Proposed Solutions for Security of Smart Traffic Lights using IoT and Machine Learning

L'GHDAICHE Sara

Network Telecoms and Electrical Engineering Department

University Ibn Tofail, National School of Applied Sciences Kenitra, Morocco

lghdaiche.sara@gmail.com

ADDAIM Adnane

Network Telecoms and Electrical Engineering Department

University Ibn Tofail, National School of Applied Sciences Kenitra, Morocco

addaim@gmail.com

EL HASSAK Imad

Network Telecoms and Electrical Engineering Department

University Ibn Tofail, National School of Applied Sciences Kenitra, Morocco

Imad.elhassak @gmail.com

Abstract **- The traffic management systems standards are being replaced by traffic lights modes, which automatically adjust control parameters and revise signal plans, and are now an integral part of modern road transport infrastructure. These advances of the Internet of Things (IoT), which allows communication and interaction with various devices in adaptive traffic signals, have been proven to be vulnerable to security breaches and could be easily exploited to allow an attacker to directly modify traffic signal indications. The vulnerabilities could allow full control of traffic control devices and could cause traffic disruption. In this article, a new deep learning model is proposed to analyze data of IoT smart cities. We offer a new model based on Long Short Term memory networks (LSTMs) for predicting anomalies in an intelligent traffic light. The proposed model shows promise and shows that the model can be used in other smart city prediction problems as well.**

Keywords - Traffic lights, Security, IoT, Long short term memory (LSTM), Smart city, Predicting anomalies.

I. INTRODUCTION

Due to the increase in the number of vehicles in cities, the traffic lights modes are replaced by the traffic management systems standards, which automatically adjust control parameters and revise signaling plans [1], are now part of modern infrastructure. These advances in the Internet of Things (IoT) which enables communication and interaction with various devices in the area of adaptive traffic lights has been proven that the IoT is vulnerable to security breaches and which could be easily exploited and which would allow an attacker to directly modify the indications of traffic lights. The vulnerabilities could allow complete control of the traffic control devices and could cause traffic disorder.

The Internet of Things (IoT) is a smart network that shares information on the Internet. IoT allows vehicles to collect information from the road unit and obtain information on the route, time and traffic details [2]. The growing number of IoT devices is changing rapidly as it crosses the total world population so the data generated by IoT devices is going to be huge. IoT is one of the most emerging technologies, but security and confidentiality are still considered as challenges in many fields of application because security problems in IoT networks are much more important with the increasing number of attacks.

Moreover, smart traffic devices face the following challenges:

- Work in real time.
- Dealing with a lot of vehicles using different communication models.
- Facing all failures and any attacks.
- Dealing with the transition time between the parties.

Nowadays some researchers are dealing with security issues in IoT, but as new technologies arrive, people are orienting more researches towards applications based on machine learning alongside that can solve the security problem in IoT, because before the calculation is done of information generated by an IoT application, it is necessary to pass through the verification process to avoid any malicious data or redundancy.

II. RELATED WORK

In this section, we look at some works that use new algorithms based on machine learning to manage security issues in IoT environments.

Currently, Deep learning is recognized as a relevant approach to intrusion detection in networks. The success of deep learning (DL) in various areas of big data has sparked several interests in the areas of cyber security [3].

The study presented in [4] found that NN was used to detect DoS attacks in IoT networks based on a multi-layer perception based control system.

Diro and al. [5] approached deep learning as a new intrusion detection technique due to its ability to extract high-level functionality for IoT. The authors proposed a deep learning-based IoT / Fog network attack detection system. Experience has shown that Distributed Attack Detection can better detect cyber-attacks than centralized algorithms due to sharing parameters and also demonstrated that the deep model has gone beyond traditional machine learning systems.

Nguyen and al. [6] Introduces an advanced detection mechanism based on a deep learning approach in the cloud environment and they are shown that their proposed learning model can achieve high precision in the detection and isolation of cyber-attacks and surpass other existing machine learning methods.

DL models are regarded as powerful models for showing excellent performance on difficult learning tasks [7]. There are many studies proposing solutions for the prediction problem of DL in the literature. LSTM which is a special type of DL is the state of the art recurrent neural network (RNN) for supervised temporal sequence learning [8]. LSTM has a structure of loops that memorize previous events to make better use of its input [9].

Deep learning for malicious traffic detection has gained several notable achievements with various network models. For example, the authors in [10] proposed a novel network-based anomaly detection method which extracts behavior snapshots of the network and uses deep autoencoders to detect anomalous network traffic emanating from compromised IoT devices.

However, the performance of the work primarily relies on several self-generated synthetic data sets, which may lack the diversity of data exchange. In another research work [11], the authors proposed a malware traffic classification method using CNN by considering traffic data as images. The work is one of the first attempts to apply a representation learning approach for malware traffic classification from raw traffic.

III. DIFFERENT TRAFFIC MANAGEMENT

Before using the attack detection model, the data processing in the system is divided into two types:

Local processing (Figure 3) is carried out by an agent installed at each intersection. It receives data from two sensors installed in the lanes of an intersection (figure 2) and from the central server. After data collection, the processing agent selects a solution from the optimization methods, and then the agent sends the new configurations to the traffic lights. Once the new configurations are defined, the collection and processing process will continue until a traffic problem occurs. In this case, a camera will take images and process them using Machine Learning algorithms (recognition and convolution) in order to detect the presence or absence of an accident at this intersection [12].

Central processing (Figure 3) does not require a lot of resources in terms of throughput. The central server receives a lot of data and then we use the concept of big data to process it, organize it and classify it according to the needs of the system. On the other hand, we use machine learning algorithms to process and analyse the images collected by the cameras in order to make decisions on the traffic situation in case of traffic problems (detect if there is an accident at an intersection or not) [12].

IV. DIFFERENT ATTACKS IN EACH LAYER OF IOT

Every layer of IoT is vulnerable to security threats and attacks. At every layer, IoT devices and services are vulnerable to Denial of Service (DoS) attacks, which render the device, resource, or network unavailable to authorized users.

This section provides a detailed analysis of the attack issues for each layer.

1. Perception Layer

There are three security concerns in the IoT perception layer [13]: first, the strength of the wireless signals, the signals of which are transmitted between the IoT sensor nodes, the effectiveness of which can be compromised by disturbing waves. Second, the sensor node in IoT devices can be intercepted by the owner and also by attackers, since IoT nodes generally operate in external environments, which involves physical attacks on sensors and IoT devices in which an attacker may damage the device. Third, the inherent nature of the network topology is dynamic because IoT nodes are often moved to different places.

The IoT perception layer mainly consists of sensors and RFID, due to which their storage capacity, their energy consumption and their computation capacity are very limited, which makes them sensitive to many types of threats and attacks. The malicious node injection attack was the most dangerous attack because it stops services and modifies data.

2. Network Layer

The network layer of the IoT is vulnerable to privacy attacks through traffic analysis, eavesdropping and passive surveillance. These attacks have a high probability of occurrence due to the mechanisms of remote access and data exchange of the devices. The network layer is very sensitive to human attack in the middle, which can be followed by eavesdropping. The key exchange mechanism in the IoT must be secure to prevent any intruder from listening and then committing identity theft. Attackers can also take advantage of the fact that everything is connected in order to obtain more information about users and to use this information for future criminal activities. The deepest attack is the most unsafe in the network layer. Because the attacker attracts all traffic to the base station and can launch other threats such as selective forwarding, packet modification, or drop packages [13].

3. Application Layer

There are many issues related to application security. Large amounts of connected devices that share data will cause significant overhead on the applications that analyze the data, which may have a significant impact on the availability of services. Among the software attacks, the worm attack is the most dangerous [13]. It is a self-replicating program that harms the computer by using security holes in software and network hardware. It can steal information or delete files from the system; it can also change passwords without notifying it and cause the computer to lock, etc. These attacks cause significant damage because they modify data, drop packets, steal private information and the encryption key.

V. SOLUTION APPROACH

A. Long Short Term Memory (LSTM)

LSTM is a type of Recurrent Neural Network (RNN) that is capable of learning long-term addictions. It was introduced in order to overcome the leakage gradient problem. In this neural network model, a memory block takes the place of each ordinary neuron in the hidden layer of the standard recurrent neural network [14].

The LSTM block shown in the following figure has an entry gate, a forgetting gate, and an exit gate which regulate the flow of information entering and leaving the cell. These doors block entry and exit as follows:

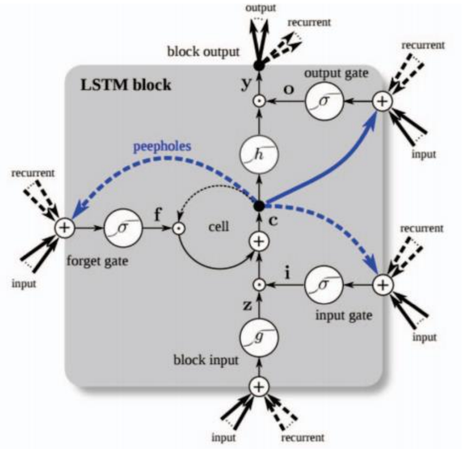

Figure 1. A Long Short-Term Memory Block [16]

LSTM has been applied to a variety of real world problems such as machine translation [17], speech recognition [18], and image recognition [19]. In this study, a new anomaly prediction model based on LSTM is proposed on IoT data.

B. Proposed anomaly prediction model

In this section, we will present our approach (see figure 3) to have a good prediction of traffic anomalies to secure traffic lights in smart cities. We will explain all the elements that must be brought together to optimize the security of traffic management systems with new techniques.

In this proposed anomaly prediction model, we propose a deep learning model composed of LSTM neural networks. According to this model, the network adopts the architecture which gives the best result.

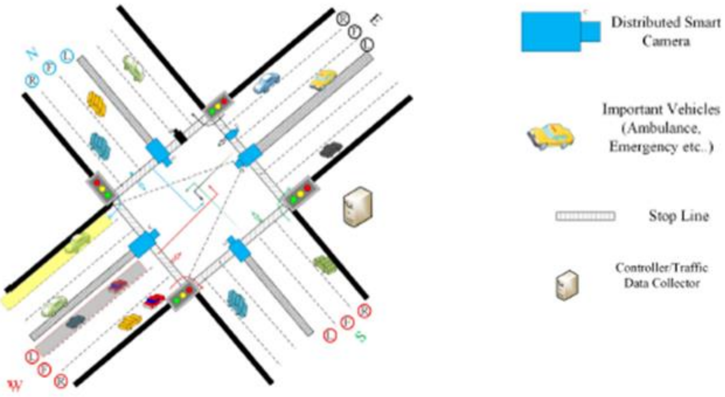
Distributed Smart Camera
Important Vehicles (Ambulance, Emergency etc..)
Stop Line
Controller/Traffic Data Collector
N
E
S
W

Figure 2. Distributed Smart-camera of IoT [1]

The first step of the processing system (see Fig. 3) is the collection of data from the IoT (Smart Camera) sensors installed in the streets (see Fig. 1) to determine the number of vehicles entering and exiting at an intersection. In addition to these sensors, there are others installed on public vehicles (Important Vehicles), these data collected from the traffic lights are among the most important parameters of this system.

After data collection, the next step is the processing of this data. In our system, we distinguish three stages of processing: the application of the Deep Learning Model, Labeling of this data and then taking the Decision. Basically, the model data is split into two parts: Training set and Test set.

Deep Learning Model (Figure.3), to create a new harmful traffic classification framework, LSTM is able to achieve this thanks to its closed cell. This closed cell has two states, open and closed, which make it act like a computer memory, as it makes decisions about what data it is allowed to write, read, and store in. This feature allows it to keep attack details in the training process and make detection decisions based on this information stored in the closed cell. Moreover, this algorithm detects DDoS attacks with high detection accuracy and low false alarm rates.

Labeling Unit (Figure 3) has been integrated into our proposed attack detection process. It is connected to the deep learning model and automatically receives the predicted data for evaluation. It's divide the data into two units, for example gives to normal information unit's (cars, public transport, ambulance,...) the number 0 and gives to the doubtful information unit's (anomalies or attacks) the number 1, in order to send it to the decision unit which makes the decision to avoid units that are equal to 1.

In the proposed model, a certain number of sequential values are taken into account and predictions are made for next step, denoted Eq. (1).

$$a(t-n),\dots,\ a(t-2),\ a(t-1),\ a(t)\ = \mathbf{a}(t+1) \qquad (1)$$

Where $a(t-n),\dots, a(t-2),a(t-1),a(t)$ are the observed values (input sequence) and $\mathbf{a}(t+1)$ is the predicted value.

The LSTM-based anomaly prediction model takes advantage of its advantages of storing long historical data and achieving higher prediction accuracy even though it has a simple network structure. Consequently, the employment of the LSTM based prediction model to the IoT data is effective and promising.

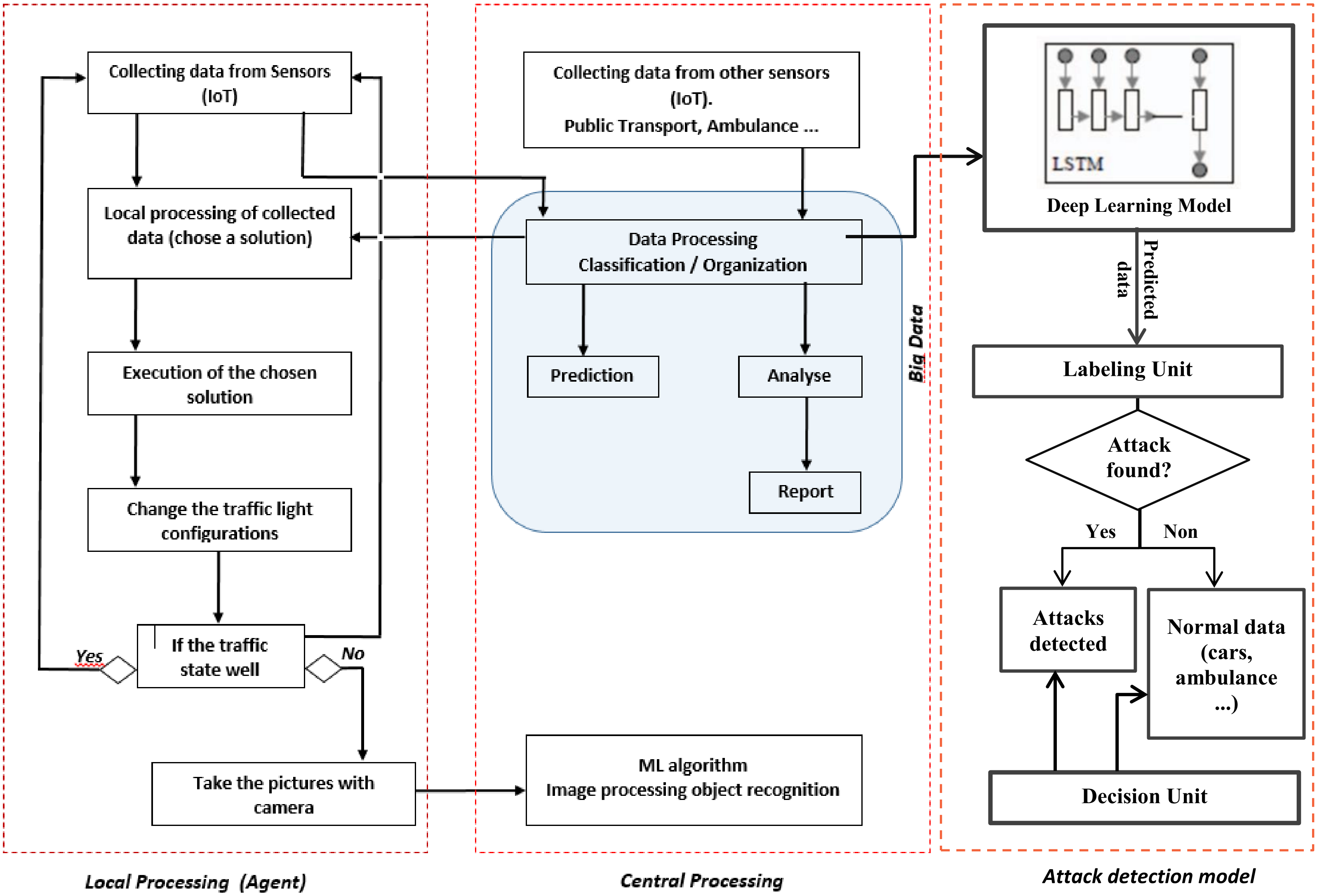
Collecting data from Sensors (IoT)
Local processing of collected data (chose a solution)
Execution of the chosen solution
Change the traffic light configurations
Yes
If the traffic state well
No
Take the pictures with camera
Collecting data from other sensors (IoT).
Public Transport, Ambulance ...
Data Processing
Classification / Organization
Prediction
Analyse
Report
Big Data
ML algorithm
Image processing object recognition
LSTM
Deep Learning Model
Predicted data
Labeling Unit
Attack found?
Yes
Non
Attacks detected
Normal data (cars, ambulance ...)
Decision Unit
Local Processing (Agent)
Central Processing
Attack detection model

Figure 3. Proposed Anomaly Prediction Model

VI. Conclusion

In this article, we have proposed an anomaly prediction model for traffic classification using the Long-Term Memory (LSTM) and Embedding Word Network model. The main advantage of the proposed framework is that it does not require pre-processing packets, thus improving the acceleration of detection. This solution may be changed in the future as the popularity of deep learning attracts more attackers to exploit its vulnerabilities for hacking. Preventing adversary models against deep learning is thus one of the most promising security research topics.

References

1. Willy Carlos Tchuitcheu, Christophe Bobda, Md Jubaer Hossain Pantho “Internet of smart-cameras for traffic lights optimization in smart cities”.
2. H. Wang, J. Gu, S. Wang, An effective intrusion detection framework based on svm with feature augmentation, Knowl. Based Syst. 136 (2017) 130–139.
3. Kulkarni, R.V., Venayagamoorthy, G.K., 2009. Neural network based secure media access control protocol for wireless sensor networks. In: Proc. Int. Joint Conf. Neural Networks. June, Atlanta, GA, pp. 3437–3444.
4. H. H. Nguyen, N. Harbi, and J. Darmont, “An efficient local region and clustering-based ensemble system for intrusion detection,” in Proc.
5. A .A. Diro, N. Chilamkurti, Distributed attack detection scheme using deep learning approach for internet of things, Future Gener. Comput. Syst. 82 (2018) 761–768.
6. Nguyen, K. K., Hoang, D. T., Niyato, D., Wang, P., \& Dutkiewicz, E. (2018). Cyberattack detection in mobile cloud computing: A deep learning approach. IEEE.
7. I. Sutskever, O. Vinyals, and Q. V. Le, "Sequence to Sequence Learning with Neural Networks," Computation and Language, 2014.
8. F. J. Gomez and J. Schmidhuber, "Co-Evolving Recurrent Neurons Learn Deep Memory POMDPs," in 7th annual conference on Genetic and evolutionary computation, Washington, USA, 2005.
9. Y. Tang, J. Xu, K. Matsumoto, and C. Ono, "Sequence to-Sequence Model with Attention for Time Series Classification," presented at the IEEE 16th International Conference on Data Mining, 2016.
10. Meidan, Y.; Bohadana, M.; Mathov, Y.; Mirsky, Y.; Shabtai, A.; Breitenbacher, D. N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders. IEEE Pervasive Comput. 2018, 17, 11–22.
11. Wang,W.; Zhu, M.; Zeng, X.; Ye, X.; Sheng, Y. Malware Traffic Classification Using Convolutional Neural Networks for Representation Learning. In Proceedings of the 31st International Conference on Information Networking, Da Nang, Vietnam, 11–13 January 2017; pp. 712–717.
12. Elhassak, Addaim, “ Proposed Solutions for Smart Traffic Lights using Machine Learning and Internet of Thing”.
13. Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul, Imran Zualkernan “ Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures”.
14. Z. C. Lipton, J. Berkowitz, and C. Elkan, "A Critical Review of Recurrent Neural Networks for Sequence Learning," 2015, 2015.
15. K. Greff, R. K. Srivastava, J. Koutn´ık, B. R. Steunebrink, and J. Schmidhuber, "Lstm:A Search Space Odyssey," presented at the IEEE Transactions on Neural Networks and Learning Systems, 2016.
16. D. Bahdanau, K. Cho, and Y. Bengio, "Neural Machine Translation by Jointly Learning to Align and Translate," in International Conference on Learning Representations, 2014.
17. A. Graves, A.-R. Mohamed, and G. Hinton, "Speech recognition with deep recurrent neural networks," presented at the 2013 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2013.
18. J. Donahue, L. A. Hendricks, S. Guadarrama, M. Rohrbach, S. Venugopalan, K. Saenko, et al., "Long Term Recurrent Convolutional Networks for Visual Recognition and Description," Conference on Computer Vision and Pattern Recognition(CVPR), 2015.
19. A. Shahid, B. Khalid, S. Shaukat, H. Ali, M. Y. Qadri, Internet of Things Shaping Smart Cities : A Survey,

Springer International Publishing, Cham, 2018, pp. 335{358.

20. H. Sak, A. Senior, and F. Beaufays, "Long short-term memory recurrent neural network architectures for large scale acoustic modeling,", 2014.