Fault data injection attack on car-following model and mitigation based on interval type-2 fuzzy logic controller

Prabhakar Gunasekaran1,2, Selvaperumal Sundaramoorthy2, Nedumal Pugazhenthi Pulikesi2
1Department of Electrical & Electronics Engineering, VSB Engineering College, Karur, Tamilnadu, India
2Department of Electrical & Electronics Engineering, Syed Ammal Engineering College, Ramanathapuram, Tamilnadu, India
E-mail: prabhakar2488@gmail.com

Abstract: Cyber defence mechanism is started with modelling the accurate car-following behaviour including cyber attack. The creation of finest models made the path of control action easier. The connection between the vehicles is mathematically formulated with the help of car-following behaviour, incorporating the derived acceleration function from the cruise control physical system. The modified car-following model is simulated as closed-loop control system to analyse its behaviour in terms of acceleration and distance. Fault data injection cyber attack is mathematically injected into the modified car-following model and simulated to analyse the impact of attack. Initially, the impact of fault data injection attack is detected and mitigated with the help of parallel proportional–integral–derivative controller and genetic algorithm tuned proportional–integral–derivative controller. Interval type-2 fuzzy proportional–integral–derivative controller is introduced to mitigate the cyber attack and to overcome the uncertainty. The integral square error and integral absolute error are used to compare the performance of the controllers.

1 Introduction

Transportation is modernised due to tremendous levels of infrastructure development. Recently, most of the vehicle parts are becoming autonomous with the help of embedded processors to avoid collision and to make communication between the vehicles. A new technology called vehicle to vehicle communication is used nowadays. Hence, there is a need to manufacture the vehicles with network connectivity. These vehicles and robotic machines are generally termed as physical systems. Due to network connectivity, anyone can access these physical systems illegally. This is termed as cyber threats to physical systems. Hence, there is a need to control the vehicle behaviour and eliminate the cyber attack [1], which leads to the emergence of cyber physical systems (CPS) [2].

CPS is characterised as frameworks by incorporating control engineering, networking, embedded systems and mechatronics to operate. Monitoring, estimating and controlling the physical processes are usually executed as closed loop. Connectivity and communication between the systems lead to the design and development of network control systems (NCS). Serious security issues are raised due to this network control, which becomes the great challenge for many researchers. In the NCS, security issue plays a significant role in the defence of industrial machines and typical infrastructure. Numerous conventional designs in control engineering are assumed to be operated in a normal form, devoid of any attacks concerned. In this situation, delay or cyber attack on any part of system like sensors, controllers, actuators and so on, can degrade the response of the system and make the system unstable.

Denial of service (DoS) attacks were modelled and implemented by Amin et al. [3] in the communication channel, which are used to send the measuring data to the control station of power systems. According to the results based on accurately designed DoS attack sequences, power systems become unstable. The Supervisory Control and Data Acquisition (SCADA) systems were used in [4], to detect the fault data injection (FDI) attack. State estimation of FDI attacks in power systems was launched by Teixeira et al. [5]. In the Viking projects [6], load frequency control of power systems was attacked to analyse the effect of cyber attacks on the control station by using reachability methods. Mo et al. [7] performed the FDI attacks on a control structure provided through Kalman filter. In [8], the minimum set of adversary controlled meters was recognised to carry out an unobservable attack. Likewise, in the zone of biomedical gadgets [9], the matter of security of these gadgets are progressively basic in light of the fact that the advancement pattern of these gadgets will associate them to different elements via both wired and remote channels. It is along these lines critical to consider medicinal gadget security issues. In aviation industries, even a small cyber attack can damage the entire system and cause the human life in critical [10]. Liu et al. [11] performed the switched DoS attack on smart grid power systems to analyse its dynamic performances.

Regardless of the way that the security plans for control engineering were created in the previous quite a while, there are yet numerous recognised cyber attacks. Some current particular occasions additionally affirm that assaults would have occurred in control systems in various ventures [12]. The security and safety of NCS has been at the centre phase for young researchers, R&D engineers, and defence sectors as security threats could have caused potential catastrophic disasters [13]. Abbaspour et al. [14] presented a neural network (NN) fault detection design for identifying the unexpected faults in system parts. They utilised the modified Kalman filter to enhance the NN capability in the identification of faults. Abbaspour et al. [15] proposed the neural observer approach with improved accuracy for detecting FDI attack. In a time-constrained NCS, time delay switched (TDS) attack causes the major problem by injecting the delay into the dynamics of the control process to influence their behaviour. This also leads to destabilising the entire NCS. In the design of power systems, Sargolzaei et al. [16] modelled the TDS attacks to shatter the entire smart grids, but no control measures are taken into the account. These are the various cyber attacks in different fields mentioned in the literature. Among the three major attacks, FDI attack is designed and applied in this case.

The FDI attack injects fault random value into any parts of the system to influence the system behaviour. Also, by altering the environmental conditions of the system, faults can be induced. For example, at an appropriate frequency, Di-Battista et al. [17] injected a laser beam as a FDI attack to the system and Moradi et al. [18] also tried to inject the unknown data packets in the...
communication channel, which lead to the collision with genuine packets. The load redistribution FDI attack was implemented by altering the selected data in a SCADA power system by Yuan et al. [19]. This attack is extremely dangerous due to the manipulating of power flow estimation. Abbaspour et al. [14] introduced a novel scheme to detect FDI attack in unmanned aerial vehicle (UAV). An adaptive NN is implemented to perceive the injected faults in sensors of an UAV. An online tuning of NNs weights is done by using Kalman filter as an embedded program. Sargolzaei et al. [20] also performed the FDI assault on a networked pacemaker system and consume more time. PID gain values have tuned using a genetic algorithm (GA) is one of the first and best optimisation algorithms in the family of evolutionary algorithms [24]. In this paper, enhancement of PID control strategy is also done by automating the tuning process with a GA. The advancement recently happened in the interval type-2 fuzzy logic system (IT2-FLS) is uncertainties. It may possibly include into the fuzzy sets directly and type reducer [25] is also introduced. To detect uncertainties available in the response of a system due to different sources of model input factors [26], sensitivity analysis is needed. Variance-based methods [27] are well suited to this task and have asserted themselves among practitioners [28–30].

The paper is organised as follows. The derivation of car-following model from state-space acceleration of the non-linear car process inputs based on the past signal and the rate of change of error signal that provides accurate control and stability [21]. Aidan O’ Dywer [22] gathered many PID tuning rules such as Zeigler-Nichols, Astrom and Hagglund, Cohen-Coon tuning and so on that are model-based rules. These tunings are manual, difficult in using and consume more time. PID gain values have tuned using optimisation techniques to surmount these limitations. The task of optimisation is to look for the best input variables by the well-known model and output variables [23]. The intelligent driver model (IDM) [34, 35] is an appropriate representation which satisfies the traffic requirements. The derived state-space acceleration of the non-linear car model from [36] is

$$w(t) = \alpha w^2(t)$$  (1)

Equation (1) is initially rearranged to obtain the velocity of leader car \(w_l\) and the velocity of follower car \(w_f\) to form the car-following model shown in Fig. 1. They are represented as

$$w_l(t) = \left(\frac{aw(t) - w_l(t)}{\alpha}\right)^{1/2}$$  (2)

$$w_f(t) = \left(\frac{aw(t) - w_f(t)}{\alpha}\right)^{1/2}$$  (3)

Considering the IDM as a benchmark car-following model and applying the velocity equations (2) and (3), the acceleration of a driver as a continuous function of the vehicle's velocity, distance between the vehicles and relative speed corresponding to the leader vehicle are derived. The formation of acceleration model is

$$\Delta \alpha(t) = A_{\text{max}} \left(1 - \frac{w_f(t)}{V_{\text{max}}}ight) (4)$$

$$\Delta v(t) = l_1 + \max \left[H w_f(t) + \left(\frac{w_f(t) - w_f(t)}{\Delta \alpha(t) - L_t}\right)^2 \frac{2 \sqrt{2 A_{\text{max}} b_f}}{b_f}\right] \geq 0$$  (5)

$$\Delta \alpha(t) = v_{l1}(t) - v_{l2}(t)$$  (6)

where \(V_1\) is the velocity of the leader vehicle; \(V_2\) is the velocity of the follower vehicle; \(\alpha_{max}(t)\) is the acceleration of the follower vehicle; \(A_{max}\) is the maximum acceleration; \(V_{max}\) is the maximum velocity; \(L_t\) is the length of the leader car; \(l_0\) is the inter-vehicle spacing at stop; \(H\) is the minimum time headway; \(b_f\) is the follower's deceleration; \(\Delta v(t)\) is the desired distance from the leader; \(\Delta \alpha(t)\) is the space between the leader's front bumper and the follower's front bumper at a time step. The closed-loop model of car-following behaviour is simulated using input profile by applying the system parameters listed in Table 1, which is shown in Fig. 2.

The input profile is the combination of step inputs obtained from the Simulink library to model the acceleration of the leader car. The car-following model subsystem is shown in Fig. 3. The acceleration response and the distance gap obtained from the

Table 1  Model specifications

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>(A_{\text{max}})</td>
<td>6 m/s²</td>
</tr>
<tr>
<td>(a)</td>
<td>4</td>
</tr>
<tr>
<td>(V_{\text{max}})</td>
<td>36 m/s</td>
</tr>
<tr>
<td>(l_1)</td>
<td>6 m</td>
</tr>
<tr>
<td>(l_0)</td>
<td>2 m</td>
</tr>
<tr>
<td>(H)</td>
<td>6 s</td>
</tr>
<tr>
<td>(b_f)</td>
<td>6 m/s²</td>
</tr>
</tbody>
</table>

Fig. 1  Car-following model

2 Car-following model

An unexpected alteration in the maximum acceleration or deceleration while driving the vehicle in a smooth manner on the road lane may cause serious collisions, since the follower human driver cannot judge a sudden change through his own senses. However, an autonomous driving system can detect sudden changes in acceleration by controlling the brake valve and throttle valve. The real-time car-following behaviour can be modelled by considering the maximum deceleration in the adaptive cruise control (ACC) system or autonomous cars [31–33], and autonomous driving is still in research. In the current trend, there is a gradual increase in the technology of ACC system. The speed of the vehicle is controlled based on the distance and the relative velocity between the follower and the leader vehicle. In this system, the driver can set the following gap manually and this gap acts a constant input value for processing, since, the ACC framework neglects to process a more sensible desired gap as per the real-time street surface conditions. To ensure computational productivity and to control the vehicle efficiently, a simple design of the ACC model must be used with a few numbers of parameters. The intelligent driver model (IDM) [34, 35] is an appropriate representation which satisfies the traffic requirements. The derived state-space acceleration of the non-linear car model from [36] is
closed-loop car-following model is shown in Figs. 4 and 5, respectively.

3 Sensitivity analysis

Variance-based sensitivity analysis was carried out in car-following model [37] to produce an effective exploration of the inputs’ domain. Considering the model in the form

\[ Z = f(k_1, k_2, \ldots, k_r) \] (7)

being \( k_i (i=1, \ldots, p) \) the model’s input and \( Z \) its output. A Monte Carlo experiment is performed with our model. This first implies sampling \( N \) combinations of the \( r \) inputs from their probability distributions in order to achieve the following matrix:

\[
M = \begin{bmatrix}
k^{(1)}_1 & k^{(2)}_1 & \cdots & k^{(N)}_1 \\
k^{(1)}_2 & k^{(2)}_2 & \cdots & k^{(N)}_2 \\
\vdots & \vdots & \ddots & \vdots \\
k^{(1)}_r & k^{(2)}_r & \cdots & k^{(N)}_r 
\end{bmatrix}
\] (8)

Then, the vector of model outputs \( z \) is obtained by evaluating the model on each combination of the \( p \) inputs, namely on each row of the matrix \( M \)

\[ z = \begin{bmatrix} z^{(1)} \\ \vdots \\ z^{(N)} \end{bmatrix} \] (9)

The first-order sensitivity index is a very important measure to understand how much the correct definition of an input may reduce the overall uncertainty in the results. It is possible to define a model as additive if

\[ \sum_{i=1}^{p} S_i = 1 \] (10)

In this case, indeed, the unconditional variance of the model can be decomposed in the sum of the first-order effect of each single variable. In this case, a low first-order sensitivity index does not necessarily imply that the corresponding variable has a scarce effect on the output variance, since it might contribute to it by means of its interactions with the other variables. To consider the effect of the interactions, a synthetic indicator to be coupled with the first-order sensitivity index is the total effects index, defined as follows [28]:

\[ S_T = 1 - \frac{V_z - \sum_i E_i(z|k_{-i})}{V_z} \] (11)

Total effects index of the input factor \( i \) provides the sum of all the interaction effects involving the \( i \)th factor. When the total index is \( S_T = 0 \), the \( i \)th factor can be fixed without affecting the outputs’ variance. The methodology adopted here is described as: (i) sampling two \((N, p)\) matrices of quasi-random numbers in the range between 0 and 1 and then the values of two matrices \( A \) and \( B \) are generated using the distributions of the \( p \) input factors; (ii) a set of \( p \) matrices, \( C \), is obtained by assembling \( p \) matrices equal to \( A \),
except for the $i$th column, which is taken from $B$; (iii) this model is evaluated for all the $[N(p + 2)]$ combinations of input variables

$$A = \begin{bmatrix} k_{p+1}^{(0)} & k_{p+1}^{(1)} & \cdots & k_{p+1}^{(p)} \\ k_{p+2}^{(0)} & k_{p+2}^{(1)} & \cdots & k_{p+2}^{(p)} \\ \vdots & \vdots & \ddots & \vdots \\ k_{p+n}^{(0)} & k_{p+n}^{(1)} & \cdots & k_{p+n}^{(p)} \end{bmatrix}$$ \hspace{1cm} (12)

$$B = \begin{bmatrix} k_{p+1}^{(0)} & k_{p+1}^{(1)} & \cdots & k_{p+1}^{(p)} \\ k_{p+2}^{(0)} & k_{p+2}^{(1)} & \cdots & k_{p+2}^{(p)} \\ \vdots & \vdots & \ddots & \vdots \\ k_{p+n}^{(0)} & k_{p+n}^{(1)} & \cdots & k_{p+n}^{(p)} \end{bmatrix}$$ \hspace{1cm} (13)

$$C_i = \begin{bmatrix} k_{p+1}^{(0)} & k_{p+1}^{(1)} & \cdots & k_{p+1}^{(p)} \\ k_{p+2}^{(0)} & k_{p+2}^{(1)} & \cdots & k_{p+2}^{(p)} \\ \vdots & \vdots & \ddots & \vdots \\ k_{p+n}^{(0)} & k_{p+n}^{(1)} & \cdots & k_{p+n}^{(p)} \end{bmatrix}$$ \hspace{1cm} (14)

for $i = 1 \ldots p$.

Global sensitivity analysis of FDI attacked car-following model is implemented in Simulink using variance-based sensitivity method with combinations of parameters generated by Monte Carlo method with a uniform probability distribution function. Uncertainty analysis of a Simulink model is done by generation of $N$ sets of parameters and $N$ simulations using the Monte Carlo method, which is shown in Fig. 6. In this case, double loop Monte Carlo method and Saltelli's single loop method are considered. The first-order Sobol index and total effect Sobol index are computed through using (12) and (13) based on the FDI attacked car-following model evaluations $y_A = f(A)$, $y_B = f(B)$ and $y_C = f(C)$ for both double loop Monte Carlo Simulation (MCS) method and single loop Saltelli simulation method. The double loop method leads to an emergence of transformation from $N \times D$ input matrix to $N \times 1$ outputs, where $N$ denotes the number of samples and $D$ denotes the dimension of input. The advantages of a double loop MCS method are high accuracy and easy programming. The computational cost function for double loop is $n^2D + n$. Then to reduce the computational cost, a single loop method ($2n + nk$) is used.

The fixed inputs are the length of the leader car ($L$), speed of the follower, leader trajectory and the initial position. In this way, they are assumed as certain, and thus they are not left to vary. The variable inputs are maximum acceleration ($A_{\text{max}}$), maximum velocity ($V_{\text{max}}$), inter-vehicle spacing at stop ($L_s$), minimum time headway ($H$), follower's deceleration ($b_f$) and a fixed model parameter ($\alpha$). These variable inputs are assumed as uncertain. Table 2 represents the input factor ranges for car-following model. First-order and total sensitivity indices for the FDI attacked car-following model based on speed is shown in Fig. 7. The minimum time headway and acceleration are the two input parameters that influence the response of car-following model in a drastic manner. The other parameters do not show much influence on the response based on this global sensitivity analysis method.

### Table 2 Input factor ranges for car-following model

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A_{\text{max}}$</td>
<td>0.2</td>
</tr>
<tr>
<td>$V_{\text{max}}$</td>
<td>6</td>
</tr>
<tr>
<td>$L_s$</td>
<td>0.5</td>
</tr>
<tr>
<td>$H$</td>
<td>1</td>
</tr>
<tr>
<td>$b_f$</td>
<td>0.4</td>
</tr>
<tr>
<td>$\alpha$</td>
<td>1</td>
</tr>
</tbody>
</table>

### 4 Attack modelling

Initially, the acceleration or the non-linear state-space model of the follower vehicle is considered and later, the fault velocity function $\tilde{w}_f(t)$ is added to the acceleration function by replacing the normal velocity function $w_f(t)$. The acceleration function of the follower vehicle with fault velocity injected attack is derived as

$$\tilde{w}_f(t) = a u(t) - a \tilde{\omega}_f(t)$$ \hspace{1cm} (15)
where
\[ \tilde{w}(t) = \begin{cases} \frac{w(t)}{D_a w(t) + F_a} & \text{otherwise} \\ \alpha u(t) - \dot{w}(t) & \end{cases} \quad (16) \]

The attack model is framed using DoS attack and FDI attack with conditions like \( D_a \) and \( F_a \) are zero for DoS attack, and \( D_a = 1 \) and \( F_a \) as any set of random values for FDI attack. Equation (16) is rearranged as
\[ \tilde{w}(t) = \left( \frac{\alpha u(t) - \dot{w}(t)}{\alpha} \right)^{1/2} \quad (17) \]

The follower velocity with FDI attack \( \tilde{w}(t) \) in (17) is applied to the acceleration model of (4) and (5). Then it is derived as a follower acceleration model with FDI attack
\[ \dot{w}(t)_{\text{attack}} = A_{\text{max}} \left[ 1 - \left( \frac{\tilde{w}(t)^*}{V_{\text{max}}} \right)^2 - \left( \frac{\Delta s(t)_{\text{attack}}}{\Delta s(t)_{\text{attack}} - L_t} \right)^2 \right] \quad (18) \]
where
\[ \Delta s(t)_{\text{attack}} = L_t + \max \left[ \left( \frac{H^* \tilde{w}(t) + \left[ \frac{\tilde{w}(t)^* \left( \tilde{w}(t) - w(t) \right)}{2 \sqrt{A_{\text{max}}^* b_t}} \right]}{0} \right] \quad (19) \]

The Simulink model of FDI attack on the car-following model is shown in Fig. 8. The acceleration response of the car-following model during an FDI cyber attack is shown in Fig. 9, which resembles the failure of the follower vehicle to match the acceleration of the leader vehicle.

5 Attack mitigation

5.1 PID controller

The parallel PID structure with filter derivative is used to control the car-following model to attain the desired response and it is expressed as
\[ G_c(s) = P + I + \frac{D_{\text{max}}}{1 + N (1/\tau)} \quad (20) \]
where \( P, I, D \) and \( N \) are proportional gain, integral gain, derivative gain and filter coefficient, respectively. The gain values are tuned by built-in interactive PID tuning algorithm in Simulink. This tuning algorithm selects a crossover frequency based on the system dynamics and design for a target phase margin. Interactive changes in the response time, transient response, bandwidth, or phase margin in the PID tuner interface provide new PID gains until it achieves the best balance between performance and robustness. The Simulink model of PID controlled car-following behaviour with FDI attack is shown in Fig. 10. Distance gap and acceleration response of the PID controlled car-following behaviour with FDI attack are shown in Figs. 11 and 12, respectively.
5.2 GA tuned PID

The manual PID tuning method adds delay to the system to obtain the desired response. Alternately, GA is a seek algorithm, which is based on genetics principles and natural selection. A better result is evolved after several numbers of iterations that also checks for the error occurrence. The fittest roots are considered for the later generation based on the selection criterion. By calculation of selection, mutation and crossover, GA generates the initial population of the PID control parameters randomly, thus optimising the control parameters. Genetic simulation programming is a probabilistic one that searches the different compositions of available functions and terminals under the track of a fitness measure. Larger the number of chromosomes, there is a better chance to get the optimal results. The overall fitness functions are mean square error, integral absolute error (IAE), integral square error (ISE) and integral time and absolute error. In that, IAE is used to implement the GA for determining the PID controller parameters to compensate the delay in this system. The objective function is based on IAE (IAE integrates the absolute error over time) defined as

\[
\text{Objective function} = \int_{0}^{\infty} |e(t)| \, dt \tag{21}
\]

In IAE fitness function, no weight added to any of the errors obtained from the response of the system. It tends to produce a slower response compared to ISE optimal plants, but generally shows less sustained oscillation. Acceleration response and distance gap of the GA-PID controlled car-following behaviour with FDI attack are shown in Figs. 13 and 14, respectively. The GA programming parameters are listed in Table 3.

5.3 Interval type-2 fuzzy PID controller on FDI attack

In fuzzy logic systems, uncertainty lies in framing the rules based on the human knowledge. The three ways of uncertainty are: (i) the usage of words in consequents and antecedents of rules denotes the different meaning for different things and differently understand by different persons; (ii) consequents acquired by surveying a gathering of specialists will regularly be distinctive for the identical rule on the grounds that the specialists would not really be in understanding; and (iii) noisy training data.
Table 3 | GA parameters
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value/method</th>
</tr>
</thead>
<tbody>
<tr>
<td>population size</td>
<td>100</td>
</tr>
<tr>
<td>variable bounds</td>
<td>$[-50,600; -50,500; -50,200]$</td>
</tr>
<tr>
<td>maximum number of generations</td>
<td>220</td>
</tr>
<tr>
<td>fitness function</td>
<td>IAE</td>
</tr>
<tr>
<td>selection method</td>
<td>normalised geometric selection</td>
</tr>
<tr>
<td>crossover method</td>
<td>arithmetic crossover</td>
</tr>
<tr>
<td>mutation method</td>
<td>uniform mutation</td>
</tr>
</tbody>
</table>

The uncertain antecedent or consequent membership functions are obtained by translating the antecedent or consequent uncertainties. The membership functions of type-1 FLSs are type-1 fuzzy sets, which failed to handle the uncertainties present in the rules. The antecedent or consequent membership functions of type-2 FLSs are type-2 fuzzy sets. It can handle the uncertainties available in the rules. The grades of membership in type-2 fuzzy sets seem to be fuzzy. In type-2 membership, grades can be in the subset of $[0, 1]$ represents the primary membership. There is a presence of secondary membership that can also be in the subset of $[0, 1]$ equivalent to each primary membership. Type-2 fuzzy sets tolerate us to deal linguistic uncertainties, as the saying 'usage of words in the rules denotes the different meaning for different things and differently understand by different persons'.

A fuzzy connection of higher kind type-2 has been viewed as one approach to expand the fuzziness of a connection and, as per Hisdal [38], 'enhanced fuzziness in a depiction implies expanded capacity to deal with inaccurate data in a consistently rectify way. This type-2 fuzzy logic system consists of a fuzzy inference engine, fuzzifier, rule base and the output processor as per the type-1 FLS. The output processor contains type-reducer, which produces a type-1 fuzzy set response and defuzzifier to produce a crisp number. A type-2 FLS is once more described by IF–THEN rules. The antecedent or consequent membership functions of type-2 fuzzy sets include into the fuzzy sets directly and also type membership functions either zero or one. Therefore, it is called as the primary membership of type-1 fuzzy system known as the secondary set. The uncertainty in the third dimension of type-2 fuzzy sets was constrained to the interval type-2 fuzzy logic systems (IT2-FLS) [39, 40].

5.3.3 Interval type-2 fuzzy logic systems: In an interval type-2 fuzzy set, the membership position of every field point is a crisp set whose field has interval limited to $[0, 1]$. For modelling the IT2-FLS and to minimise the impact of uncertainties in rule base [41], the third dimension of type-2 fuzzy sets was constrained to the values of either zero or one.

5.3.3.1 Takagi Sugeno Kang (TSK) model: TSK model consists of fuzzy rules used for modelling and control of complex and high-dimensional systems. Fuzzy rules are something like IF this is happened THEN that to do. It is characterised by functional type consequents instead of fuzzy consequents. Using small number of rules, it can describe highly non-linear system. TSK model has more flexible representation capability than Mamdani fuzzy model.

TSK fuzzy rules are specified as

$$R_i: \text{if } y_1 \text{ is } l_1 \text{ and } y_2 \text{ is } l_2 \text{ and } y_3 \text{ is } l_3$$

Then

$$f_i(y_1, y_2, \ldots, y_3), \quad \text{where } i = 1, 2 \ldots n$$

or

$$R_i: \text{if } y_1 = l_1 \text{ Then } f_i(y_1), \quad i = 1, 2 \ldots n$$

where

$$f_1, f_2, \ldots, f_n$$

are functions

$$y_1, y_2, \ldots, y_n$$

are input variables,

$$l_1, l_2, \ldots, l_m$$

are reference fuzzy sets over input spaces

$$\mu_{y_1}, \mu_{y_2}, \ldots, \mu_{y_n}$$

The rules are combined to get a function

$$R(y) = \frac{\int f(y, u) \mu_{y_1}(y, u) \mu_{y_2}(y, u) \ldots \mu_{y_n}(y, u) \, du}{\int \mu_{y_1}(y, u) \mu_{y_2}(y, u) \ldots \mu_{y_n}(y, u) \, du}$$    \hspace{1cm} (22)$$

5.3.3.2 Interval type-2 fuzzy logic systems: In an interval type-2 fuzzy set, the membership position of every field point is a crisp set whose field has interval limited to $[0, 1]$. For modelling the IT2-FLS and to minimise the impact of uncertainties in rule base [41], the third dimension of type-2 fuzzy sets was constrained to the values of either zero or one.

An interval type-2 fuzzy set $(\tilde{y})$ is defined with a type-2 membership function $\mu_2(y, u)$ as follows:

$$\tilde{y} = \int_{y \in Y} \int_{u \in I_y} \frac{\mu_2(y, u)}{(y, u)} \, du \, dy$$    \hspace{1cm} (23)$$

where $\int \int$ signifies the union over all acceptable $u$ and $y$, $J_y$ is referred to as the primary membership of $y$, while $\mu_2(y, u)$ is a type-1 fuzzy system known as the secondary set. The uncertainty in the primary membership of a type-2 fuzzy set $\tilde{y}$ is defined by a section named path of uncertainty (POU). The POU can be depicted as far as an upper membership function $\mu_U$ and a lower membership function $\mu_L$. If the primary membership $J_y$ is an interval set of IT2-FLS is constructed, i.e. $\mu_2(y, u) = 1$ for $\forall u \in J_y$ is a subset of $[0, 1]$. IT2-FLS has the extra type-reduction process. The block diagram of the IT2-FLS structure is given in Fig. 15. Interval type-2 fuzzy logic contains a fuzzy rule base, fuzzifier, fuzzy inference engine and output processing, where output processing includes type reducer and defuzzifier.

5.3.3.3 IT2-FLS toolbox: In the IT2-FLS toolbox [42], intuitive operation is implemented using TSK type. It is proficient to face all the stages of control design. The construction of IT2-FLS toolbox has designed from the commercial fuzzy logic toolbox available in the MATLAB by introducing latest functions for TR process. This toolbox has a Guided User Interface, separate Simulink library and a connection to the Simulink. The structure of IT2-FLS toolbox has a file extension of ‘*.it2fis’. It creates a memory space in the MATLAB workspace. This toolbox contains information about the membership functions, rules, types and TR methods. When the user designs the fuzzy rules based on their knowledge in the IT2-FLS toolbox, the fuzzy structure is refreshed naturally. This

This is an open access article published by the IET under the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0/).
toolbox comprises of four primary user interfaces such as main editor, membership function editor, rule editor and surface viewer. The created guided user interface is related to the MATLAB commercial type-1 fuzzy logic toolbox.

5.3.4 Design of fuzzy controller: In TSK model based fuzzy PID controller, knowledge-based rule matrix is formed using five membership functions such as NB (negative big), NS (negative small), Z (zero), PS (positive small) and PB (positive big) as input members. The output membership functions are VN (very near), N (near), CE (close enough), F (far) and VF (very far).

These membership functions are type-2 trapezoidal in shape to handle uncertainties in the cyber attack on car-following behaviour. The range of error input is from −53.03 to 28.97, derivative of error is from −11.57 to 26.22 and the range of controller output is from −0.48 to 3.38. The $K_e$, $K_d$ and $K_a$, $K_b$ are the input and output scaling factors, respectively. The IT2-FLS controller is raised with $N = 25$ rules are provided in Table 4. The method for TR and defuzzification used here is enhanced Karnik Mendel algorithm. The scaling components of interval type-2 fuzzy PID are set as $K_e = 63$, $K_d = 1.5$, $K_a = 0.3$ and $K_b = 106$ to demonstrate the impact of the type reducer strategy on the controller execution. The Simulink model of IT2-FLS PID controlled car-following behaviour with FDI attack is shown in Fig. 16. The structure of interval type-2 fuzzy PID is shown in Fig. 17. Figs. 18 and 19 have shown the type-2 trapezoidal membership functions of error input and change in error input, respectively. The rule matrix of the fuzzy inference engine is shown in Table 4.

Distance gap and acceleration response of the IT2-FLS PID controlled car-following behaviour with FDI attack are shown in Figs. 20 and 21, respectively. The integral error analysis on FDI attack based on PID, GA-PID and IT2-FLS PID controller is listed in Table 5.

6 Real-time implementation

Consider the scenario of involving robotic vehicles named as leader vehicle, follower vehicle and an attacker, a device to inject fault data into the follower vehicle. The leader vehicle consists of NodeMCU controller, sensors and actuators. It transmits its own speed to the follower vehicle through Wi-Fi networks. The
follower vehicle also consists of NodeMCU controller, sensors and actuators, which receives the transmitted speed from the leader vehicle. This speed acts as a set point for the follower vehicle to accelerate or decelerate its own speed.

The attacker also consists of NodeMCU controller connected with laptop, which also accesses the open Wi-Fi network to inject the random fault speed values into the follower vehicle. These random fault values make the follower vehicle to mislead from the leader pathway. The cyber defence mechanism is embedded in the processor of follower vehicle to mitigate this FDI attack. The concept for real-time implementation of leader-follower setup and cyber defence mechanism is clearly shown in Fig. 22.

The cyber defence mechanism is designed and simulated with the help of an integrated car-following model including the cyber attack. Initially, PID controller is used to mitigate the cyber attack. For further enhancement, interval type-2 fuzzy PID controller is designed to mitigate the cyber attack. This cyber defence mechanism is utilised by the follower vehicle to regulate its own speed for maintaining the safe distance from the leader vehicle. The prototype model of the leader follower setup is shown in Fig. 23, involves two cars like robots. Each robot consists of two DC encoder motors with wheels (12v Planetary DC Geared Motor 1140 RPM), one Castor wheel, NodeMCU Processor (Built-in Wi-Fi), UV Obstacle Sensor and L293d motor driver circuit. The disc attached with encoder generates a pulse signal depending on the rotation of the shaft.

![Fig. 19 Input 2 – change in error](image1)

**Table 4** Fuzzy rule matrix

<table>
<thead>
<tr>
<th>e&lt;sub&gt;0&lt;/sub&gt;de</th>
<th>NBig</th>
<th>NSmall</th>
<th>Zero</th>
<th>PSmall</th>
<th>PBig</th>
</tr>
</thead>
<tbody>
<tr>
<td>NBig</td>
<td>VN</td>
<td>VN</td>
<td>N</td>
<td>N</td>
<td>CE</td>
</tr>
<tr>
<td>NSmall</td>
<td>VN</td>
<td>N</td>
<td>N</td>
<td>CE</td>
<td>F</td>
</tr>
<tr>
<td>Zero</td>
<td>N</td>
<td>N</td>
<td>CE</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>PSmall</td>
<td>N</td>
<td>CE</td>
<td>F</td>
<td>F</td>
<td>VF</td>
</tr>
<tr>
<td>PBig</td>
<td>CE</td>
<td>F</td>
<td>F</td>
<td>VF</td>
<td>VF</td>
</tr>
</tbody>
</table>

![Fig. 20 Distance gap from the leader (interval type-2 fuzzy PID on attack)](image2)

**Table 5** Integral error analysis on FDI attack

<table>
<thead>
<tr>
<th>Metrics</th>
<th>PID</th>
<th>GA tuned PID</th>
<th>IT2-FLS PID</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISE</td>
<td>15,370</td>
<td>6473</td>
<td>3377</td>
</tr>
<tr>
<td>IAE</td>
<td>2372</td>
<td>1123</td>
<td>536</td>
</tr>
</tbody>
</table>

![Fig. 21 Acceleration response of interval type-2 fuzzy PID on FDI attack](image3)

![Fig. 22 Concept block for hardware setup](image4)

![Fig. 23 Hardware setup](image5)
These pulses are read by micro-controller, and the motor voltage is controlled by the pulse width modulation pulses that are regulated with the help of control algorithm embedded in the micro-controller chip to match the set point RPM. The real-time output has obtained from the Serial chart software module installed on windows 7 OS in DELL laptop, which connected to the NodeMCU board through a serial communication port at the baud rate of 115,200. The real-time output of PID control on FDI attack and interval-type 2 fuzzy PID control on FDI attack is shown in Fig. 24.

7 Conclusion

Among the three major attacks (DoS, FDI and TDS), FDI attack is implemented in the non-linear physical system and hence, the car-following behaviour with FDI cyber attack is modelled and simulated to analyse the behaviour. Sensitivity analysis is performed to analyse the impact of input parameters of the car-following model. For further improvement in control, PID, GA-PID and interval-type 2 fuzzy PID controller is used to mitigate the cyber attack. Based on the integral error analysis ISE and IAE, interval-type 2 fuzzy PID controller is found to perform better than PID and GA-PID controller in the mitigation of cyber attack. This modelling and control feature enhances the cyber defence mechanism and makes the non-linear physical system to be robust against cyber attacks. Real-time operating system based hardware implementation has been carried out using leader and follower robots including attacker device to realise the simulation results in real time. This cybersecurity feature enriches the safety features of the non-linear physical systems. This research investigation paves the way for the researchers, design engineers to understand the nature and practical implementation of non-linear physical systems with cybersecurity that led to the growth of CPS.

8 References


Fig. 24 Real-time control output on FDI attack

These pulses are read by micro-controller, and the motor voltage is controlled by the pulse width modulation pulses that are regulated with the help of control algorithm embedded in the micro-controller chip to match the set point RPM. The real-time output has obtained from the Serial chart software module installed on windows 7 OS in DELL laptop, which connected to the NodeMCU board through a serial communication port at the baud rate of 115,200. The real-time output of PID control on FDI attack and interval-type 2 fuzzy PID control on FDI attack is shown in Fig. 24.


