World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:17, No:12, 2023

Current Drainage Attack Correction via Adjusting the Attacking Saw Function Asymmetry

Yuri Boiko, Iluju Kiringa, Tet Yeap

Abstract**—**Current drainage attack suggested previously is further studied in regular settings of closed-loop controlled Brushless DC (BLDC) motor with Kalman filter in the feedback loop. Modeling and simulation experiments are conducted in a MATLAB environment, implementing the closed-loop control model of BLDC motor operation in position sensorless mode under Kalman filter drive. The current increase in the motor windings is caused by the controller (p-controller in our case) affected by false data injection of substitution of the angular velocity estimates with distorted values. Operation of multiplication to distortion coefficient, values of which are taken from the distortion function synchronized in its periodicity with the rotor's position change. A saw function with a triangular tooth shape is studied herewith for the purpose of carrying out the bias injection with current drainage consequences. The specific focus here is on how the asymmetry of the tooth in the saw function affects the flow of current drainage. The purpose is two-fold: (i) to produce and collect the signature of an asymmetric saw in the attack for further pattern recognition process, and (ii) to determine conditions of improving stealthiness of such attack via regulating asymmetry in saw function used. It is found that modification of the symmetry in the saw tooth affects the periodicity of current drainage modulation. Specifically, the modulation frequency of the drained current for a fully asymmetric tooth shape coincides with the saw function modulation frequency itself. Increasing the symmetry parameter for the triangle tooth shape leads to an increase in the modulation frequency for the drained current. Moreover, such frequency reaches the switching frequency of the motor windings for fully symmetric triangular shapes, thus becoming undetectable and improving the stealthiness of the attack. Therefore, the collected signatures of the attack can serve for attack parameter identification via the pattern recognition route.

Keywords**—**Bias injection attack, Kalman filter, BLDC motor, control system, closed loop, P-controller, PID-controller, current drainage, saw-function, asymmetry.

I. Introduction

With the integration of the Internet of Things (IoT) technology into industrial infrastructure, the significance of developing robust algorithms for cyber-attacks and defenses targeting cyber-physical systems has increased. The expansion of IoT technology into industrial contexts has augmented the potential attack surface and vulnerability of these systems, necessitating the creation of sophisticated defense mechanisms to counteract evolving cyber threats. Recently, the current drainage attack has been suggested [1] to take place as a result of bias injection into feedback loop of closed loop-controlled BLDC motor under Kalman filter drive [2]. Such research effort contributes to development of cyber security of the industrial control systems (ICS) connected to a cyber space [3]. Maintaining security of such systems becomes essential for operation of ICS [4]. On the other hand, this also opens exploration area for potential attacks, initiated from either inside the industrial facilities or alternatively from the cyber space [5]. Potential purpose of the attackers of ICS may become disruption of industrial process, reducing its efficiency, or overtaking control of various parts of it or of systems as a whole [6]. As a measure of defense in this case comes techniques of intrusion detection [7], attacks dissemination as well as control regaining methods [8].

Successful demonstration of engaging Transmission Control Protocol/Internet Protocol (TCP/IP) connections to obtain the channels for cyber-attack and based on that a stealthy attack methodology was suggested against closed-loop cyber-physical systems with reference signals [9].

Specific components that may be a target for attacks include electrical motors, which are a common place in robotics, automation systems, transportation vehicles. A Raspberry PI based controller of DC motor revealed vulnerability via TCP port connection, which was shown to allow an attacker switching input and output port connectivity and then substituting the reference speed of operated DC motor with false data [10].

Another type of attack may include attempts of compromising the integrity of the acting state estimator, for example by hijacking data for selected subset of sensors and sending altered readings [11]. As Kalman filter gained popularity in state estimator role, such attack may be efficient if directed against Kalman filter [12]. However, in the current literature the dynamics of false data injection process is regarded to be independent on dynamics of the system. Linking both via some interdependence via specific functionalities may create additional possibilities for cyber-attacks, of which it is important to be aware of as well as have detection and defense tools.

II. Problem Formulation

In the first report of the current drainage attack, the triangular saw function was considered as a distortion tool for the modification of the feedback data stream values of the angular velocity [1]. Various depths of triangular saw function profiles were considered in terms of its effect on the current drainage flow. This effort brought about set of specific signatures of current drainage attack for future use via pattern recognition for

Yuri Boiko, Iluju Kiringa, and Tet Yeap are with Electrical Engineering and Computer Science Dept., University of Ottawa, Ottawa, ON, Canada (e-mail: yboik074@uottawa.ca, Iluju.Kiringa@uottawa.ca, tyeap@uottawa.ca).

attack detection purposes. Consideration, however, was limited to only single type of triangular shape, specifically, to the right triangle. This type of triangle in saw function has highest possible asymmetry along the direction of time flow. In turn, this means, from one hand, the strongest possible change of disturbance with the time, from the other hand, it also corresponds to the least stealthy approach for the attack. Therefore, in order to find better balance between the strength of the attack and its stealthiness, alternative shapes for the tooth of saw function need to be explored. For that matter, the opposite to the right triangle in terms of asymmetry along time axis would be isosceles triangle shape, which would provide best symmetry for saw tooth in time direction. Between the two opposites, a set of various acute triangle shapes of the tooth in saw function would represent partial asymmetry case. Therefore, the goal of the present research is to verify the effect of the asymmetry in triangular tooth shapes of attacking saw function on current drainage flow in terms of the attack strength, its stealthy implementation, as well as to determine attack signature features which are linked to the saw tooth asymmetry.

In mathematical terms, the bias injection here is represented by the following substitutions at the update stage of the state equation for the Kalman filter driving BLDC motor [1]:

(i) $\omega \rightarrow \chi\omega$,

(ii) $u_a \rightarrow u_a+\Delta u/3$,

(iii) $u_b \rightarrow u_b+\Delta u/3$,

(iv) $u_c \rightarrow u_c+\Delta u/3$

where all variables are defined as follows (see Fig. 1):

- ω is the angular speed of rotor (it is state variable); $\omega = d\theta/dt$;
- θ is angular position of the rotor;
- χ is a distortion coefficient used by the attacker to alter the values in the data stream of estimated values of ω;
- u_a, u_b, and u_c are the operating voltages of the motor's windings enumerated alphabetically;
- Δu is the corrective voltage generated by the controller.

Quantitatively, substitution *(i)* originated by the attacker to affect the state equation is causing the controller response to generate compensating substitutions *(ii), (iii)* and *(iv)* to restore the balance.

III. System Architectures

To address the set goal, selected is an architecture with position sensorless drive for BLDC motor (see Fig. 1). An earlier report [1] describes the initial version of similar architecture in more details and shows model verification via various tests. Such tests have been repeated herewith and the time slots in $t = [0; 1.5]$ are aiming to demonstrate reaching the stable operation of the model. The attack starting point here is always $t_{start} = 1.5$ *sec,* while termination of the attack occurs at $t_{end} = 2.0$ *sec*.

A distinctive feature of the architecture in Fig. 1 is the presence of the access point for the bias $\partial\omega$ injection where angular speed ω estimates made by Kalman filter are modified by the multiplication to distortion coefficient χ thus injecting the bias term $\partial\omega$. At that moment ω is replaced with $\chi\omega = \omega\pm\partial\omega$ to be processed by the controller's comparator node to calculate deviation of the $\omega\pm\partial\omega$ from the reference value ω_{ref}, to produce an error term:

$$error = \omega_{ref} - (\omega\pm\partial\omega) \tag{1}$$

for the controller to compensate.

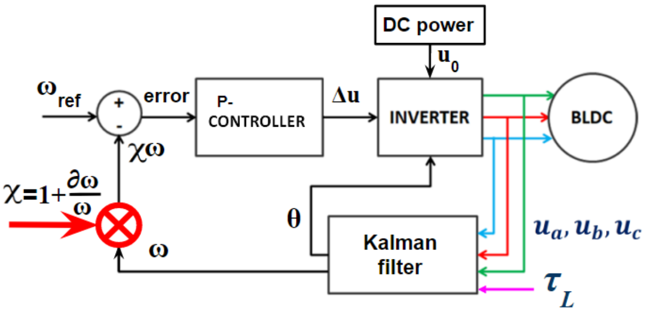

Fig. 1 Bias injection architecture with position sensorless drive for BLDC motor as well as bias injection $\partial\omega$ access point; Kalman filter inputs are voltages in the windings, u_a, u_b, u_c, and load torque τ_L.

A. No Bias Injection Case

Under normal operating conditions without any attack (i.e., no injected bias, $\partial\omega = 0$, and $\chi = 1$), a stable motor operation is characterized by the following parameters: $error = 0$, $\omega = \omega_{ref}$ at a reference speed, the controller outputs $\Delta u = 0$, and consequently, the inverter only receives the input voltage u_0 from the power source. If an error deviates from *0*, the controller outputs addition of Δu to the DC power supplied to inverter totaling it to $u_{DC} = u_0+\Delta u$, where for proportional controller:

$$\Delta u = K_p{*}error \tag{2}$$

and where K_p is the proportionality coefficient for *P*-controller used as a controller's tuning parameter for an error compensation. Operation with no bias injection occupies herewith the time slots in $t = [0; 1.5]$ *sec* to reach stable operation of the model and start the attack test at $t_{start} = 1.5$ *sec*.

B. Operation with Bias Injection

Bias injection occurs when attacker sets $\partial\omega \neq 0$, either positive or negative, substituting initial Kalman filter estimation ω with modified value $(\omega\pm\partial\omega)$. Equations (1) and (2) still apply, however the resulting value of Δu produced by controller would account on the bias term as if it were part of Kalman filter estimate. The resulting mismatch between the state estimate provided to the controller and the actual state constitutes the condition indicating operation under attack.

Calculation of $\partial\omega$ at each point of time has been carried out from the following equality:

$$\chi\omega = \omega\pm\partial\omega \tag{3}$$

with χ being a desired by attacker distortion coefficient in transforming the estimation of ω by Kalman filter into modified values $\chi\omega$.

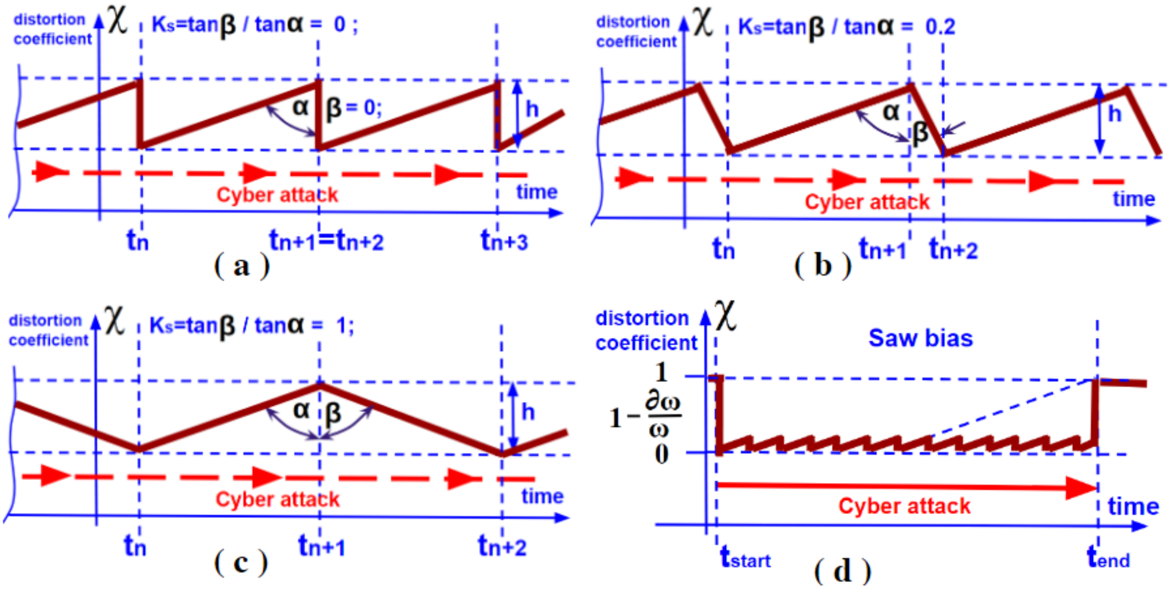

Fig. 2 Tested distortion bias coefficient, χ, saw-functions: (a) fully asymmetric triangle; (b) partially asymmetric triangle; (c) fully symmetric triangle; (d) attack flow engaging saw function

C. Asymmetry in Saw Function

To quantitatively characterize the asymmetry of the triangular tooth in the attacking saw-function, we introduce a symmetry coefficient K_S defined as:

$$K_S = tan(\beta)/tan(\alpha) \tag{4}$$

and where angles α and β are shown in Figs. 2 (a)-(c). Thus defined, $K_S = 0$ brings about fully asymmetric case of Fig. 2 (a) (zero symmetry), $K_S = 1$ corresponds to fully symmetric tooth in saw-function shown in Fig. 2 (c), whereas intermediate cases of $0 < K_S < 1$ in tooth asymmetry are represented in Fig. 2 (b) (partial symmetry/asymmetry).

D. Bias Coefficient Functions Tested

To assess how asymmetry in the tooth shapes of the attacking saw-function impacts the observed attack flaw in the current drainage scenario illustrated in Fig. 2 (d), a range of tests were performed using different tooth shapes depicted in Figs. 2 (a)-(c) for the bias coefficient saw-functions. This investigation aimed to uncover the relationship between diverse tooth shapes (from Figs. 2 (a)-(c)) and the resulting attack flaw. Varied here is also tooth height, which in turn is related to the modulation depth of the attacking distortion coefficient χ.

IV. Simulation Results

For comparative purpose, herewith we follow the timing schedule as in [1], implementing the bias injection attack starting at $t = 1.5$ *sec* and ending it at $t = 2.0$ *sec*. The red arrow in Figs. 2-6, running along the time axis, indicates the time interval during which the attack occurred in the corresponding plots below. The respective tests have been conducted prior to modeling and simulation experiments, specifically verification test of model operation under standard conditions, such as (i) acceleration and (ii) stabilization under open loop operation, followed by closed loop control tests, namely, (iii) step-function response and (iv) stabilization test (see [1] for details). Additionally, the test was conducted with attack engaging double step-function for distortion coefficient χ used in the bias injection. This was followed by test of linearly increasing χ as a bias. All these tests were producing the same results as in [1] and thus it does ensure compatibility of the condition to make comparisons.

Next, we shall see in the modeling and simulation experiment on how the change of the asymmetry of the tooth in saw-function of χ within the current drainage attack affects the flaw of the attack itself. To do so, we follow the sequence of experiments shown in Figs. 2 (a)-(c) while implementing the attack based on sequence shown in Fig. 2 (d). As Fig. 2 (d) suggests, the attack is preceded by stable, a "no-attack" state with χ = 1. Then the attack begins with χ dropping down to zero (χ = 0) and initiating saw-function tooths sequence oscillating above zero level of χ, which is representing the attack window marked with red arrow on the plots. As a starting point for demonstrating the effect of saw-function tooth asymmetry on attack induced current drainage, the fully asymmetric tooth shape with $K_S = 0$ will be considered (i.e., the right triangle tooth shape). Then, the tooth shape will be modified to increase the symmetry, rendering intermediate cases of $0 < K_S < 1$ in tooth asymmetry (i.e., various acute triangle shapes of the tooth in saw function representing partial asymmetry case will be scanned). Finally, isosceles triangle shape will be tested which provides best symmetry for saw tooth in time direction.

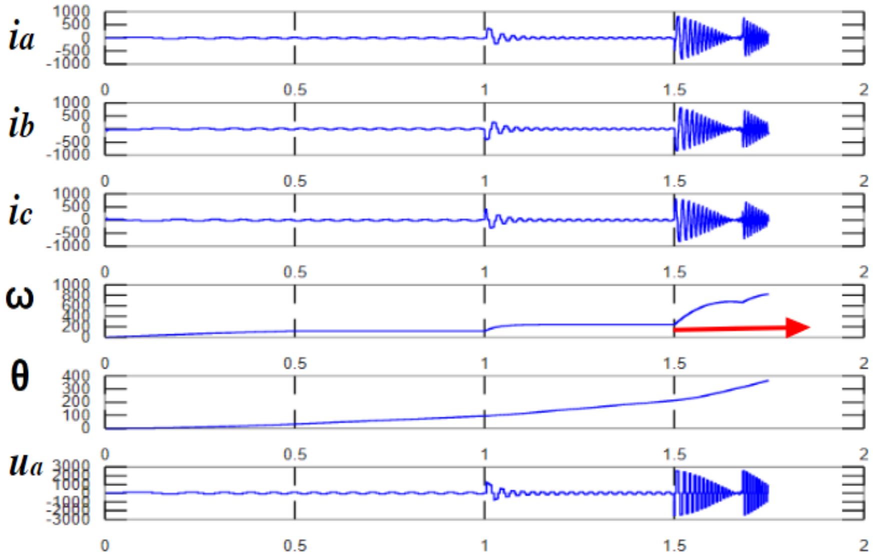

Fig. 3 Attack using saw function with fully asymmetric triangle as a tooth shape as bias distortion coefficient χ (*K_S = 0*, right triangle case with h = 0.1, i.e., 10% of the attack depth on a χ-scale); values of $\boldsymbol{i_a}$, $\boldsymbol{i_b}$, $\boldsymbol{i_c}$ are in Amps, ω are in rad/sec, θ are in radians, $\boldsymbol{u_a}$ are in Volts; horizontal axis is time in seconds

A. Injecting Fully Asymmetric Saw Bias

Fully asymmetric saw-function for χ in current drainage attack via bias injection was presented in prior publication [1]. Here we reproduce the one which begins the chain of trials with changing K_S. The case of $K_S = 0$ is shown in Fig. 3, where time slot *t = [0, 1.5] sec* is taken to the test-drive and after stabilization the attack begins at *t = 1.5 sec*. The attack follows the schedule shown in Fig. 2 (d) starting from χ = 1 (i.e., from no distortion) and dropping down to χ = 0 (i.e., maximum distortion with negative bias). Then the saw function of χ values sets in and oscillations above zero level of χ continue until the end of the attack (t_{end} *< 2 sec*), after which the value of returns back to χ = 1 level of no attack state. In Fig. 3 the periodic oscillation of the current has the same period as the saw function. Gradual linear decrease of the amplitude of current oscillations is linearly proportional to the respective increase of the saw tooth's cross-section height at the same time moment.

Next, we shall modify saw function by replacing right triangle tooth shape to the acute one.

B. Injecting Partially Asymmetric Saw Bias

When replacing the right triangle with acute one in saw function, the time of ascend to the triangle highest point was retained the same. It means that the period of oscillations for saw function with such acute triangles as tooth shapes was higher than that for the case of right triangles. This fact has implications in observed features of occurring system response.

By comparing periods of current modulation in the attack time window, it is seen that the modulation frequency of the current drainage is increasing for the acute triangle shape case. This goes even though the period of acute triangle saw function is higher than that of the right triangle. Explanation of this may be in emergence of the higher harmonics for the case of acute triangle.

The result of further increase of the symmetry and connected to that increase in modulation frequency of the current drainage is shown in Fig. 5. The symmetry of the acute triangle-shaped tooth is increased by 2.5 times compared to what is depicted in Fig. 4, resulting in a symmetry parameter measurement of K_S = 0.0005. Consequently, modulation frequency of the current drainage is increasing approximately 2.5 times as well, thus confirming inter-relation between saw tooth symmetry and current drainage modulation.

Having established the linear proportional relation between saw tooth symmetry and current drainage modulation frequency, it is logical to proceed to the case of strongest possible symmetry in the next Subsection *C*.

C. Injecting Fully Symmetric Saw Bias

The best symmetry for saw tooth in time direction is provided by the isosceles triangle shape, which has symmetry coefficient K_S = 1. Ascending time from the triangle left hand lowest point to its top in the middle becomes equal to the descending time from the top point to the right-hand side lowest point. Fig. 6 shows the result of engaging the isosceles triangle shape for the tooth in saw function for the attack.

It is seen that the smoothest change in current drainage is achieved for isosceles triangle shape of the tooth in saw function.

Next, we shall discuss implications of the observed dependencies.

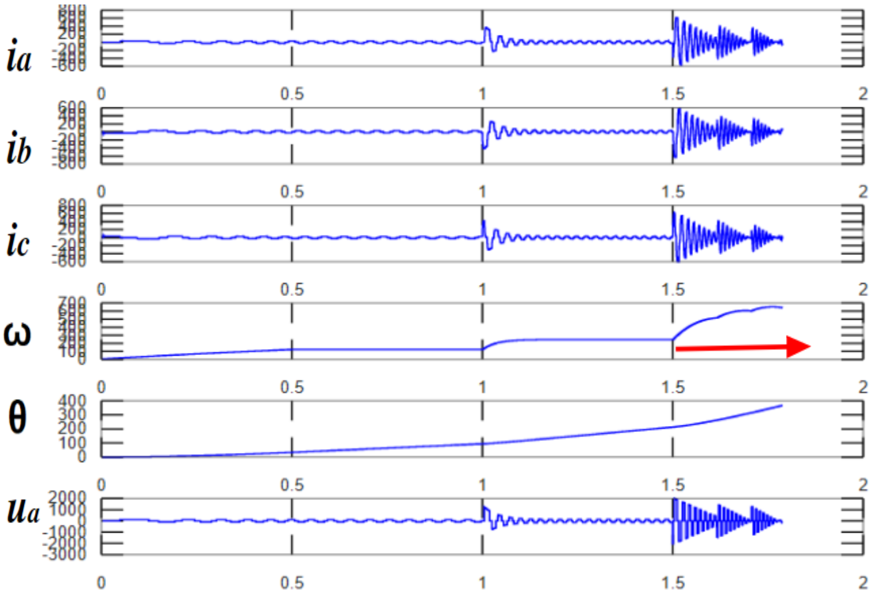

Fig. 4 Attack with acute triangle saw function as bias distortion coefficient with symmetry K_S = 0.0002 and saw depth h = 0.1; values of $\boldsymbol{i_a}$, $\boldsymbol{i_b}$, $\boldsymbol{i_c}$ are in Amps, ω are in rad/sec, θ are in radians, $\boldsymbol{u_a}$ are in Volts; horizonal axis is time in seconds

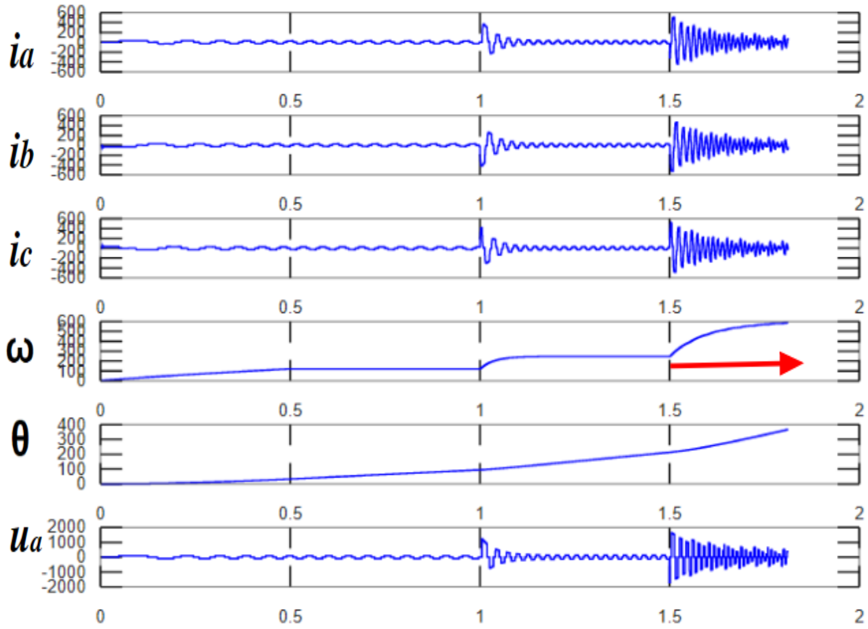

Fig. 5 Attack with acute triangle saw function as bias distortion coefficient with symmetry K_S = 0.0005 and saw depth h = 0.1; values of $\boldsymbol{i_a}$, $\boldsymbol{i_b}$, $\boldsymbol{i_c}$ are in Amps, ω are in rad/sec, θ are in radians, $\boldsymbol{u_a}$ are in Volts; horizonal axis is time in seconds

V. Discussion

The above simulations reveal a way in which current drainage attack may be affected via change of symmetry in the triangular tooth shape of a saw function – such a change modifies modulation of the occurring current flow. The current modulation amplitude and its frequency appears to be a function of the symmetry of the tooth shape employed. An extreme case of the fully asymmetric tooth shape of the right triangle brings about proportional modulation when the current drain repeats the shape of the attacking saw function in its amplitude and frequency. Modulation frequency harmonics occur on the current profile when symmetric features are introduced into saw function. Their frequency increases with the extent of symmetry until its reaching switching frequency of the windings. When a fully symmetric tooth shape is employed, the harmonics in the current drainage modulation profile disappear.

Detection of higher harmonics in the current drainage flow provides information on the attacking function parameters, such as symmetry of engaging triangular saw function. In turn, presence of harmonics in current drainage modulation offers distinguishing pattern of the attack, suitable for signature-based classification.

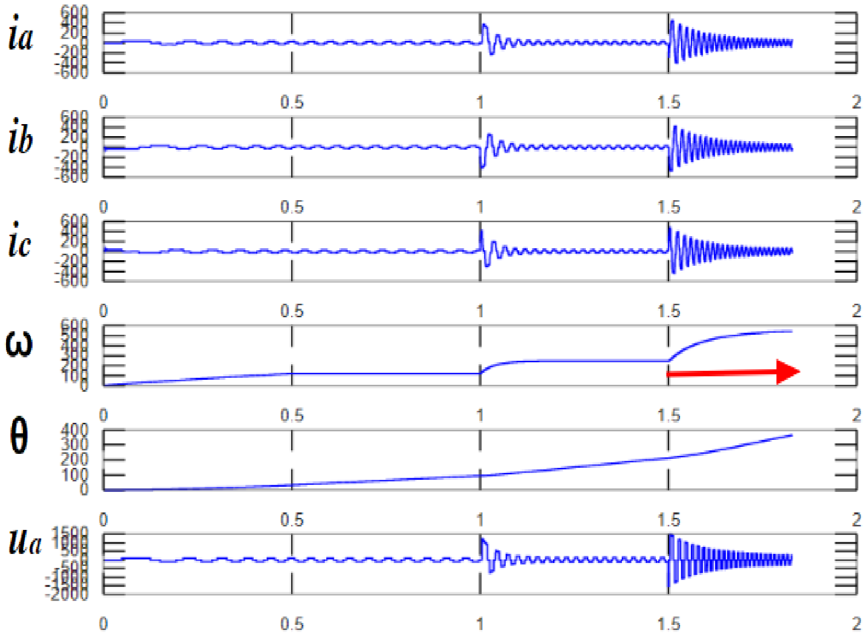

Fig. 6 Attack with the isosceles triangle saw function as bias distortion coefficient with symmetry $K_S = 1$ and a saw depth $h = 0.1$; values of $\boldsymbol{i_a}$, $\boldsymbol{i_b}$, $\boldsymbol{i_c}$ are in Amps, ω are in rad/sec, θ are in radians, $\boldsymbol{u_a}$ are in Volts; horizontal axis is time in seconds

Moreover, the stealthy approach for the attack gives preference to the symmetric type of the saw function employed where current drainage modulation profile stays harmonics free. Signature of the attack becomes less expressive for identification which help the attack to stay undetected.

VI. Conclusion

A set of features is identified and verified via modeling and simulation in the current drainage attack against closed loop-controlled BLDC motor. Specifically, an asymmetry of triangular tooth shape in the employed saw function is found to affect the modulation frequency of the drained current.

The proportional reproduction of the saw function oscillations in the current drainage takes place for fully asymmetric triangular shape of the tooth in the saw function.

Higher frequency harmonics occur in modulation signal of the drained current for partially asymmetric tooth shapes in saw function. The frequency of the harmonic's modulation of the current increases with the increase of symmetry of the triangular tooth shape involved.

Ultimately, for fully symmetric triangular tooth shape in the attacking saw function the higher harmonics vanish in the current modulation profile thus rendering smoother current drainage flow.

Signatures of the current drainage patterns for varying asymmetry in the tooth shape of saw function engaged are gathered with potential to identify the attack and its parameters via pattern recognition approach.

As a future development, the details of mathematical formulation of the attack description will be pursued.

Acknowledgment

Useful discussions with the professors at the University of Ottawa on the subject matter are gratefully acknowledged.

References

[1] Y. Boiko, I. Kiringa and T. Yeap, "Current drainage induced by bias injection attack against Kalman filter of BLDC motor," 2022 IEEE International Conference on Cyber Security and Resilience (CSR), 2022, pp. 364-369, doi: 10.1109/CSR54599.2022.9850310. https://ieeexplore.ieee.org/document/9850310

[2] Y. Boiko, C. Lin, I. Kiringa, and T. Yeap. "Performance of BLDC Motor under Kalman Filter Sensorless Drive," International Journal of Electrical and Information Engineering, vol.15, no. 7, pp.282-288, 2021. https://publications.waset.org/10012126/pdf

[3] A. W. Colombo, S. Karnouskos, O. Kaynak, Y. Shi and S. Yin, "Industrial cyberphysical systems: A backbone of the fourth industrial revolution", IEEE Ind. Electron. Mag., vol. 11, no. 1, pp. 6-16, Mar. 2017.

[4] A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee and S. K. S. Gupta, "Ensuring safety security and sustainability of mission-critical cyber-physical systems", Proc. IEEE, vol. 100, no. 1, pp. 283-299, Jan. 2012.

[5] M. Yampolskiy, P. Horvath, X. D. Koutsoukos, Y. Xue and J. Sztipanovits, "Taxonomy for description of cross-domain attacks on CPS", Proc. 2nd ACM Int. Conf. High Confidence Netw. Syst., pp. 135-142, 2013.

[6] S. Kriaa, L. Piètre-Cambacédès, M. Bouissou and Y. Halgand, "A survey of approaches combining safety and security for industrial control systems", Rel. Eng. Syst. Safety, vol. 139, pp. 156-178, 2015.

[7] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems", ACM Comput. Surveys, vol. 46, no. 4, pp. 55:1-55:29, Mar. 2014.

[8] A. A. Cárdenas et al., "Attacks against process control systems: Risk assessment detection and response", Proc. 6th ACM Symp. Inf. Comput. Commun. Security, pp. 355-366, 2011.

[9] J. Wang and G. Yang, "Data-Driven Methods for Stealthy Attacks on TCP/IP-Based Networked Control Systems Equipped with Attack Detectors," in IEEE Transactions on Cybernetics, vol. 49, no. 8, pp. 3020-3031, Aug. 2019, doi: 10.1109/TCYB.2018.2837874.

[10] M. Jablonski and D. Wijesekera, "Attacking Electric Motors for Fun and Profit",- BlackHat USA 2019, August 3-8, 2019, Las Vegas, NV, USA

[11] Y. Mo, E. Garone, A. Casavola and B. Sinopoli, "False data injection attacks against state estimation in wireless sensor networks," 49th IEEE Conference on Decision and Control (CDC), 2010, pp. 5967-5972, doi: 10.1109/CDC.2010.5718158.

[12] J. Lu and R. Niu, "False information injection attack on dynamic state estimation in multi-sensor systems," 17th International Conference on Information Fusion (FUSION), 2014, pp. 1-8. https://i.blackhat.com/USA-19/Wednesday/us-19-Jablonski-Attacking-Electric-Motors-For-Fun-And-Profit.pdf