IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON NEW TRENDS IN BRAIN SIGNAL PROCESSING AND ANALYSIS

Received January 31, 2019, accepted February 11, 2019, date of publication February 20, 2019, date of current version March 7, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2899558

A Novel Deep Learning Strategy for Classifying Different Attack Patterns for Deep Brain Implants

HEENA RATHORE[1], (Member, IEEE), ABDULLA KHALID AL-ALI[1], (Member, IEEE), AMR MOHAMED[1], (Senior Member, IEEE), XIAOJIANG DU[2], (Senior Member, IEEE), AND MOHSEN GUIZANI[1], (Fellow, IEEE)

[1]Department of Computer Science and Engineering, Qatar University, Qatar
[2]Department of Computer and Information Sciences, Temple University, Philadelphia, PA 19122 , USA

Corresponding author: Heena Rathore (heena.rathore@ieee.org)

This work was supported by the Qatar National Research Fund (a member of Qatar Foundation) through NPRP under Grant 8-408-2-172.

ABSTRACT Deep brain stimulators (DBSs), a widely used and comprehensively acknowledged restorative methodology, are a type of implantable medical device which uses electrical stimulation to treat neurological disorders. These devices are widely used to treat diseases such as Parkinson, movement disorder, epilepsy, and psychiatric disorders. Security in such devices plays a vital role since it can directly affect the mental, emotional, and physical state of human bodies. In worst-case situations, it can even lead to the patient's death. An adversary in such devices, for instance, can inhibit the normal functionality of the brain by introducing fake stimulation inside the human brain. Nonetheless, the adversary can impair the motor functions, alter impulse control, induce pain, or even modify the emotional pattern of the patient by giving fake stimulations through DBSs. This paper presents a deep learning methodology to predict different attack stimulations in DBSs. The proposed work uses long short-term memory, a type of recurrent network for forecasting and predicting rest tremor velocity. (A type of characteristic observed to evaluate the intensity of the neurological diseases) The prediction helps in diagnosing fake versus genuine stimulations. The effect of deep brain stimulation was tested on Parkinson tremor patients. The proposed methodology was able to detect different types of emulated attack patterns efficiently and thereby notifying the patient about the possible attack.

INDEX TERMS Deep brain stimulators, deep learning, implantable medical devices, machine learning, security.

I. INTRODUCTION

For a few decades electrical stimulation has been utilized to tweak the sensory and neurological system in human patients [1]. The principal reports of deep brain stimulation, being utilized to treat Parkinsons disease at professor Benabid's facility, were distributed in 1993 despite the fact that the group had performed initial experiments in 1987 [2]. In 2002, Deep Brain Stimulators (DBS) were granted endorsement by the US Food and Drug Administration (FDA) for the treatment of Parkinson's ailment [3]. Thereafter, DBS, which utilizes a pacemaker-like gadget to convey consistent electrical stimulation inside the cerebrum, has been utilized to treat more than 100,000 individuals around the world with Parkinsons disease and tremor. The worldwide DBS market was estimated to be around USD 618.6 million in 2014 and is expected to grow at a compound annual growth rate of over 17.0% over the next years [4]. Worldwide DBS market is expected to achieve USD 1,592.9 million by 2020, as per a review by Grand View Research, Inc [5]. Current DBS frameworks incorporate a quadripolar electrode embedded into the human brain, inline expansions either running behind or embedded inside the ear, and an Implantable Pulse Generator (IPG) embedded either on top of or inside the region above the chest as shown in Figure 1. The patient is given a controller to turn the device on or off. Some IPGs can likewise be customized to permit the patient to change the voltage inside set points of confinement. Needless to say DBS has led to enhancements and personal life satisfaction in patient's with Parkinson disease.

The associate editor coordinating the review of this manuscript and approving it for publication was Victor Hugo Albuquerque.

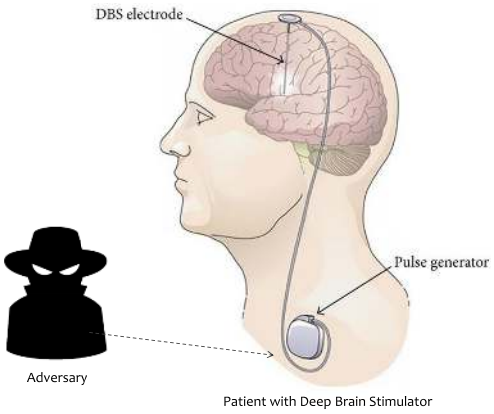

FIGURE 1. Threat Model: Adversary inhibit the implanted DBS inorder to generate fake stimulations.

It has also shown tremendous efficacy for patients with movement disorders. It has been estimated that there are over 180,000 individuals in the United States below 70 years of age with Parkinson Disease [6]. Moreover, depression influences more than 18 million individuals in the United States alone [7]. Notwithstanding psychiatric disorders, DBS has additionally been proposed as a potential treatment for hypertension, obesity and dietary issues. Also, it is also being used for neurological pains and headaches [8]. Medtronic65 and Advanced Neurologic Frameworks are some of the types of frameworks which are utilized as a part of DBS.

A novel innovation such as DBS has a set of issues especially related to security. This requires training of doctors, medical attendants, and patients to learn how to deal with these unpredictable security issues in such gadgets. The ability to control the gadget, and generate stimulation, allows us to perform randomized, blinded, hybrid trials to assess the efficacy of the device [9]. With practical imaging and fundamental science systems recognizing discrete regions of the brain associated with various neurological and psychiatric conditions, security to such vulnerable device plays a major role. Archimedes [10] has demonstrated that they could forge an erratic signal with radio frequency electromagnetic waves in order to hack the implants inside the body. Theoretically, a false signal, like the one they created, could inhibit required stimulation or induce unnecessary shocks in human brain. Thus, brain implants such as DBS are turning out to be a more typical example of a device that can be hacked. As the brain implants are getting cheaper and better, more and more patients are heavily relying on them. Consider what a terrorist could do with the access to a politician's mind or how coercive blackmail would be if someone were to alter how you act and think? To date, while there are few accidents or disasters due to faulty or malicious devices, as the volume and application space increases, these devices would be more prone to such attacks.

The future of neurological implants is bright, but even a single high-profile incident could irreparably damage public confidence in the safety of these devices, so the risk of brain jacking should be taken seriously and proactively before it is too late. The methodology proposed in this paper brain tunes DBS with the help of its own replica, i.e., a biologically neural inspired model, to develop an efficient, robust and secure solution. The proposed work, i.e., deep learning strategy, is inspired from biological neural networks (human brain). The biological neural network comprises of interconnected neurons utilized to trade messages between one another. The interconnections have weights that can be tuned with respect to experience, thus making neural networks fit for learning [11]. The objective here is not to make practical models of the human brain, but rather to create robust and effective information structures that we can use to model difficult problems. This paper presents techniques to emulate attack patterns and propose deep learning strategy to classify different attack patterns for deep brain implants. The outline of the paper is as follows: Section II presents the related work on the security of implantable medical devices. Section III provides an insight on the network and attack model. Section IV presents the details on the proposed model. This section also gives the motivation for the proposed problem. Results of the proposed work is shown in Section V. Section VI concludes the paper and presents scope for future work.

II. RELATED WORK AND BACKGROUND

Wireless Implantable Medical Devices (IMDs) have wireless capability of transmitting information. This capability provides room for the attackers to eavesdrop the information, compromise the patient's data with the intent to physically harm them by reprogramming the implanted devices [12]. For instance, an intruder can listen to an IMD's radio transmissions and can frequently learn private data with insignificant effort from his side. Such an attack can access to the data acquisition of an oscilloscope, programming radio, directional receiving wires, and other listening gears of the medical devices. A few reviews have considered such an attack of listening stealthily or eavesdropping to steal patients' information [13], [14]. Besides this, another type of attack can be introduced in IMDs where in the intruder has the capability to create radio transmissions to replay repeated operations and commands. A study performed by Halperin *et al.* [15] shows that with a programmable radio, one can control an implanted defibrillator by replaying messages, thereby incapacitating modified treatments. Alternatively, it can also convey a message to stun planned to initiate a deadly heart attack. Insulin pumps used to monitor glucose for the diabetic patients works on an open loop methodology, i.e., they require patients to change the pump setting [16]. Modifying the pump settings showed a threat vulnerability which proved to be a crucial concern for the patients. Work presented in [13] has shown comparable control over an insulin pump, including the capacity to stop insulin or infuse enormous dosage. Another way is to dismantle the framework to control the device operation. By assessing the Java-based program provided with his own particular insulin pump, analyst Jerome Radcliffe was able to figure out the insulin pump's structure, uncovering that the pump neglected to preserve the medical

information it transmitted [17]. Moreover, there may be a situation which is much more coordinated where the attacker can be both near the patient and the device programmer. Even during the setting or modifying of the IMD code for security, software/hardware engineer or health care professional can install a malign code to give excess dosage in case of medical devices. Thus, IMDs should address the above mentioned threat vulnerabilities to ensure safety, security, availability and privacy for the patients. Thus, these medical devices should be secure to capture any sort of threat that can be injurious for the health of the patients.

There are a number of diverse solutions which address the security issues in wireless IMDs [18]. Bio-metric based approaches access the unique physiological characteristics of the human body and provide authentication. Though the mechanism is secure and lightweight, the scheme lacks to accommodate the changes of bio-metric with respect to time [19], [20]. Distance based approaches estimate the physical distance between the IMD and the caregiver by utilizing the transmitted and received transmission in proximity through piezoelectric elements [15], Diffie Hellam protocol [21], and near field communication [22]. The scheme fails since the attacker can make a physical connection with the patient by approaching in near proximity, thus leading to weak authentication. Key management protocols are used for providing authentication to the authorised users using symmetric [15], public key [23] and physiological [24] signals for the generation of keys. Key management protocols are less reliable and incur extra waiting time for the authentication. Additionally, anomaly detection mechanism such as deep learning [29], [30] and support vector machines [28], [31] have been used for determining the dosage pattern for the insulin pump security. External device methodologies employ extra devices to be worn to provide authentication such as IMDGaurd [36], MedMon [37], Cloaker [38] and IMDShield [39]. These methodologies not only require extra gadget to be carried besides the wireless medical device, but also consume battery life of the medical device. Additionally, the adversary can come close to the patient and disrupt the functionality of the device. Besides this, there are a diverse set of the conventional schemes utilized for overcoming attacks in wireless medical devices [32]–[35]. Several other papers (e.g., [40]–[42]) studied related security issues to such gadgets.

The present state of art does not provides security solutions for DBS. This paper is a first attempt towards classifying attack patterns of DBS. It presents a fast and efficient model for improving the security issues in DBS with the help of human inspired model, viz deep learning strategy. Though Pycroft *et al.* [25] study the types of attacks in implantable DBS, we emulate some of the attacks presented in [25] and predict them using deep learning strategy. More specifically, this paper plans to achieve the following research objectives:

- Design and train a Long Short Term Memory (LSTM), a deep learning classifier to predict and forecast consecutive brain stimulation pattern.

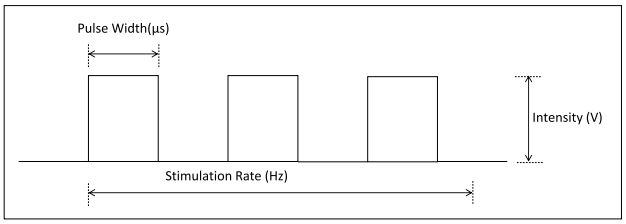

FIGURE 2. Stimulation waveform in DBS.

- Emulate different types of attack patterns and classify them in deep brain implants, i.e., determine or classify the type of attack strategy used by the attacker. More specifically, a prediction mechanism is developed by emulating different attack patterns that can be utilized by the attacker. Once the attack has been predicted by the classifier, patient is notified about the attack.

III. NETWORK AND ATTACK MODEL

A. ADVERSARY MODEL

Neural implants such as DBS are intended to stimulate certain regions of the brain for the treatment of various chronic diseases. DBSs are implanted to treat diseases such as Parkinsons disease, chronic pain, and other therapeutic conditions such as tremors, movement disorders, and psychiatric treatment. In the near future, DBSs hold the potential to be ubiquitous, mechanically fit, thereby addressing more extensive clinical needs [26]. As this happens addressing brain implants security turns out to be a key challenge. For instance, patients may endeavor to self-endorse raised states of mind or expanded initiation in the cerebrum, or programmers may endeavor to program the stimulation treatment. However these perfectly valid actions may breach the integrity property of the device. Moreover, the attacker can damage the brain cells or can cause diverse neural pathways by inserting the mind with arbitrary stimulation signals. On the other hand, attacker may remotely keep the gadget from working as designed to diminish availability property. Besides that, the risk escalates if the patient is receiving treatment on more sensitive condition such as depression. Pycroft *et al.* [25] have divided the types of attacks in DBS in two ways namely blind attacks and targeted attacks. Blind attacks include cessation of stimulation, draining implant batteries, inducing tissue damage, and information theft. Targeted attacks include impairment of motor function, alteration of impulse control, modification of emotions or affect, induction of pain, and modulation of the reward system. In this paper, we would investigate these attacks by emulating these attack patterns and classifying them.

B. PROBLEM STATEMENT

The primary goal of DBS is to superimpose a stimulation pattern over the patient's chronic pain pattern and to establish a correct stimulation waveform with the help of specified stimulation parameters such as amplitude, pulse width, effective or ineffective stimulation etc. Figure 2 shows a typical continuous stimulation waveform given to DBS.

When an external reader attempts to connect with an IMD, authentication followed by communication between the IMD and the reader is made. In such cases, the attacker can modify the stimulation pattern in order to introduce acute stimulation pattern inside the human brain. The attacker can introduce different types of stimulation parameters to disrupt the normal functionality of the DBS. This paper emulates different types of attack strategies by changing the patterns of pulse width, stimulation rate, intensity etc. It then studies the pattern of rest tremor velocity (a type of characteristic observed to evaluate the intensity of the neurological diseases) based on the pattern of introduced attack strategies.

IV. PROPOSED WORK

A. MOTIVATION

Biological systems have caught the attention of scientific community in diverse fields such as computer science, mechanical, agriculture, energy etc [27]. Bio-inspired systems refer to applying concepts from biology domain such as body and brain operation to practical problems in other domains such as security and intrusion prevention. Biologically inspired approaches seem promising and are considered stronger in comparison to any other system. It can be observed that, in contrast to the existing models which require regular updating, replacement, nourishing, bio-inspired models maintain themselves and even learn during changing conditions. Therefore, engineers and scientists of diverse domains are engaging themselves in investigating innovative design architectures to resolve different challenges. In the near future we may even create machines that repair themselves, like the way skin recuperates over an injury. The future of engineering lies in the development of flexible, self-healing bio-inspired models.

B. RECURRENT NEURAL NETWORK

Deep learning, a type of biologically inspired model, is a special branch of machine learning used to understand the inbuilt patterns in the information. Deep learning model comprises of neural network training which conditions the available data by calibrating the weights and input data with the help of an activation function. This paper uses recurrent neural network which permits the information to persist. With recurrent neural network, the input data is passed into a cell, which besides outputting the activation function, passes the output as a feedback to the cell. Long Short Term Memory (LSTM) network is a type of recurrent neural network which stores the information for longer period of time. LSTM, with the help of Keep Gate or Forget Gate, decides which data to keep, or remove from the recurring data. Those gates either block or pass on the information recieved based on its strength. This action, similar to neural networks, is done by filtering with their own sets of weights. Those weights, like the weights that modulate input and hidden states, are adjusted via the recurrent networks learning process. That is, the cells learn when to allow data to enter, leave or be deleted through the iterative process of making guesses, backpropagating error, and adjusting weights via gradient descent.

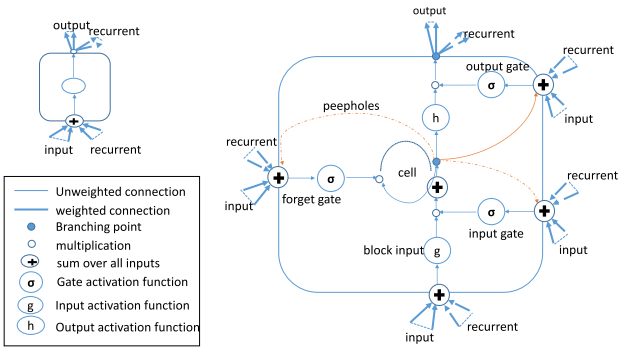

FIGURE 3. Detailed schematic of simple recurrent neural network and long short term memory neural network (reproduced from [44]).

Figure 3 shows the schematic diagram of a simple recurrent neural network and LSTM neural network. LSTMs' memory cells give different roles to addition and multiplication in the transformation of input. The central plus sign (additional node) helps them preserve a constant error when it must be backpropagated at depth. Instead of determining the subsequent cell state by multiplying its current state with new input, they add the two. Different sets of weights filter the input data for input, output and forgetting gates. The forget gate is represented as a linear identity function, because if the gate is open, the current state of the memory cell is simply multiplied by one, to propagate forward one more time step.

C. LSTM FOR PARKINSON DISEASE

This paper has two contributions. First, we design and train a LSTM classifier to predict consecutive deep brain stimulation patterns for all the patients. Secondly, we emulate and predict different types of attack patterns in deep brain implants for individual patients. By doing so we can determine the type of attack strategy that can be used by the attacker. More specifically, a prediction mechanism is developed by emulating different attack patterns to change brain stimulation parameters which can be utilized by the attacker for deep brain implants.

1) MULTIVARIATE LSTM FORECAST MODEL FOR ALL PATIENTS

The essential objective of programming the neurostimulators is to superimpose the stimulation or paraesthesia design over the patient to set up the right stimulation waveform. Every patient requires a unique stimulation pattern to help control their pain. The classification task involves predicting the genuine or fake stimulaion of DBS from the data obtained from Physionet [45]. To evaluate the performance of the proposed approach, experiments were ran on following 10 features. A typical brain stimulator has following parameters which are used to control individual pain [46]:

- *Stimulation Target*: Parkinson's disease which receives chronic high frequency electrical DBS in one of

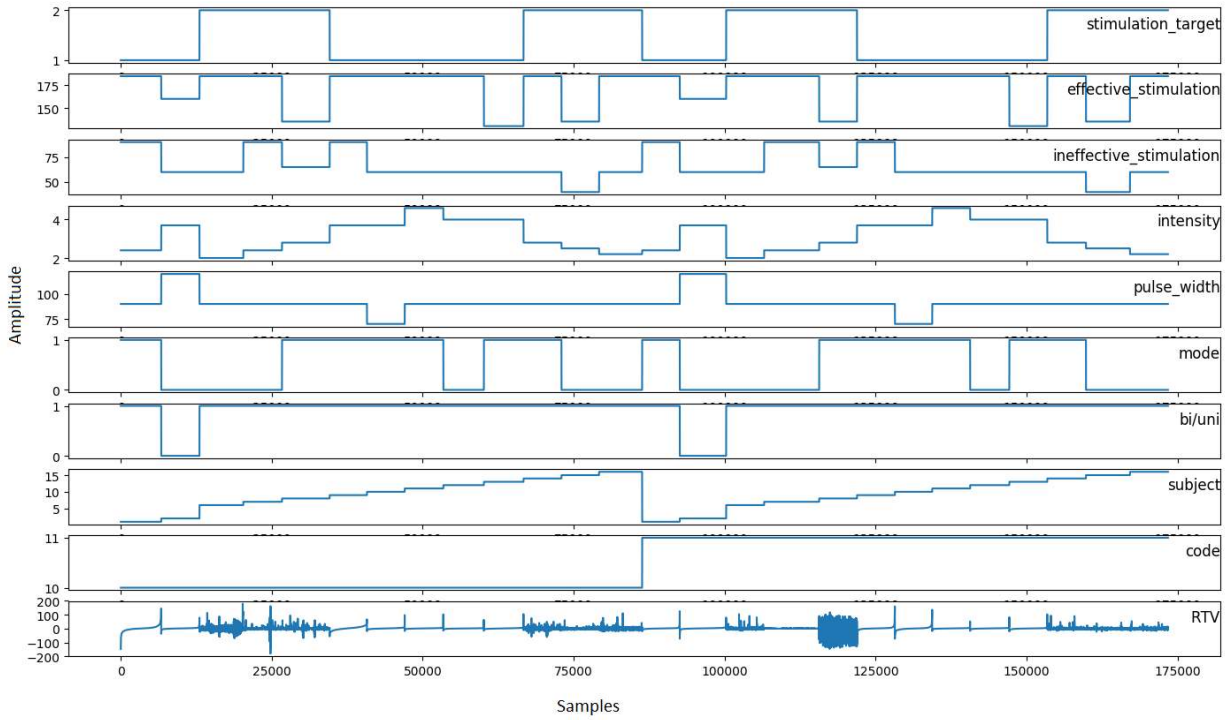

FIGURE 4. Line plots of parkinson tremor stimulation pattern for different subjects.

three targets viz: the ventro-intermediate nucleus of the thalamus, the internal Globus pallidus, or the subthalamic nucleus.

- *Stimulation Rate*: Frequency (Hz) of effective stimulation ($>$ 100 Hz).
- *Intensity*: It is experienced by the patient as the strength of the paraesthesia, measured in volts (V). It can be set from 0 to 10.5 V, depending on the patient's needs.
- *Pulse Width*: A measure in microseconds (μs) of the duration of a pulse. In general, the wider the pulse width, the larger the tissue area being stimulated, and the stronger the sensation of paraesthesia. For neurostimulation, the pulse width is normally set at $180\mu s$.
- *Mode*: Various stimulation alternatives can be utilized to enhance comfort, increment battery life, and modify the stimulation design. For instance: the continuous mode conveys continuous electrical stimulation to the chosen nerves over a drawn out timeframe on 24 hour basis. After the patient gets accustomed to the vibe of stimulation, the cycling mode is generally modified in light of the fact that it might fundamentally expand battery life, while regulating pain. The cycling mode consequently invigorates for indicated ON and OFF duty cycle e.g., 30 seconds ON and 30 seconds OFF.
- *Electrode selection*: This includes bipolar or unipolar stimulation.
- *Patient information*: 16 subjects with Parkinson's disease in the age group of 37-68 are studied.
- *Code*: Two conditions of DBS are studied viz with medication (11) and without medication (10).
- *Rest Tremor Velocity (RTV)*: It is defined as the tremor which occurs when the muscles are not being voluntarily moved. The recordings in this database are of RTV in the index finger.

Figure 4 shows the plot with 10 subplots of Parkinson tremor data for each stimulation parameter. The Parkinson tremor dataset from Physionet is used to frame a forecasting problem where, given the stimulation conditions and RTV for a time period T, we forecast the stimulation condition and RTV at $T + \delta T$. For this study, T and δT are set to 1 second. The training makes the classifier learn the consecutive stimulation pattern.

In this study, as seen in Figure 4, we can analyze the pattern of deep brain stimulation. Here, we frame the supervised learning problem as predicting the RTV at the current second (t) given the RTV measurement and DBS parameters conditions at the prior time step. The training is made on 8760 samples and validated on 164638 samples. Also, the features are normalized to fed into the network. Finally, the stimulation parameters inputs (X) are reshaped into the 3D format expected by LSTMs, namely [samples, timesteps, features]. The LSTM is defined with 50 neurons in the first hidden layer and 1 neuron in the output layer for predicting RTV. The input shape is of 1 time step with 9 features. We used mean absolute error loss function and the efficient Adam version of stochastic gradient descent. The model is fitted for 50 training epochs with a batch size of 72. For this study we calculate the loss between the actual stimulation parameter and the predicated consecutive stimulation parameter as shown in Figure 8.

2) PREDICTING THE REST TREMOR VELOCITY BY EMULATING DIFFERENT ATTACK PATTERN

Adversary can apply different attack strategies as explained in Section V in order to change the behavior of the patient using DBS. In order to study the effect of deep brain stimulation on amplitude and frequency characteristics of rest tremor in Parkinson's disease [43], different attack strategy was carried out. RTV generally has a frequency of about 46 Hz for controlled neurological patients. It is considered as the main characteristic to be measured for DBS implanted patients. Besides this, Beuter [43] has studied four more tremor characteristics. These are:

- *Amplitude*: It is defined as the root mean square of the RTV signal. The increase in the RTV amplitude is considered as the sign of abnormality. For each patient, for our study, we computed the amplitude for next 100 steps, i.e., RTV for nearly 1 min.
- *Amplitude Fluctuations*: It is defined as the variability of the RTV amplitude. Increasing scores indicate that tremor amplitude is fluctuating over time and is considered as a sign of abnormality.
- *Spectral Concentrations*: It is measured by the concentration of power in a narrow frequency range which is set as 100 for our study. Decreasing scores are sign of abnormality.
- *Median Frequency*: Median RTV is calculated for every 100 samples (1 min). Decreasing values are sign of abnormality.

For this study, besides RTV, we also calculated aforementioned tremor characteristics to feed in the LSTM for training and predicting purposes. Once the attack is classified, a warning is given to the patient about the attack to check the settings of the brain stimulation and change accordingly.

For this study, the data is transformed and loaded from the CSV file to the array that feeds in the LSTM. The Keras LSTM layers take the **numpy** array of 3 dimensions (N, W, F) where N is the number of training sequences, W is the sequence length and F is the number of features of each sequence. For this paper, W(read window size) is set as 50 which allows the network to get glimpses into the shape of the RTV at each sequence. This process enable us to build up a pattern of the sequences based on the prior window received. The sequences themselves are sliding windows and hence shift by 1 each time, causing a constant overlap with the prior windows. We used 1 input layer (consisting of a sequence of size 50) which feeds into an LSTM layer with 50 neurons, that in turn feeds into another LSTM layer with 100 neurons which then feeds into a fully connected normal layer of 1 neuron with a linear activation function. These steps will be used to give the prediction of the next time step. We used 1 training epoch with this LSTM. With this 1 epoch, an LSTM will cycle through all the sequence windows in the training set once. At each time step, we then pop the oldest entry out of the rear of the window and append the prediction for the next time step to the front of the window, in essence shifting the window along so that it slowly builds itself with predictions,

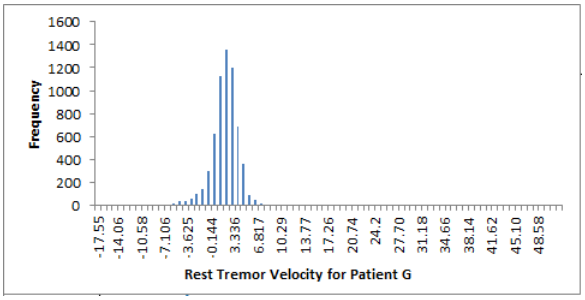

FIGURE 5. Patient G rest tremor velocity analysis: With stimulation on and medication on, RTV is close to zero (No attack).

until the window is full of only predicted values. In our case, as our window is of size 50 this would occur after 50 time steps. We then keep this up indefinitely, predicting the next time step on the predictions of the previous time steps, to see an emerging trend. We limited our prediction sequence to 50 future time steps and then shifting the initiation window by 50 each time, in effect creating many independent sequence predictions of 50 time steps.

V. PERFORMANCE EVALUATION

The hardware used for the training phase was nvidia GPU card and Windows 7 operating system with nvidia Cuda 7.5 as the general software architecture. For data preparation, training, and evaluating deep neural networks, the Keras [50] framework with Theano [51] backend was used. The section presents the data analysis of Parkinsons disease patients and the results for the proposed work. It presents the study of Parkinsons disease patients with and without the stimulation.

A. DATA ANALYSIS AND INSIGHTS FROM PHYSIONET DATA

Among all the features, Rest Tremor Velocity (RTV) is the most important feature for evaluating the Parkinson tremor intensity. It is considered as the first sign of neurological disorder. RTV value is negligible or close to zero for normal individuals and controlled Parkinson disease patients. Figure 5 shows the frequency of RTV values for patient 'G' from the physionet dataset. It is observed that the RTV is generally close to zero when the DBS is controlled with genuine stimulations.

The RTV for a Parkinson disease patient is shown in Figure 6 on various conditions viz.: stimulation on, medication on; stimulation on, medication off; and stimulation off and medication off. It can be inferred from the figure that after the DBS implantation, the RTV is controlled and the value is mostly close to zero as compared to other conditions.

B. ADVERSARY ATTACK STRATEGIES

The adversary can employ different types of attack strategies [47] in DBS. We have emulated different attack strategies by changing the learnt stimulation pattern from study 1. The different attack strategies that can be emulated in DBS are:

- *Spike (Single Acute Spike Attack)*: Spike attack strategy, as shown in Figure 7(a), are multiple data points with a

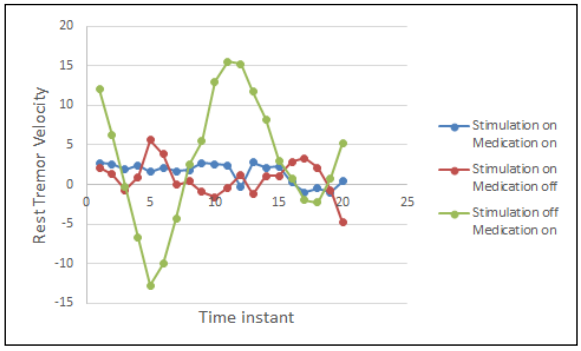

FIGURE 6. Rest tremor velocity of a parkinson disease patient g2 for 20 sec (stimulator implanted in the globus pallidus).

much greater expected rate of change. These pattern can be caused by multiple acute intensity pulses targeted to the patient.

- *Outlier (Multiple Overdose Attack Strategy)*: Outlier attack strategy produces discontinuous acute stimulation which produces the rest tremor velocity pattern shown in Figure 7(b). It can be caused by high intensified pulse at discontinuous stimulation rate.
- *Stuck At Attack Strategy*: Stuck-at attack strategy, as shown in Figure 7(c) also make RTV experience zero variation for unexpected lengths of time, which can be caused by increased pulse width for a definite amount of time.
- *Incremental (Increasing Attack Strategy)*: RTV pattern shows a increasing trend with the increased stimulation rate, as shown in Figure 7(d).
- *Chronic (Incremental Decremented Attack Strategy)*: Chronic attack strategy looks similar to incremental attack strategy with the continuous form of increase and decrease in the RTV pattern, as shown in Figure 7(e).
- *Noise (Arbitrary Attack Strategy)*: Noise faults make RTV values experience unexpectedly high variation, which can be due to hardware failure caused by the adversary (See Figure 7(f)).
- *Unusual Attack Strategy*: The unusual attack pattern can be caused by the adversary by arbitrary changing the intensity, pulse width, stimulation rate and intensity of the DBS. Here, the RTV pattern shows an arbitrary form.

The observable pattern of these attacks can be pictorially represented in Figure 7. The emulated pattern is made by changing the deep brain parameters such as stimulation rate, intensity, pulse width, mode etc. as explained earlier. RTV is the obervable pattern or outcome of simulations.

C. PERFORMANCE METRICS

The following performance evaluation metrics are used to validate the proposed work.

- Training Loss: It is the average loss during the epoch between real RTV and predicted RTV.
- Validation Loss: It is the average loss after the end of the epoch.

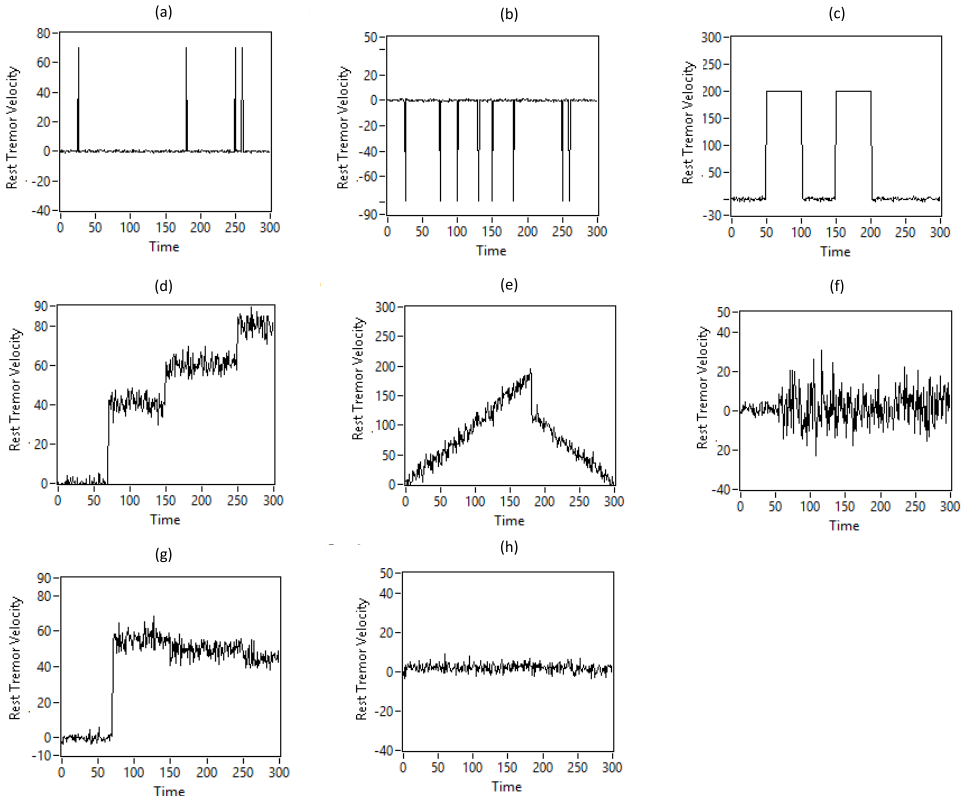

FIGURE 7. Emulating different attack strategies in DBS. (a) Spike attack strategy. (b) Outlier attack strategy. (c) Stuck at attack strategy. (d) Incremental attack strategy. (e) Chronic attack strategy. (f) Noise attack strategy. (g) Unusual attack strategy. (h) Genuine measurements.

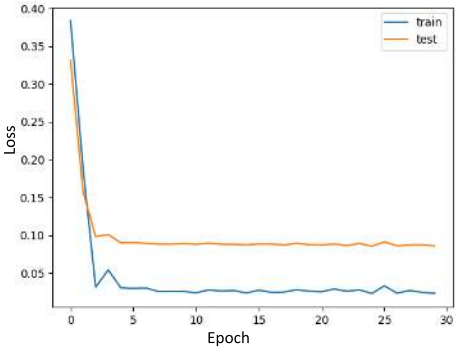

FIGURE 8. Loss plot of the actual stimulation parameter and the predicated ponsecutive stimulation parameter.

- Training Duration: Amount of time required to learn and train the classifier for different attack strategies.

D. RESULTS

For study 1, we calculate the Root Mean Squared Error (RMSE) to find the error between the predicted and actual value of RTV. Figure 8 plot shows the train and test loss during training. As seen from figure, the loss between the predicted and actual data is minimal. Also, the model achieved RMSE as 0.095.

For study 2 (introducing attack strategies), we predict RTV and calculate amplitude, amplitude fluctuations, spectral concentrations and median frequency to feed them as features to LSTM. LSTM detects abnormality in the RTV, by observing the signals of amplitude, amplitude fluctuations, spectral concentrations and median frequency, (which is calculated by observing next 100 time steps). LSTM is used here to predict the next epoch (50 steps forward). Figure 9 shows the predicted and true attack RTV data values 50 time step ahead at each step in time for 700 steps. The figure explains after LSTM learns the system in such a way that even after the introduction of attack (blue lines), it predicts the RTV should be approximately close to zero. For instance, in case of spike attack, RTV could reach upto 50, but the system based on the learning predicts the genuine RTV should not be greater than zero. Stuck at attack and incremental attack patterns predicted RTV values comes approximately in the range of $0 - 3$. Further, Table 1 shows the training loss, validation loss and training duration for different types of attack strategy for deep brain implants. It can be seen for continuous and single pulse attack patterns such as spike, outlier, incremental, chronic, the loss values were less in comparison to the discontinuous and arbitrary attack patterns(stuck-at and noise). Stuck-at and noise attack pattern showed the maximum loss values

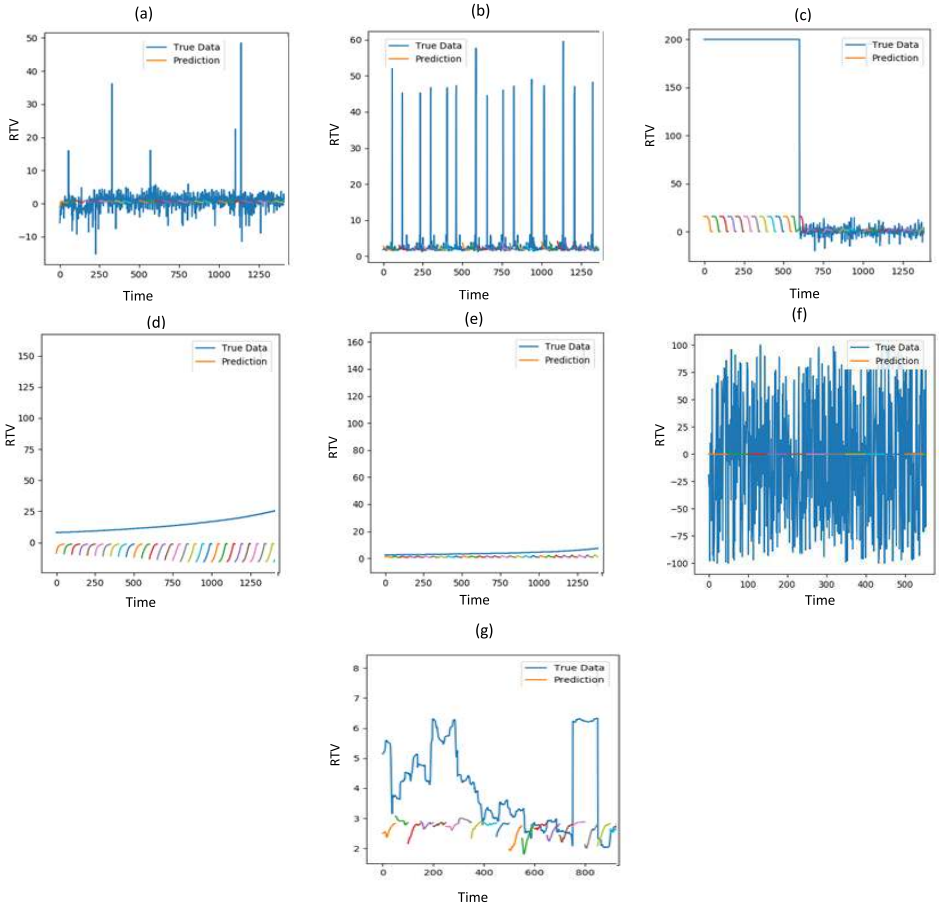

FIGURE 9. Emulating different attack strategy in DBS: epochs = 1, window size = 50, sequence shift = 50. (a) Spike attack. (b) Outlier attack. (c) Stuck at attack. (d) Incremental attack. (e) Chronic attack. (f) Noise attack. (g) Unusual attack.

TABLE 1. Performance evaluation for DBS.

Attack	Training-Loss	Validation-loss	Training Duration(ms)
Spike Attack	56.87	239.48	84.28
Outlier Attack	60.47	43.67	81.9 7
Stuck at Attack	13120.94	27.24	199.77
Incremental Attack	22.67	176.65	80.101
Chronic Attack	122.66	3.36	79.49
Noise Attack	2839.15	3473.6162	80.07
Unusual Attack	388.07	44.65	79.86

since they require more training as the pattern is hard to be predicted. Whenever the predicted RTV and the true RTV exhibited a difference, a flag was raised and consecutive iterations was studied to predict the emulated attack. Our model was able to classify the emulated attack strategies in the deep brain implants and thereby raising the flag. As soon as the attack is detected, the patient and the doctor is warned about the attack and are notified to change the current stimulation parameters set.

VI. CONCLUSION

Deep brain stimulators (DBS), a type of wireless implantable medical device, treats neurological disorders by giving stimualtions inside the patients brain. DBS have progressively benefited patients, yet they have posed in parallel certain security implications. Security for such devices is important since they can directly affect the mental and physical orientation of patients. This paper utilizes Long Short Term Memory, a type of recurrent neural network, to predict and forecast the pattern of DBS. Rest Tremor Velocity (RTV) is examined to study the intensity of neurological disorders. For this, we studied and examined RTV values to design and train the neural network. Various attack patterns were introduced in the DBS framework to emulate and classify different attack strategies. The results show that the model was able to classify different attack patterns in the DBS with smaller loss values and minimal training time. In the near future, the proposed framework will be implemented on a real deep brain stimulator environment with real RTV measurements. To evaluate the performance of the framework in terms of accuracy and reliability, genuine and fake measurements will be classified and predicted at run time.

ACKNOWLEDGEMENT

The statements made herein are solely the responsibility of the authors.

REFERENCES

[1] D. M. Long, "Electrical stimulation of the nervous system for pain control," *Electroencephalogr. Clin. Neurophysiology. Suppl.*, vol. 34, pp. 343–348, 1978.
[2] T. Parkinson, "Appeal for deep brain stimulation, history of deep brain stimulation," Tech. Rep., Jun. 2018.
[3] J. Gardner, "A history of deep brain stimulation: Technological innovation and the role of clinical assessment tools," *Social Stud. Sci.*, vol. 43, no. 5, pp. 707–728, 2013.
[4] *Deep Brain Stimulators (DBS) Market Analysis By Application (Pain Management, Epilepsy, Essential Tremor, Obsessive Compulsive Disorder, Depression, Dystonia, Parkinsons Disease) And Segment Forecasts To 2020*, Market Research Report, 2015.
[5] *Deep Brain Stimulators Market Worth $1.6 Billion by 2020*, Grand View Research, 2015.
[6] E. R. Dorsey *et al.*, "Projected number of people with Parkinson disease in the most populous nations, 2005 through 2030," *Neurology*, vol. 68, no. 5, pp. 384–386, 2007.
[7] J. M. Schwalb and C. Hamani, "The history and future of deep brain stimulation," *Neurotherapeutics*, vol. 5, no. 1, pp. 3–13, 2018.
[8] M. Leone *et al.*, "Deep brain stimulation and cluster headache," *Neurological Sci.*, vol. 26, pp. s138–s138, May 2005.
[9] M. B. Keller, "Issues in treatment-resistant depression," *J. Clin. Psychiatry*, vol. 66, pp. 5–12, Jan. 2005.
[10] (2017). *Archimedes*. [Online]. Available: https://Www.Youtube.Com/Watch?V=Fmflalzo6ig
[11] H. Rathore, "Artificial neural network," in *Mapping Biological Systems to Network Systems*. Springer, 2016, pp. 79–96.
[12] Z. E. Ankarali, Q. H. Abbasi, A. F. Demir, E. Serpedin, K. Qaraqe, and H. Arslan, "A comparative review on the wireless implantable medical devices privacy and security," in *Proc. EAI 4th Int. Conf. Wireless Mobile Commun. Healthcare (Mobihealth)*, Nov. 2014, pp. 246–249.
[13] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *Proc. 13th IEEE Int. Conf. e-Health Netw. Appl. Services (Healthcom)*, Jun. 2011, pp. 150–156.
[14] N. Paul, T. Kohno, and D. C. Klonoff, "A review of the security of insulin pump infusion systems," *J. Diabetes Sci. Technol.*, vol. 5, no. 6, pp. 1557–1562, 2011.
[15] D. Halperin *et al.*, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *Proc. IEEE Symp. Secur. Privacy*, May 2008, pp. 129–142.
[16] W. Burleson, S. S. Clark, B. Ransford, and K. Fu, "Design challenges for secure implantable medical devices," in *Proc. 49th Annu. Design Autom. Conf.*, Jun. 2012, pp. 12–17.
[17] J. Radcliffe, "Hacking medical devices for fun and insulin: Breaking the human SCADA system," in *Proc. Black Hat Conf. Presentation Slides*, 2011.
[18] H. Rathore, A. Mohamed, A. Al-Ali, X. Du, and M. Guizani, "A review of security challenges, attacks and resolutions for wireless medical devices," in *Proc. 13th Int. IEEE Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2017, pp. 1495–1501.
[19] H. Rathore *et al.*, "Multi-layer security scheme for implantable medical devices," *Neural Comput. Appl.*, pp. 1–14, Oct. 2018.
[20] H. Rathore, A. Al-Ali, A. Mohamed, X. Du, and M. Guizani, "DTW based authentication for wireless medical device security," in *Proc. IEEE 14th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2018, pp. 476–481.
[21] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, "Proximity-based access control for implantable medical devices," in *Proc. 16th ACM Conf. Comput. Commun. Secur.*, 2009, pp. 410–419.
[22] B. Kim, J. Yu, and H. Kim, "*In-vivo* NFC: Remote monitoring of implanted medical devices with improved privacy," in *Proc. 10th ACM Conf. Embedded Netw. Sensor Syst.*, 2012, pp. 327–328.
[23] K. Singh and V. Muthukkumarasamy, "Authenticated key establishment protocols for a home health care system," in *Proc. 3rd Int. Conf. IEEE Intell. Sensors, Sensor Netw. Inf. (ISSNIP)*, Dec. 2007, pp. 353–358.
[24] G. Zheng, G. Fang, R. Shankaran, M. A. Orgun, and E. Dutkiewicz, "An ECG-based secret data sharing scheme supporting emergency treatment of implantable medical devices," in *Proc. IEEE Int. Symp. Wireless Pers. Multimedia Commun. (WPMC)*, Sep. 2014, pp. 624–628.
[25] L. Pycroft *et al.*, "Brainjacking: Implant security issues in invasive neuromodulation," *World Neurosurgery*, vol. 92, pp. 454–462, Aug. 2016.
[26] T. Denning, Y. Matsuoka, and T. Kohno, "Neurosecurity: Security and privacy for neural devices," *Neurosurgical Focus*, vol. 27, no. 1, p. E7, 2009.
[27] H. Rathore, "Bio-inspired approaches in various engineering domain," in *Mapping Biological Systems to Network Systems*. Springer, 2016, pp. 177–194.
[28] X. Hei, X. Du, S. Lin, I. Lee, and O. Sokolsky, "Patient infusion pattern based access control schemes for wireless insulin pump system," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 11, pp. 3108–3121, Nov. 2015.

[29] H. Rathore, A. Al-Ali, A. Mohamed, X. Du, and M. Guizani, "DLRT: Deep learning approach for reliable diabetic treatment," in *Proc. IEEE Globecom*, Dec. 2017, pp. 1–6.
[30] H. Rathore, L. Wenzel, A. K. Al-Ali, A. Mohamed, X. Du, and M. Guizani, "Multi-layer perceptron model on chip for secure diabetic treatment," *IEEE Access*, vol. 6, pp. 44718–44730, 2018.
[31] X. Hei, X. Du, S. Lin, and I. Lee, "PIPAC: Patient infusion pattern based access control scheme for wireless insulin pump system," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 3030–3038.
[32] X. Hei and X. Du, "Biometric-based two-level secure access control for implantable medical devices during emergencies," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 346–350.
[33] X. Du, Y. Xiao, M. Guizani, and H.-H. Chen, "An effective key management scheme for heterogeneous sensor networks," *Ad Hoc Netw.*, vol. 5, no. 1, pp. 24–34, 2007.
[34] X. Hei, X. Du, J. Wu, and F. Hu, "Defending resource depletion attacks on implantable medical devices," in *Proc. IEEE GLOBECOM*, Dec. 2010, pp. 1–5.
[35] X. Du, M. Guizani, Y. Xiao, and H.-H. Chen, "A routing-driven elliptic curve cryptography based key management scheme for heterogeneous sensor networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1223–1229, Mar. 2009.
[36] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, "IMDGuard: Securing implantable medical devices with the external wearable guardian," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 1862–1870.
[37] M. Zhang, A. Raghunathan, and N. Jha, "MedMon: Securing medical devices through wireless monitoring and anomaly detection," *IEEE Trans. Biomed. Circuits Syst.*, vol. 7, no. 6, pp. 871–881, Dec. 2013.
[38] T. Denning, K. Fu, and T. Kohno, "Absence makes the heart grow fonder: New directions for implantable medical device security," in *Proc. HotSec*, 2008.
[39] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," *SIGCOMM Comput. Commun. Rev.*, vol. 41, no. 4, pp. 2–13, Aug. 2011.
[40] Y. Xiao *et al.*, "A survey of key management schemes in wireless sensor networks," *Comput. Commun.*, vol. 30, nos. 11–12, pp. 2314–2341, Sep. 2007.
[41] X. Du, M. Guizani, Y. Xiao, and H. H. Chen, "Secure and efficient time synchronization in heterogeneous sensor networks," *IEEE Trans. Veh. Technol.*, vol. 57, no. 4, pp. 2387–2394, Jul. 2008.
[42] X. Du and H. H. Chen, "Security in wireless sensor networks," *IEEE Wireless Commun. Mag.*, vol. 15, no. 4, pp. 60–66, Aug. 2008.
[43] A. Beuter, M. S. Titcombe, F. Richer, C. Gross, and D. Guehl, "Effect of deep brain stimulation on amplitude and frequency characteristics of rest tremor in Parkinson's disease," *Thalamus Rel. Syst.*, vol. 1, no. 3, pp. 203–211, 2001.
[44] *Deeplearning4j*. Accessed: Oct. 18, 2017. [Online]. Available: https://deeplearning4j.org/lstm.html
[45] *Physionet*. Accessed: Oct. 18, 2017. [Online]. Available: https://physionet.org/physiobank/database/tremordb/
[46] *Functional Neurosurgery*. Accessed: May 10, 2018. [Online]. Available: http://www.functionalneurosurgery.net/programmingofneurostimulationdevices.htm
[47] H. Rathore, V. Badarla, and S. Shit, "Consensus-aware sociopsychological trust model for wireless sensor networks," *ACM Trans. Sensor Netw.*, vol. 12, no. 3, p. 21, 2016.
[48] T. Heida, E. C. Wentink, and E. Marani, "Power spectral density analysis of physiological, rest and action tremor in Parkinson's disease patients treated with deep brain stimulation," *J. Neuroeng. Rehabil.*, vol. 10, no. 1, p. 70, 2013.
[49] Accessed: May 14, 2018. [Online]. Available: http://www.jakob-aungiers.com/articles/a/LSTM-Neural-Network-for-Time-Series-Prediction
[50] F. Chollet. (2015). *Keras: Theano-Based Deep Learning Library*. [Online]. Available: https://github.com/fchollet. Documentation:. [Online]. Available: http://keras.io
[51] Theano Development Team. (2016). "Theano: A Python framework for fast computation of mathematical expressions." [Online]. Available: https://arxiv.org/abs/1605.02688

HEENA RATHORE received the bachelor's degree (Hons.) in computer science engineering from the College of Technology and Engineering, in 2010, and the Ph.D. degree (With Distinction) from the Computer Science and Engineering Department, IIT, India. She was a Tata Consultancy Services Research Scholar with IIT, India. She was a Visiting Scholar with Wichita State University. She was a Design Executive with Phosphate India Pvt. Ltd. She was a Guest Professor with The University of Texas, Austin, and an Assistant Professor with the SS College of Engineering, India. She is currently a Postdoctoral Researcher with the U.S.–Qatar Joint Collaborative Project between Temple University, USA, University of Idaho, USA, and Qatar University. She has published more than 30 papers in peer-reviewed conferences and journal papers in her field. She has authored *Mapping Biological Systems to Network Systems* (Springer). She was also featured on TedX, Qatar, held by TedXAlDafnaEd, Qatar. She is the Editor of professional and trade publications, such as *Microwave Journal* and *Indian Science Journal*, IndiaTechOnline and EverythingRF.com have written about her research within their publications. Likewise, journalists of major newspapers, such as the Times of India, Economic Times and India Today have written news stories about her original research and its significance. Her research interests include cryptocurrency, cyber-physical systems, deep learning, machine learning, security, distributed systems, wireless networks biologically inspired systems, and software-defined networks. She received several prestigious awards including the Graphical System Design Achievement Awards by National Instruments. She is invited as a Panelist, a TPC Member, and the Chair of multiple sessions. She is a Reviewer for many peer-reviewed journals and conferences in IEEE, IET, and Elsevier.

ABDULLA KHALID AL-ALI received the master's degree in software design engineering and the Ph.D. degree in computer engineering from Northeastern University, Boston, MA, USA, in 2008 and 2014, respectively. He is an Active Researcher of cognitive radios for smart cities and vehicular ad-hoc networks. He is currently the Head of the Technology Innovation and Engineering Education, College of Engineering, Qatar University. He has published several peer-reviewed papers in journals and conferences.

AMR MOHAMED received the M.S. and Ph.D. degrees in electrical and computer engineering from the University of British Columbia, Vancouver, Canada, in 2001 and 2006, respectively. He was an Advisory IT Specialist with the IBM Innovation Centre, Vancouver, from 1998 to 2007, taking a leadership role in systems development for vertical industries. He is currently an Associate Professor with the College of Engineering, Qatar University, and the Director of the Cisco Regional Academy. He has over 22 years of experience in wireless networking research and industrial systems development. He has authored or co-authored over 140 refereed journal and conference papers, textbook, and book chapters in reputed international journals and conferences. His research interests include wireless networking, and edge computing for the Internet of Things applications. He received three awards from IBM Canada for his achievements and leadership, and three best paper awards, latest from the 2015 IEEE/IFIP International Conference on New Technologies, Mobility, and Security, Paris. He serves as a Technical Editor for the *Journal of Internet Technology* and the *International Journal of Sensor Networks*. He has served as a Technical Program Committee (TPC) Co-Chair for workshops in IEEE WCNC'16. He has served as a Co-Chair for the technical symposia of international conferences, including Globecom'16, Crowncom'15, AICCSA'14, IEEE WLN'11, and IEEE ICT'10. He has served on the organization committee of many other international conferences as a TPC Member, including the IEEE ICC, GLOBECOM, WCNC, LCN and PIMRC, and as a Technical Reviewer for many international IEEE, ACM, Elsevier, Springer, and Wiley journals.

XIAOJIANG (JAMES) DU received the B.S. and M.S. degrees in electrical engineering from Tsinghua University, Beijing, China, in 1996 and 1998, respectively, and the M.S. and Ph.D. degrees in electrical engineering from the University of Maryland College Park, in 2002 and 2003, respectively. He is currently a Professor with the Department of Computer and Information Sciences, Temple University, Philadelphia, USA. His research interests include security, wireless networks, and systems. He has authored over 300 journal and conference papers in these areas and a book published by Springer. He is/was a Technical Program Committee Member of several premier ACM/IEEE conferences such as INFOCOM, from 2007 to 2019, IM, NOMS, International Communication Conference (ICC), GLOBECOM, Wireless Communications and Networking Conference (WCNC), BroadNet, and IPCCC. He is a Life Member of ACM. He received more than U.S. $5 million research grants from the U.S. National Science Foundation, Army Research Office, Air Force, NASA, the State of Pennsylvania, and Amazon. He received the Best Paper Award at the IEEE GLOBECOM 2014 and the Best Poster Runner-Up Award at the ACM MobiHoc 2014. He serves on the editorial boards for three international journals. He served as the Lead Chair for the Communication and Information Security Symposium of the 2015 IEEE ICC and a Co-Chair for the Mobile and Wireless Networks Track of the 2015 IEEE WCNC.

MOHSEN GUIZANI (S'85–M'89–SM'99–F'09) received the B.S. (With Distinction) and M.S. degrees in electrical engineering and the M.S. and Ph.D. degrees in computer engineering from Syracuse University, Syracuse, NY, USA, in 1984, 1986, 1987, and 1990, respectively. He held different academic and administrative positions with the University of Idaho, Western Michigan University, University of West Florida, University of Missouri-Kansas City, University of Colorado-Boulder, and Syracuse University. He is currently a Professor with the CSE Department, Qatar University, Qatar. He has authored nine books and more than 500 publications in refereed journals and conferences. His research interests include wireless communications and mobile computing, computer networks, mobile cloud computing, security, and smart grid. He also served as a member, the Chair, and the General Chair for a number of international conferences. He is a Senior Member of the ACM. Throughout his career, he received three teaching awards and four research awards. He was a recipient of the 2017 IEEE Communications Society WTC Recognition Award and the 2018 AdHoc Technical Committee Recognition Award for his contribution to outstanding research in wireless communications and ad-hoc sensor networks. He is currently the Editor-in-Chief of the *IEEE Network Magazine*. He serves on the editorial boards for several international technical journals and the Founder and the Editor-in-Chief of *Wireless Communications and Mobile Computing Journal* (Wiley). He guest edited a number of special issues in IEEE journals and magazines. He was the Chair of the IEEE Communications Society Wireless Technical Committee and the Chair of the TAOS Technical Committee. He served as the IEEE Computer Society Distinguished Speaker. He is currently the IEEE ComSoc Distinguished Lecturer.