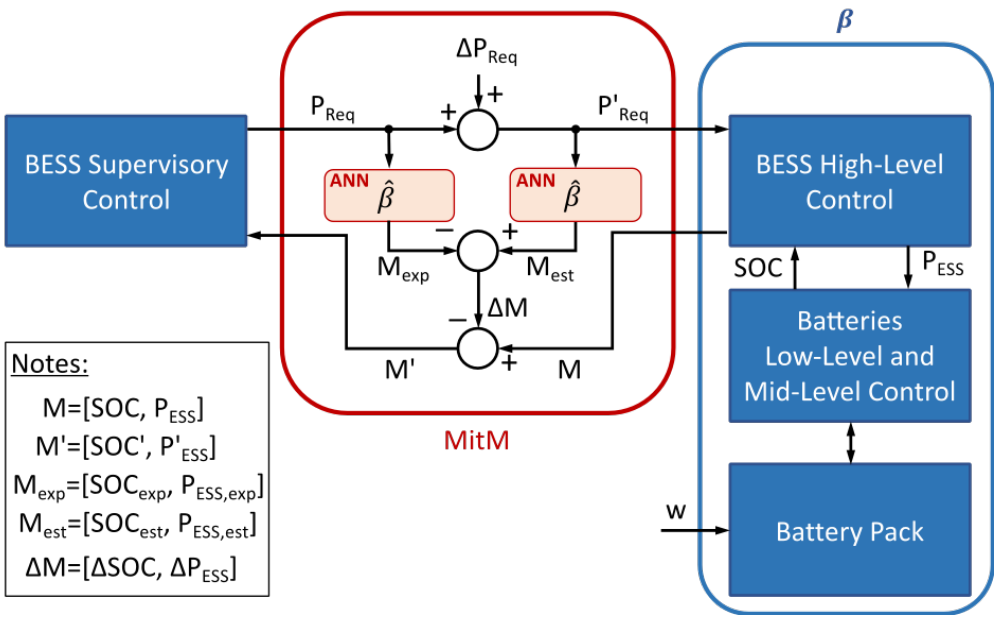

A.Machine Learning of the System

Recent works [2]–[4] present System Identification attacks intended to learn the models of plants and control functions, in order to support the design of stealth and model-based attacks. In these works, the devices to be identified are Linear Time-Invariant (LTI) systems, which are components of a single feedback control loop typically located in the lower level of a SCADA system. These attacks, by design, are limited to estimate the coefficients of LTI transfer functions, which make them not suitable to identify the model of nonlinear and more complex systems, such as the BESS. In order to overcome this constraint of the System Identification attacks reported in the literature, this work proposes the ANN-based System Identification attack herein described, which is executed in stage S-2 of the attack sequence. The proposed approach provides more flexibility to aggregate in a single model a complex system containing a physical plant (the BESS battery pack), and different control levels (BESS high, medium and low control levels) with unknown control rules/algorithms in a single model.

To model the system described in Fig. 2 and predict SOC and P_{ESS} signals in face of a given P_{Req} , two different ANNs were designed: one to estimate the P_{ESS} signal; and another to estimate the batteries SOC signal. Each one ANN was trained separately using the signals captured during stage S-1 of the attack.

The first ANN-model (ANN-1) was created and trained to mimic the behavior of "BESS High-Level Control" block shown in Fig. 2. During the training stage, the network was configured in open loop (i.e. without feeding back the estimated $P_{ESS,est}$ signal) as shown in Figure 3. The inputs of ANN-1 are the sniffed values of P_{Req}, P_{ESS} and SOC obtained of the actual system during its normal operation and the output is $P_{ESS,est}$. The prediction error between the actual plant output $P_{ESS}(k)$ and the neural network output $P_{ESS,est}(k)$ was used as the neural network training signal. The mapping function of the ANN-1 is defined according to (xxx).

$$P_{ESS,est}(k) = \alpha_1(P_{Req}(k), P_{ESS}(k-1), SOC(k-1)) \quad \text{(xxx)}$$

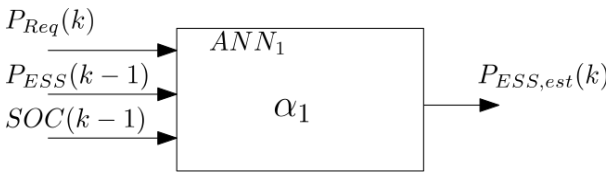

Fig. 3 Neural Network for predicting P_{ESS}

The ANN-2 was designed to predict the SOC by modeling the "Batteries Low-Level and Mid-Level Control" and the "Battery Pack" blocks shown in Fig. 2. During the training, the sniffed values of SOC and P_{ESS} were used as training sequence and the network was configured in open loop (i.e. without feeding back the estimated SOC_{est} signal) as shown in Figure 4. The prediction error between the actual plant output $SOC(k)$ and the neural network output $SOC_{est}(k)$ was used as the neural network training signal. The mapping function α_2 of the ANN-2 is defined according to (xxx).

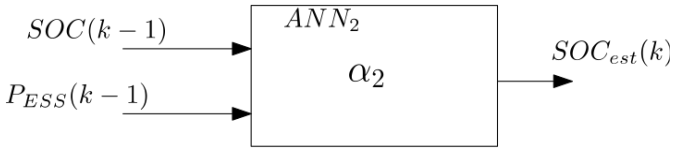

Fig. 4 Neural Network for predicting SOC

$$SOC_{est}(k) = \alpha_2(P_{ESS}(k), SOC(k)) \quad \text{(xxxx)}$$

The Table xx shows the configuration and parameters used for the training of each ANN-model.

	ANN-1		ANN-2
Configuration (Number of neurons)	3-15-10-5-1 (Feedforward - Backpropagation)		2-10-5-1 (Feedforward - Backpropagation)
Activation Functions	Hidden layer 1	linear	hidden_layer{1} - linear hidden_layer{2} - Hyperbolic tangent sigmoid output_layer - linear
	Hidden layer 2	Hyperbolic tangent sigmoid	
	Hidden layer 3	Hyperbolic tangent sigmoid	
	Output layer	linear	

For test/operation mode, a complete model combining both ANNs was proposed. Figure xx shows the complete ANN-based model of the BESS system (which is used to perform the stealth attack), the dashed rectangle represents the estimated model $\hat{\beta}$. Note that in test/operation mode the ANN-1 and ANN-2 run in closed loop form and only P_{Req} is acquired from the actual system. The predict values $P_{ESS,est}$ and SOC_{est} can be rewritten as (xx) and (xx) , respectively.

$$P_{ESS,est}(k) = \alpha_1(P_{Req}(k), P_{ESS,est}(k-1), SOC_{est}(k-1)) \quad \text{(xxx)}$$

$$SOC_{est}(k) = \alpha_2(P_{ESS,est}(k), SOC_{est}(k)) \quad \text{(x x x x)}$$

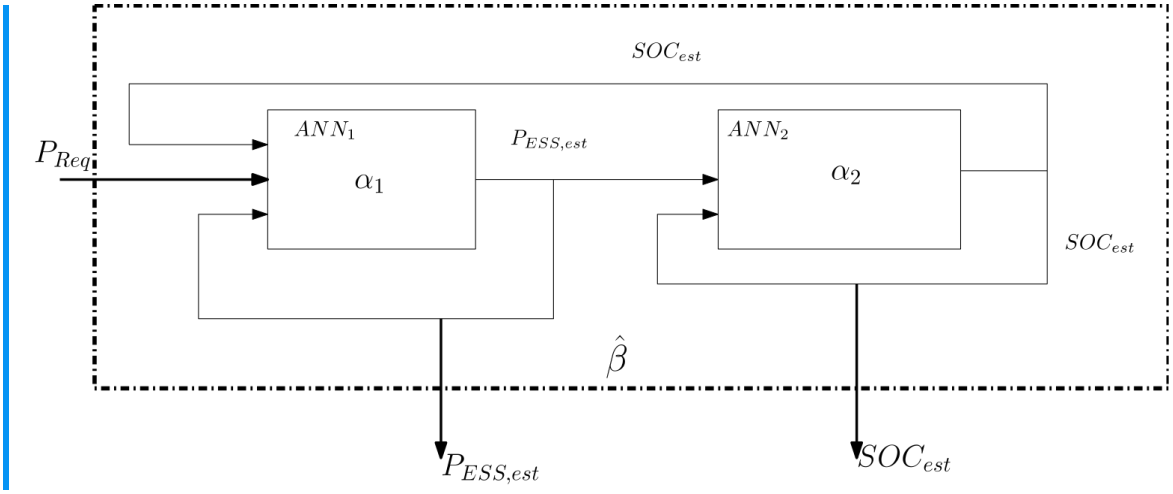

Fig. xx ANN-based System Identification.