which helps to enhance the NIDS system's performance. Benford's Law is concerned with the starting digits of numerical data, whereas Zipf's Law is concerned with the rank-frequency distribution of numerical data. In some circumstances, both of these laws may be used concurrently to achieve a more complete picture of the data. Our strategy is to first analyse the distribution of numerical data inside network traffic using Benford's Law, and then utilise Zipf's Law to analyse the distribution of the flow of traffic or packet sizes. A more detailed knowledge of network traffic patterns may be acquired by studying both the leading numerals and the rank-frequency pattern distribution of the data, allowing for improved identification of aberrant behaviour. Once the criteria have been accurately selected, we categorise the data set as labelled or unlabelled in our study. The tagged data is utilised to train the ML model with the random forest algorithm (RFA), which is a more conventional and widely used machine learning strategy for classification problems. It is capable of detecting known dangers and handling a wide range of input properties. The unlabeled data is then utilised to train the model using the isolation forest algorithm (IFA), a newer and less extensively used method for spotting anomalies and outliers in large datasets. It is useful for detecting new or unusual attacks that do not fit into any of the established patterns. With the inclusion of RFA and IFA, the ML-NIDS becomes more robust and effective. RFA can identify known attacks and regular traffic patterns, whereas IFA can detect anomalous traffic patterns that deviate from the norm. These two algorithms' results can be merged to create a more accurate and comprehensive ML-NIDS. With the inclusion of RFA and IFA, the ML-NIDS becomes more robust and effective. RFA can identify known attacks and regular traffic patterns, whilst IFA can detect anomalous traffic patterns that deviate from the norm. These two algorithms' results can be merged to create a more precise and comprehensive ML-NIDS. The Benford's law is stated as follows:

$$P(d) = \log10(1 + 1/d)$$

where P(d) is the probability that the first digit is d and d is a digit from 1 to 9. Zipf's law is an empirical statement stated mathematically as follows:

$$f(r) = C / r^k$$

where f(r) is the mean frequency of the word at r representing the rank, C is a constant, and k is a parameter that is normally near to 1.

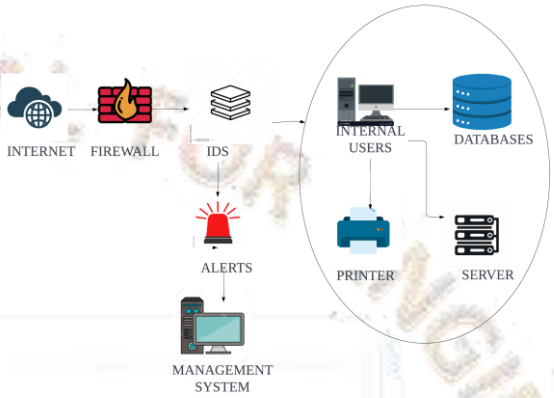

Figure 1. Architecture diagram for the IDS used in our study

The above figure 1 describes how a network packet is routed from the internet to a computer via a firewall. The firewall is a kind of network security device that monitors and restricts network traffic based on predefined security rules. If the packet matches the firewall's requirements, it is let through and routed to the IDS system. The intrusion detection system (IDS) is a kind of security device that examines network traffic for anomalous behaviour. or policy breaches and warns administrators. The IDS examines the packet headers and payload for evidence of intrusion or abnormal behaviour. We employ Benford's law and Zipf's law within the IDS system to acquire feature characteristics that are beneficial for the NIDS, and the chosen characteristics are then used as input for future ML models. Once the qualities have been successfully selected, we label a data set as labelled or unlabeled. The labelled data is utilised to train the ML model, which is trained using RFA, a more conventional and widely used machine learning strategy for classification problems. It is capable of detecting known dangers and handling a broad spectrum of input properties. The unlabeled data is subsequently utilised to train the model using the IFA, a newer yet less extensively used method for spotting anomalies and outliers in large datasets. It is useful for identifying new or unusual attacks that do not fit into any of the recognised patterns. With the inclusion of RFA and IFA, the ML-NIDS becomes more robust and effective. RFA can identify known attacks and regular traffic structures, however IFA can detect anomalous traffic patterns that deviate from the norm. These two algorithms' results can be merged to create a more precise and comprehensive ML-NIDS. After the IDS system analyzes the packet, it is forwarded to the destination PC. If an IDS identifies an anomaly or suspicious behaviour, it sends an alert or notice to the

security personnel or administrator, containing information about the discovered activity such as the addresses of the source and destination, the protocol, and any additional pertinent data. The notice can be delivered through SMS, email, or any other method of communication.

V RESULTS AND DISCUSSION

The categorization strategy, particularly Benford's law and Zipf's law, is used to construct table 1, which indicates the relevance of the parameters that impact the detection system. Table 2 lists numerous classes, their attack kinds, and their total number of attacks. It denotes the number of separate attacks that have been counted using the specified attributes from the dataset. Both Figures 2 and 3 show the accuracy curve for the set that was trained as well as the observed validation loss. This accuracy curve is obtained by combining the semi-supervised model, i.e. the random forest method, with the isolation algorithm. RFA is a powerful classifier that can handle high-dimensional data with a large number of features successfully, while IFA is another powerful technique for detecting anomalies in high-dimensional datasets. It is especially well-suited for identifying odd and unexpected occurrences, which are the source of zero-day attacks. The combination of RFA and IFA in NIDS may significantly improve the accuracy and efficacy of intrusion detection, as demonstrated by our suggested system's confusion matrix revealed that the macro avg accuracy is 0.53, and the weighted avg is 0.91. The f1- score has a precision of 0.92.

Feature	**Importance(in %)**
duration	0.153
protocol_type	6.705
service	0.001
flag	0.014
src_bytes	3.115
dst_bytes	6.372
land	0.012
wrong_fragment	1.140
urgent	0.002
logged_in	4.677
num_failed_logins	0.024
is_guest_login	0.208
num_access_files	0.004
dst_host_count	2.560
dst_host_srv_count	2.864
same_srv_rate	4.442
rerror_rate	0.901
srv_serror_rate	4.321
root_shell	0.018
srv_rerror_rate	0.478
dst_host_same_srv_rate	2.610
srv_diff_host_rate	0.664
srv_count	11.467
serror_rate	5.463
dst_host_diff_srv_rate	1.567
num_root	0.008
diff_srv_rate	3.226
dst_host_same_src_port_rate	5.043
dst_host_serror_rate	9.601
dst_host_srv_serror_rate	5.529
dst_host_rerror_rate	2.247
dst_host_srv_rerror_rate	1.882

Table 1:feature selection importance

Class	**Attack Type**	**Count**
dos	smurf	280790
dos	neptune	107201
normal	normal	97278
dos	back	2203
edos	satan	1589
edos	ipsweep	1247
edos	portsweep	1040
r2l	warezclient	1020
dos	teardrop	979
dos	pod	264
edos	nmap	231
r2l	guess_passwd	53
u2r	buffer_overflow	30
dos	land	21

r2l	warezmaster	20
r2l	imap	12
u2r	rootkit	10
u2r	loadmodule	9
r2l	ftp_write	8
r2l	multihop	7
r2l	phf	4
u2r	perl	3
r2l	spy	2

Table 2: attacks and its count

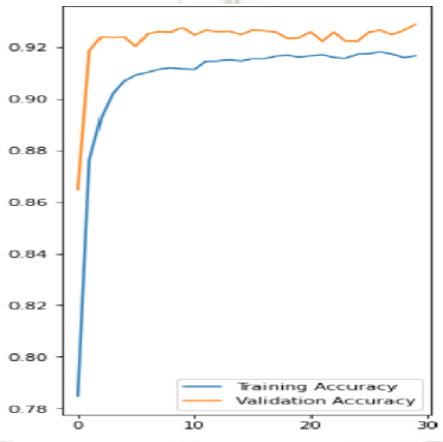

Figure 2: Accuracy on test dataset

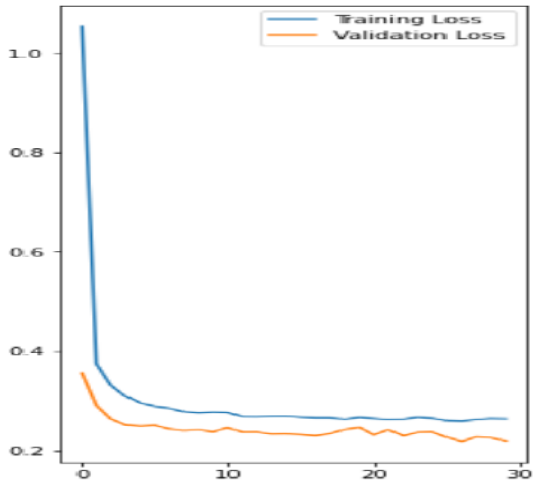

Figure 3: Training and validation loss

VI CONCLUSION

In conclusion, IDS is a critical component of network security that monitors and identifies any hostile or suspicious network activity. It functions as a detective control, alerting security professionals to possible security concerns and directing them to investigate and respond. IDS can be either host-based or network-based, and it can employ a variety of detection approaches such as detection based on signatures, anomaly-based being identified, or ML based detection. NIDS generally have three components: a sensor, a console, and a database. The sensor monitors network traffic and sends warnings to the console whenever an abnormality is found. The application of selective method of feature extraction such as Benford's law and Zipf's law has enhanced the detection of zero-day attacks.The usage of RFA and IFA in NIDS can enhance the accuracy of identifying zero-day threats greatly. RFA and IFA efficacy may vary based on the features of network traffic data. As a result, further study and testing are required to adequately assess the potential of these techniques for NIDS. Overall, the incorporation of RFA and IFA into NIDS is a positive step towards increasing the reliability and efficiency of identifying zero-day threats.

REFERENCES

[1]. Shim, H, Back, J..: Reduced-order implementation of disturbance observers for robust tracking of non-linear systems. IET Control Theory & Applications 8(17), 1940–1948 (2014)

[2]. Freudenberg, J. S., Middleton, R. H., Braslavsky, J. H.: Robustness of zero shifting via generalized sampled-data hold functions. Transaction on Automatic Controls (12) IEEE, 1681–1692 (1997)

[3]. Giles, A.: Triton is world's most murderous malwares, and it's spreadings. MIT Technology Reviews, March 5 (2019)

[4]. Anderson, B.D.O., Hitz, B.E.: Discrete positive-real functions and their application to system stability. Proc. of IEE 116(1), pp. 153–155, 1969

[5]. Hoehn, A., Zhang, P.: Detection of covert attacks and zero dynamics attacks in cyber-physical systems. In: Proc. of American Control Conference, pp. 302–307 (2016)

[6]. Jeon, H., Aum, S., Shim, H., Eun, Y.: Resilient state estimations for control system using multiple observers and median operations. Mathematical Problem in Enginering, Hindawi Publishing Corporations (2016).

[7]. Amir Baniamerian, Khashayar Khorasani, Nader Meskin, : Monitoring and Detection of Malicious Adverserial Zero Dynamics Attacks in Cyber Physical System in IEEE Conference on Control Technology and Applications 24-26 Aug. 2020.

[8]. Kim, D., Ryu, K., Back, J.: Zero Assignment via Generalized Sampler: A Countermeasure against Zero-Dynamics Attack (2012)

[9]. Yuz Ryu., Back, A.: Security enhancements of sampled-data system: Zero assignment via generalized samplers. In: Process of IFAC Worlds Congress (2020)

[10]. Shim, H., Back, J., Kim, J., Lee, C., Voulgaris, P.G., Park, G.,: Neutralizing zero dynamics attack on sampled-data systems via generalized holds. Automatica 113 (2020).

[11]. Kim, J., Park, G., Shim, H., Eun, Y.: Masking attack for sampled-data systems via input redundancy. IET Control Theory & Applications 13(14), 2300–2308 (2019).

[12]. Yunfei Ge, Quanyan Zhu, :MUFAZA: Multi-Source Fast and Autonomous Zero-Trust Authentication for 5G Networks in MILCOM, 2022 IEEE Military Communication Conference (MCC); 02 December 2022.

[13]. Assante, M.J., Lee, R.M., and Conway, T.: Analysis of cyber attacks on the Ukrainian power grid. SANS Industrial Control System, Washington, DC. USA, Tech. (2016)

[14]. Eun, Y. Shim, H., and Lee, C.: On redundant observability: From security index to attack detection and resilient state estimation. IEEE Transaction on Automatic Controls (2019).

[15]. G., Kim, Lee, J, and J., Shim, H.: Fully distributed resilient state estimations based on the distributed medians solver. IEEE Transaction on Automatic Controls (2020).

[16]. Naghnaeian, M., Hirzallah, N.H., Voulgaris, P.G.: Security via multirate control in cyber–physical systems. Systems & Control Letters 124, 12 – 18 (2019)

[17]. W. Steven Gray, Kurusch Ebrahimi-Fard, Alexander Schmeding, : Universal Zero Dynamics: The SISO Case; 2021 55th IEEE Annual Conference Informations Sciences and Systems (CISS); 19 April 2021.

[18]. Park, G., Lee, C., Shim, H.: On stealthiness of zero-dynamics attacks against uncertain nonlinear systems: A case study with quadruple-tank process. In Proc. of International Symposium on Mathematical Theory of Networks and Systems (MTNS), Hong Kong (2018)

[19]. Park, G., Lee, C., Shim, H., Eun, Y., Johansson, K.H.: Stealthy adversaries against uncertain cyber-physical systems: Threat of robust zero-dynamics attack. IEEE Transactions on Automatic Control 64(12), 4907–4919 (2019)

[20]. Park, G., Shim, H., Lee, C., Eun, Y., Johansson, K.H.: When adversary encounters uncertain cyber-physical systems: Robust zero-dynamics attack with disclosure resources. In: 2016 IEEE 55th Conference on Decision and Control, pp. 5085–5090 (2016).

[21]. Shieh, L.S., Wang, W.M., Bain, J., Sunkel, J.W.: Design of lifted dual-rate digital controllers X-38 vehicle. Journals of Guidance, Control, and Dynamic 23(4), 629–639 (2001)

[22]. Sai C. Pallaprolu; Rishi Sankineni; Muthukumar Thevar; George Karabatis; Jianwu Wang, :Zero-Day Attack Identification in Streaming Data Using Semantics and Spark; 2017 IEEE International Conference on Services Economics (SE); 11 September 2017

[23]. Shim, H., Park, G., Joo, Y., Back, J., Jo, N.H.: Yet another tutorial of disturbance observer: Robust stabilization and recovery of nominal performance. Control Theory and Technology 14(3), 237–249 (2016)

[24]. Slay, J., Miller, M.: Lessons learned from the Maroochy water breach. Critical Infrastructure Protection 253, 73–82 (2007)

[25]. Sussmann, H., Kokotovic, P.: The peaking phenomenon and the global stabilization of nonlinear systems. IEEE Transactions on Automatic Control 36(4), 424–440 (1991)

[26]. Teixeira, A., Shames, I., Sandberg, H., Johansson, K.H.: Revealing stealthy attacks in control systems. In: 2012 50th Annual Allerton Conference on Communication, Control, and Computing, pp. 1806–1813 (2012).

[27]. Yuz, J.I., Goodwin, G.C.: Sampled-Data Models for Linear and Nonlinear Systems. SpringerVerlag (2014)