ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 4, No. 5, 97-103 (2019)

www.astesj.com

Special Issue on Advancement in Engineering and Computer Science

ASTESJ

ISSN: 2415-6698

Toward a Smart Campus Using IoT: Framework for Safety and Security System on a University Campus

Alghamdi Abdullah[*,1], Mohammed Thanoon[2], Anwar Alsulami[3]

[1]*Information Systems Department, Najran University, Najran, Saudi Arabia*

[2]*Electrical and Computer Eng. Dept., Tennessee State University, Nashville, USA*

[3]*Department of Mechanical Eng., Jazan University, Jazan, Saudi Arabia*

ARTICLE INFO

Article history:
Received: 17 May, 2019
Accepted: 09 July, 2019
Online: 03 September, 2019

Keywords :
IoT
Smart Campus
Safety and Security

ABSTRACT

Recently, there is an enormous research on the smart campus concept due to the revolution of the IoT technologies. The motivation of this paper is to: reinforce the safety on campus, reduce the cost, and take one step forward toward a University smart campus. In this paper, we are not only proposing a framework that would act as an instantaneous responder, but we also provide a glimpse of the evolving research on smart campus. In addition, we explore the challenges, and highlight the future work regarding this on-the-spot responder system.

1. Introduction

The smart campus concept has been the main focus of many researchers recently due to the valuable insights gained toward developing smart cities. The university campus theoretically is a small city where it delivers variant services to variant users. There are several factors that attract the investigators to study the smart campus including: delivering high quality services, protecting the environment, and saving the cost. The internet of things is a fundamental part of the smart campus, and it is inescapable getting it invoked.

The internet of things is a communication paradigm that gained its tenacity from its capability of connecting variety of everyday life objects to the internet. These objects include, but not limited to, sensors, robots, security locks, alarms, drones, appliances, smart grid systems, office equipment and so on. Even though IoT is in its early stages, there are many applications and standardization that has been developed in many domains including: home automation, smart grids, water and waste management, traffic control, smart vehicles, healthcare assistance, and industrial automation. Moreover, the realization of the IoT network is facing two main challenges. First, technical challenges because of IoT novelty and heterogeneous nature. Second, business challenges due to the lack of complete and approved business model that would encourage investments.

In this paper, we are proposing a safety and security framework based on the IoT which would enhance the safety on a university campus. The work in this paper is not only an extension of the investigation originally presented at the 2016 International Conference on Future Internet of Things and Cloud (FiCloud) [1], but we also propose a new system, and identify the limitations and research opportunity in this field.

The safety on a university campus is a growing concern among the campus community across the U.S. and across so many other countries due to the horrific crimes and mass shooting committed, lately. Regardless of whether the campus is rural or urban, large or small, significant number of people on campus seems to be reluctant to walk out at night alone [2]. According to Clery Center for security on campus [3], the crimes committed by students on campus is about 80% of the overall crime number. For example, Tennessee State University (TSU) is considered about an average in crime rates [4]; However, there were recent cases which saddened TSU community such as the shooting in 2015 that killed one, and injured three students [5]. Figure 1 shows statistics of the crimes committed on post high school education campuses in the United States over the period of 2015 to 2017 [6]. Our proposed system will not only enhance the safety, but also it would reduce the cost, make efficient use of resources, and

*Alghamdi Abdullah, Assistant Professor, IS Dept., NU, Najran, Saudi Arabia.
Email: aaalghamdi@nu.edu.sa

become one step closer toward a smart campus by utilizing the recent advances in technology.

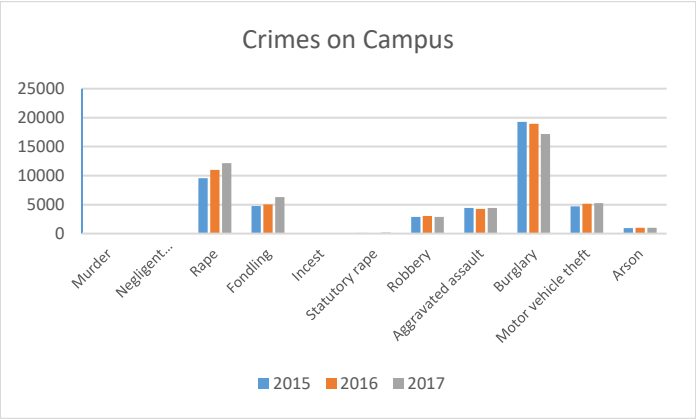

Figure 1 Statistics of The Crimes Committed on more than 11000 Campuses [6].

2. Smart Campus and Its Applications

The smart campus market springs from being a diverse environment regarding the services conveyed and the recipients of these services. The impact of conveyed services is not limited to the academic aspect, but also the social, financial, and environmental aspects. We can categorize the current research in smart campus into four main areas: intelligent buildings, campus smart grid, learning environment, and other applications. Figure 2 shows the context of a smart campus, its impacts, and many examples of its applications. On the rest of this section, we will present the research being done toward achieving a smart campus.

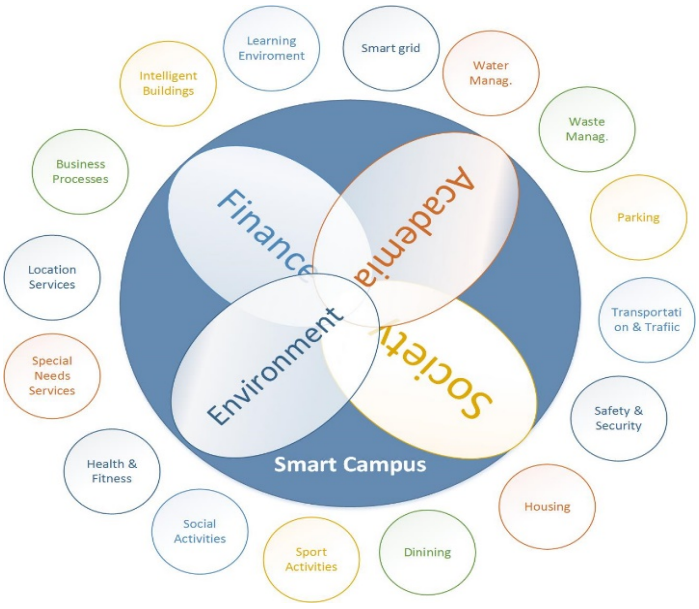

Figure 2 Impacts and Applications of Smart Campus Concept [1].

2.1. The Intelligent Buildings

Given that there is no de facto guide which would lead the people in the construction industry on how to build an intelligent building, a novel approach would be the plan to achieve the stakeholders' goals [7]. The planners need to focus on two main aspects. First, Information and Communication Technology (ICT) infrastructure where at least one fast backend network is needed for both business and building systems. Servers and variant sensors are essential part of the automation process of buildings. Sensors routine includes, detecting carbone dioxide levels in buildings, monitoring building stress, adjusting temperature, turning off the services in empty spaces, and measuring humidity and pollution levels [8,9]. Second, reporting and collaboration between various department is crucial to improve business processes and workflow, and it can be done by sharing information and reports, and enhancing communication [7]. The reports include building occupancy, staff attendance, patterns of utility usage, real-time warnings, energy usage, and so on. Knowing that the productivity gets increased by boosting the comfort of the community on campus, the stakeholders would make that as one of their goals [10].

2.2. Campus Smart Grid

Smart grid "is an opportunity to use new information and communication technologies (ICTs) to revolutionize the electrical power system" [11]. There are many universities adopting smart grids such as Oregon State University, which integrated Synchrophasor technology to have better monitoring and alarming system; however, the optimized results are not realistic due to the fact that this technology is relatively new and needs further studies [12]. In case of failures with SCADA, Santos *et al.* [13] suggests an automation process of power restoration using Open Platform Communications (OPC) protocol, and to characterize detection, isolation, and self-healing. Examining demand patterns, implementing a self-organized mapping (SOM), which is favored load profiling algorithm, and analyzing the current grid to provide a methodology and recommendations for smart microgrid in a university campus are discussed in [14,15]. Web-based systems on a cloud platform are introduced in: [16] for the analysis of energy consumption and behavior patterns, [17] for the purpose of controlling the demand response, and [18] for forecasting of future demand using machine learning (ML) models. Bracco *et al.* [19] propose a quantifying method for the usage of primary energy, predict CO2 emissions cut, and assess the cost reduction at the University of Genoa campus. Finally, IoT made it possible to control and monitor the energy consumption by users, identify energy draining devices, and suggests actions to optimize their behavior.

2.3. The Learning Environment

Given that the primary ambition of e-learning systems is to provide an articulated learning environment for learners based on their aspirations, knowledge, and talent, Wang *et al.* [20] characterize the learning process in an intelligent environment as a recursive process of four stages: learning, assessment, interaction, and analysis. Several papers published in this area including [21] which proposes students profiling based on their behavior over on-campus social network to provide a context-based personalized learning experience to achieve a ubiquitous learning (uLearning); however, additional study in terms of

learners' behavior and content design would exaggerate the benefit of such system. Microsoft and MIT started a research collaboration to achieve an intelligent campus, so called (MIT iCampus) [22]. This collaboration resulted in developing several intelligent systems including: class communicator system (CCS) to overcome communication issues between instructors and students, and class learning partner (CLP), and to provide an exercises and instant feedback during the class. Finally, given that mobile phones, tablets, laptops, and other wearable devices are among the most prominent devices that have influenced this universe [23], and utilizing them in education is inevitable.

2.4. Other Applications

Even though they do not get enough attention, there are plenty of other applications where IoT can be utilized to dramatically change campus to a smart one such as: waste and water management, parking, voting, safety and security, and so on. Regarding waste management, many papers published recently including [24-26] which generally suggest planting sensors at the bins, and waste trucks that collect real-time data for analysis, and a system would use the collected data to suggest better cleaning schedule and a superior and cost-effective route for waste contractors.

One the other hand, Mudumbe and Abu-Mahfouz [27] present a user-centric smart water management system which represent consumption in visual graphs to increase awareness. Gabrielli *et al*. [28] describe a sustainable prototype for smart metering devices and the associated network. Despite the feasibility of the project, the focus of their experiment is to build a sustainable metering device. Moreover, the authors [29,30] demonstrate: a parking guidance system for the parking building, and an electronic voting system that uses RFID technology for the authentication process, respectively.

Keeping in mind that most of recent work is focused on energy, learning environment, and intelligent buildings, the safety and security did not attract the attention of researchers; however, the intrinsic need of: better safety, instantaneous response to emergency, and cost effective solution on campuses actuated our team to investigate this area.

3. Safety and Security System

In this section, we will describe our system in details. At first, we will show the overall architecture of the system followed by the technique that will be used to deploy the sensors. Considering four different types of undesirable incidents: gun possession, assault, burglary and firing arms, we will show how to detect such suspicious activity. After that, we will show how to detect and track the suspect until the backup team arrives to the scene.

3.1. System Architecture

The safety and security system work with a variety of devices including: cameras, microphone sensors, glass break sensors, Raspberry Pi boards (RPis), a drone, and a server connected to the safety and security Operation Control Center (OCC) on campus. Figure 3 shows the general architecture of the system. To avoid overwhelming one server by making it process all the data collected by sensors across the campus, we would use the RPis to accomplish a distributed data processing architecture. Taking advantage of its cheap cost, the RPis would be used to process images, voices and other collected data by attached sensors. In case of detecting suspicious activity, the RPi would notify the server which will identify the location of the RPi using table for mapping the RPi's ID and its predefined location. The server would trigger the alert, identify the fastest route to the incident location, and instruct the drone to observe the situation, and wait for further actions.

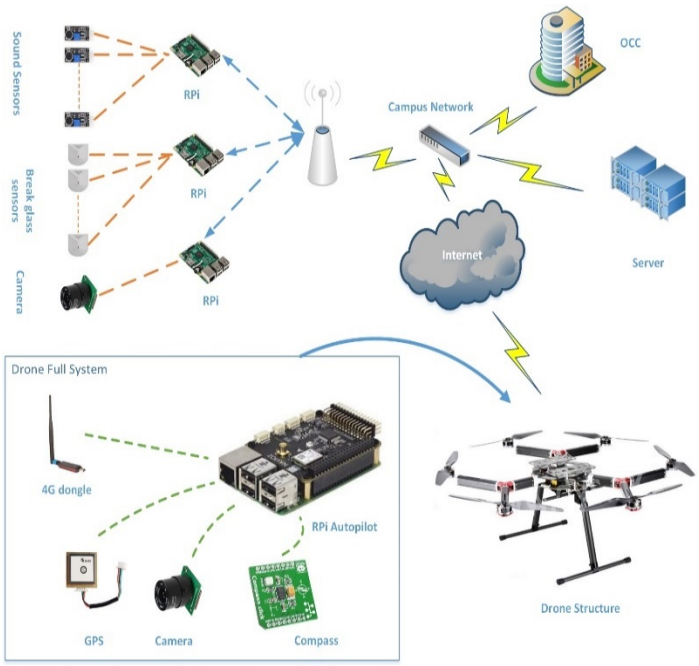

Figure 3 System Architecture

A sophisticated and robust drone need to be used as an instantaneous responder to observe the situation, and send live updates to the OCC for assessment and evaluation. The drone's autopilot would be attached to: a 4G dongle for internet connection, a GPS, a camera, and a compass.

3.2. Sensors Deployment

Since we have different types of sensors and our system depend on them, we need to deploy them carefully. The deployment technique is planned attentively to achieve two goals: to be cost effective regarding the number of sensors, and to avoid degrading the effectiveness of the system by deploying less sensors than required. The cameras would be deployed at parking lots, sidewalks, and buildings' entrances. The glass break sensors need to be deployed inside the buildings. Because one sensor covers around 25 feet, we would deploy one sensor per room wherever applicable. Finally, we decided to choose a microphone that covers 20 to 30 feet in a spherical area such as QSPMIC microphone by Q- See.

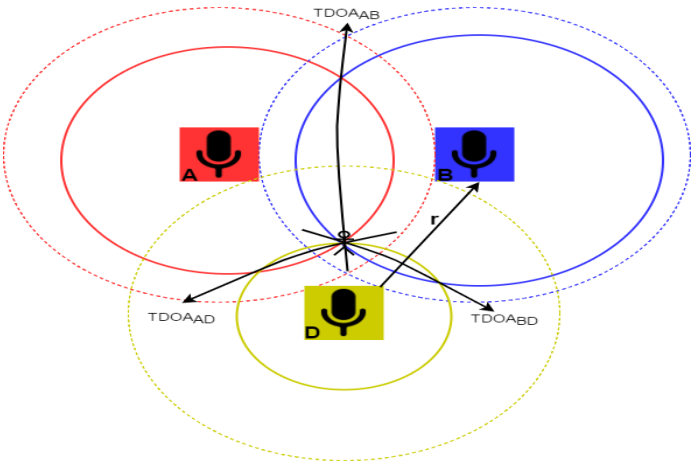

Figure 4 Sound Sensors Deployment

Figure 4 shows the way of planting the sound sensors where every sensor is planted at the end of the previous sensor coverage. Thus, the horizontally and vertically distance between sensors is equal to the radius of the coverage area (r). The sound source location can be determined using the Time Difference of Arrival (TDOA) or Multilateration (MLAT) method [31]. TDOA is an algorithm used to determine the location of the sound source by calculating the differences in arrival time of the sound at spatially separated sensors. The time difference of arrival of sound at different sensors must be known and processed at the central location. When the possible distance of the source from each sensor is drawn, it creates a hyperbolic curve. The location of the sound source lies in the intersection of all the hyperbolas from different sensors. This method works quite accurately for relatively static sources. If dynamic sources to be tagged, modified TDOA can be used [32].

3.3. Suspicious Activity Detection

The proposed system considers four different undesirable incidents to prove its effectiveness which are: gun possession, assault, burglary, and firing arms. The following paragraphs will study these scenarios in details.

Gun possession would be caught using the cameras distributed all over the campus parking lots, entrances, and sidewalks. The Raspberry Pies (RPis) attached to cameras would be able to detect guns automatically using Convolutional Neural Networks (CNNs) [33]. CNN is the state of the art technology in computer vision and it has been proven as a reliable architecture in object detection, giving its high accuracy with sufficient training. CNN is a special case of Neural Networks that apply the convolution operation to an input image for the purpose of feature extraction; however, the usage of the convolution operation demands high computational time, which is a challenge in our environment, knowing that we are using limited, low-energy devices. Fortunately, Iandola *et al.* [34] were able to achieve a smaller CNN architecture that performs the same accuracy as the AlexNet-level on ImageNet with fifty times fewer parameters, and they named it SqueezeNet. As a result, the SqueezeNet can be used on almost any controller or embedded computers. On RPis, it takes SqueezeNet approximately 2 seconds to process an image, which is enough time to: detect a person with a gun on a sidewalk, issue an alarm on the building, automatically close the inner doors of buildings, and notify the safety and security OCC on campus. Using a significant number of images of different types of guns, the SqueezeNet would be trained. The trained model would be deployed on the RPis wherever the cameras are applicable. After the detection of the gun, the RPis would alert the server. Using the predefined mapping between RPis and locations, the server would be able to instantaneously deduce the location of the gunman, plan the fastest route for drone, and instruct the drone to find and tracking the gunman until a backup team arrives to the scene.

There are some cases where the gun would not be detected by the distributed cameras. Therefore, we introduce another method for detection which is by detecting the sounds of firing arms. Usually, firing the arms and assault crimes are accompanied by sounds such as the sounds of gunshots and yelling for help. In case of any of these undesirable incidents happened, the microphones attached to RPis would catch the accompanied signals, and pass it to the neural network to identify if there is any suspicious activity. Since the CNN is proven to be effective in speech recognition [35], likewise, the SqueezeNet architecture would be used here too. Gunshots and yelling for help spectrograms would be used to train the network, and the pre-trained model would be deployed on the RPis. Similar to the previous scenario when the detection happens, the RPis would notify the server. Then, the server would identify the location of the incident and instruct the drone to observe the situation.

For burglary detections, we are using a glass break sensors which are connected to RPis. By listening to acoustical frequencies generated when a glass gets broken, the sensor would alert the RPi over the wireless which would lead to issuing an alarm to the server. Because the RPi mapped the sensor with its location on the building, the server would send the drone to that location to give real-time updates of the broken window. This would be important in case the burglar tried to run away because the drone can always detect and track people on the scene. Meanwhile, the OCC room should have sent a backup team to that room to investigate the situation.

3.4. Target Detection and Tracking

As soon as the drone arrives into the scene, it has to detect and track the suspect. To add more capability, our algorithm would allow two methods of detection: manually and automatically based on the situation. Figure 5 shows the general flowchart of target detection and tracking process. Upon the arrival of drone, it would start: capturing videos frames, notifying the OCC with updates, and analyzing the captured frames for detection of the suspect. Knowing that CNN requires high computation demand, Histogram Oriented Gradient (HOG) [36] would be used to detect upright persons in the scene. Because we need to reduce the computation overhead of the RPi on drone, we would analyze only five frames out of the twenty-five frames per

second that the camera can detect. If there is more than one upright person on the scene, the system would allow the OCC to decide which one to track. Otherwise, the drone will track the detected target. Regardless of the method used to detect the target, the drone will keep the target on its camera frame center, while the OCC will get real-time updates of the location which would be shown on an interactive map. Because we don't want to overwhelm the drone's connection to the internet, the OCC will get few captured frames only.

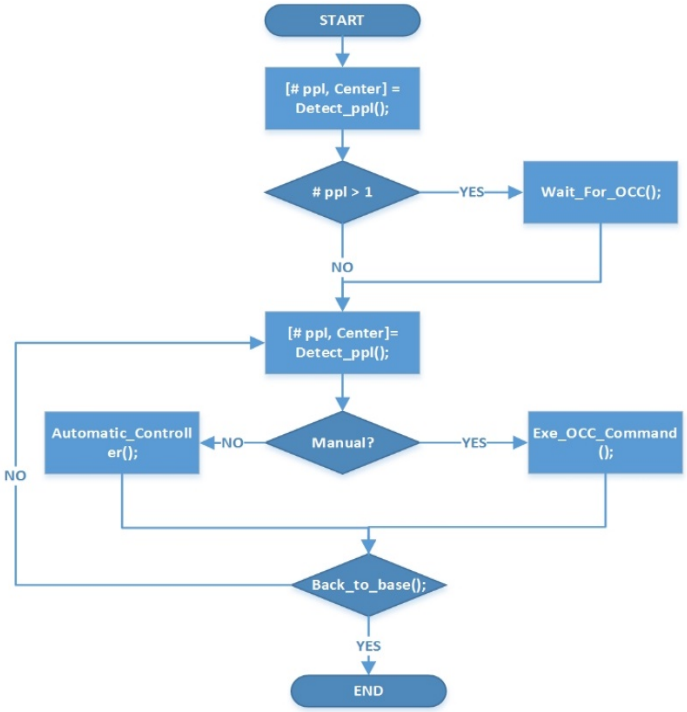

Figure 5 Target Detection and Tracking Flowchart

For the tracking, our system would allow the manual tracking of the suspect where the OCC officer can remotely control the drone without the need for frames analysis; however, this would require a high speed internet because the OCC needs a live streaming to be able to remotely control the drone. In case of automatic tracking, the optical flow method and its estimation using the Lucas-Kanade method will be used to track the suspect at the first frame only of every second [37,38]. The method works as the following: consider a pixel *I(x,y,t)* at the first frame, and it moves by distance *dx, dy,* in the frame that is compared to which is taken at *dt*. Because we are tracking the same person on real time, we assume the intensity does not change.

$$I(x, y, t) = I(x + dx, y + dy, t + dt) \quad (1)$$

by taking Tylor series approximation, and dividing by *dt*, we get:

$$f_x u + f_y v + f_t = 0 \quad (2)$$

$$f_x = \frac{\partial f}{\partial x}; \quad f_y = \frac{\partial f}{\partial y} \quad (3)$$

$$u = \frac{dx}{dt}; \; v = \frac{dy}{dt} \quad (4)$$

Then, using the Lucas-Kanade method, the final solution will be:

$$\begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} \sum_i fx_i^2 & \sum_i fx_i fy_i \\ \sum_i fx_i fy_i & \sum_i fy_i^2 \end{bmatrix}^{-1} \begin{bmatrix} -\sum_i fx_i ft_i \\ -\sum_i fy_i ft_i \end{bmatrix} \quad (5)$$

Then, the drone will move to the desired direction to make u, and v in its frame center. This method will be repeated once every second. Because we are capturing from the drone, the capture has a wide area where the suspect is in the center of the frame. It is less likely that the suspect will be able to go beyond the area of the drone's camera in one second. So, we are processing one frame per second only, and to avoid overwhelming the RPi with computation demands. Figure 6 illustrates the detection and tracking process, and the movement of the drone.

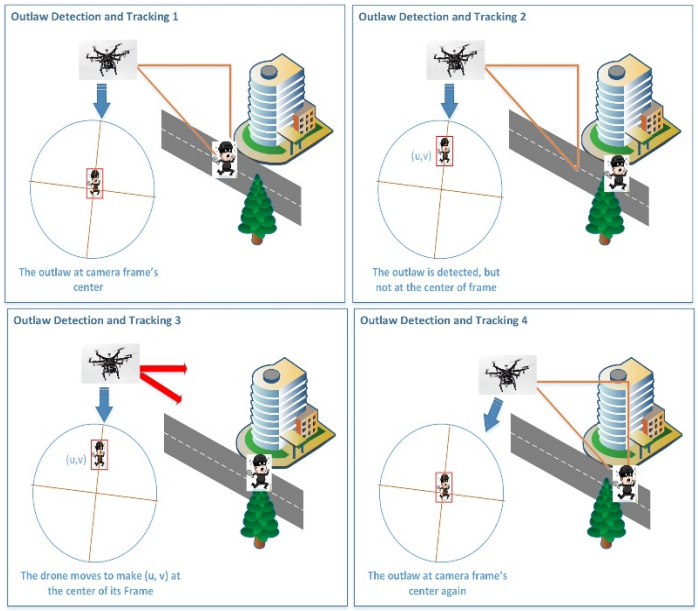

Figure 6 Target Detection and Tracking

4. Challenges and Future Work

Basically, the proposed safety and security framework inherited the obstacles that are facing the smart campus market which we can summarize in three areas: technical, financial, and political.

The technical barriers can be observed from the following perspectives: security, privacy, and configuration [1]. Being able to planet a massive number of low-energy and wirelessly connected devices on campus and meeting the security requirements is a problematic task due to the heterogeneous and intensive communication environment. Giving that we are utilizing various types of sensors, the privacy of people on campus is an issue where we need to be absolute that nobody can misuse the system to invade the people's privacy. Adopting the safety and security system on campus would result in using hundreds if not thousands of sensors which can be an enormous burden to configure them manually. Certainly, new ways of the automated configuration of IoT devices need to be thoroughly investigated.

In general, the smart campus market is facing financial difficulties giving that the limited resources of universities, regardless of immature experiences here and there. Even though the proposed system would save the university tons of many regarding the number of security officers on the long term, the initial investment is an impediment to the implementation of this system.

Regarding political hindrances, this system would need a waiver of some restrictions for unmanned aerial vehicles (UAV) by the Federal Aviation Administration (FAA), in the United States or such agencies in other countries, such as: the maximum altitude of 400 feet above ground level, visual line of sight, daylight only operations and some others [39]. Also, the system may face forceful opposition from people on campus and nearby neighborhoods regarding the invasion of their privacy. Even though it is almost inconceivable, the opposition of anti-tech security officers is a possible hindrance that needs to be considered.

After finalizing the implementation, our work opens the doors for researchers to improve the capability of this system to achieve optimum performance. The detection of outlaws during night-time and tracking them is a possible area of improvement. Moreover, the profiling of crimes respecting the hotspots, timings, and frequent suspicious activities using data collected by sensors would provide copious information about the crimes. The refined information would lead to crimes' prediction and prevention, eventually. Reducing the time between incident and arrival of drone is another area of improvement. Arming the drone with stun gun shocks could be considered for improvement. In addition, finding ways to avoid outlaws targeting the drone such as working on a bulletproof drone structure and trying to balance that with the speed of the drone is another area of improvement.

5. Conclusion

After presenting the recent work in smart campus technologies using IoT, we proposed a safety and security framework tailored to fit any university campus that would like to take advantage of recent advances in technology. The proposed framework would act as an instantaneous responder to incidents that could happen on campus. The proposed system is a good tool that would not only detect the incidents, but also it can track the outlaws even outside the campus until a backup team arrive to the scene. Also, we discussed the challenges of the system from three different perspectives: technical, and financial, and political. Finally, we highlighted the future work for this system to achieve its optimum performance.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] A. Alghamdi and S. Shetty, "Survey Toward a Smart Campus Using the Internet of Things," in *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, 2016, pp. 235–239.

[2] A. L. Ball, "Students Fear Venturing Out Alone at Night on Campus.," *The New York Times*, 20-Jul-2012.

[3] "Clery Center For Security On Campus." [Online]. Available: http://clerycenter.org/. [Accessed: 25-Dec-2018].

[4] College Factual, "Tennessee State University Crime," *College Factual*, 20-Feb-2013. [Online]. Available: http://www.collegefactual.com/colleges/tennessee-state-university/student-life/crime/. [Accessed: 25-Dec-2018].

[5] N. N. Alund, "Two men in custody in 2015 TSU fatal campus shooting," *The Tennessean*. [Online]. Available: http://www.tennessean.com/story/news/crime/2016/08/23/two-people-custody-2015-tsu-campus-shooting/89211076/. [Accessed: 25-Dec-2018].

[6] U.S. Department of Education, "Campus Safety and Security." [Online]. Available: http://ope.ed.gov/campussafety/#/. [Accessed: 25-Dec-2018].

[7] S. Hipwell, "Developing smart campuses #x2014; A working model," in *2014 International Conference on Intelligent Green Building and Smart Grid (IGBSG)*, 2014, pp. 1–6.

[8] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, Feb. 2014.

[9] J. P. Lynch, "A Summary Review of Wireless Sensors and Sensor Networks for Structural Health Monitoring," *The Shock and Vibration Digest*, vol. 38, no. 2, pp. 91–128, Mar. 2006.

[10] W. Kastner, G. Neugschwandtner, S. Soucek, and H. M. Newmann, "Communication Systems for Building Automation and Control," *Proceedings of the IEEE*, vol. 93, no. 6, pp. 1178–1203, Jun. 2005.

[11] A. B. M. S. Ali, Ed., *Smart Grids Opportunities, Developments, and Trends*. London: Springer London, 2013.

[12] C. Huo, J. Song, K. Wagner, G. Harold, and E. Cotilla-Sanchez, "Integrating synchrophasor technology with the Oregon State University campus smart grid project," in *2014 IEEE Conference on Technologies for Sustainability (SusTech)*, 2014, pp. 125–129.

[13] L. A. Santos *et al.*, "Towards a smart grid to the university campus of the federal university of Cear??," in *2015 IEEE 13th Brazilian Power Electronics Conference and 1st Southern Power Electronics Conference (COBEP/SPEC)*, 2015, pp. 1–6.

[14] I. P. Panapakidis, T. A. Papadopoulos, G. C. Christoforidis, and G. K. Papagiannis, "Analysis of the electricity demand patterns of a building in a university Campus," in *2013 12th International Conference on Environment and Electrical Engineering (EEEIC)*, 2013, pp. 382–387.

[15] R. M. González, T. A. J. van Goch, M. F. Aslam, A. Blanch, and P. F. Ribeiro, "Microgrid design considerations for a smart-energy university campus," in *Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), 2014 IEEE PES*, 2014, pp. 1–6.

[16] V. Nikolopoulos, G. Mpardis, I. Giannoukos, I. Lykourentzou, and V. Loumos, "Web-based decision-support system methodology for smart provision of adaptive digital energy services over cloud technologies," *IET Software*, vol. 5, no. 5, pp. 454–465, Oct. 2011.

[17] H. Kim, Y. J. Kim, K. Yang, and M. Thottan, "Cloud-based demand response for smart grid: Architecture and distributed algorithms," in *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2011, pp. 398–403.

[18] Y. Simmhan *et al.*, "Cloud-Based Software Platform for Big Data Analytics in Smart Grids," *Computing in Science Engineering*, vol. 15, no. 4, pp. 38–47, Jul. 2013.

[19] S. Bracco, F. Delfino, F. Pampararo, M. Robba, and M. Rossi, "Economic and environmental performances quantification of the university of Genoa Smart Polygeneration Microgrid," in *Energy Conference and Exhibition (ENERGYCON), 2012 IEEE International*, 2012, pp. 593–598.

[20] M. Wang and J. W. P. Ng, "Intelligent Mobile Cloud Education: Smart Anytime-Anywhere Learning for the Next Generation Campus Environment," in *2012 8th International Conference on Intelligent Environments (IE)*, 2012, pp. 149–156.

[21] Y. Atif and S. Mathew, "A Social Web of Things Approach to a Smart Campus Model," in *Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing*, 2013, pp. 349–354.

[22] "iCampus," *iCampus*. [Online]. Available: http://icampus.mit.edu/. [Accessed: 05-Oct-2018].

[23] V. G. Cerf, "Prospects for the Internet of Things," *XRDS*, vol. 22, no. 2, pp. 28–31, Dec. 2015.

[24] T. Anagnostopoulos, A. Zaslavsky, and A. Medvedev, "Robust waste collection exploiting cost efficiency of IoT potentiality in Smart Cities," in

2015 International Conference on Recent Advances in Internet of Things (RIoT), 2015, pp. 1–6.

[25] F. Folianto, Y. S. Low, and W. L. Yeow, "Smartbin: Smart waste management system," in *2015 IEEE Tenth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*, 2015, pp. 1–2.

[26] T. Anagnostopoulos, A. Zaslavsy, A. Medvedev, and S. Khoruzhnicov, "Top – k Query Based Dynamic Scheduling for IoT-enabled Smart City Waste Collection," in *2015 16th IEEE International Conference on Mobile Data Management (MDM)*, 2015, vol. 2, pp. 50–55.

[27] M. J. Mudumbe and A. M. Abu-Mahfouz, "Smart water meter system for user-centric consumption measurement," in *2015 IEEE 13th International Conference on Industrial Informatics (INDIN)*, 2015, pp. 993–998.

[28] L. Gabrielli, M. Pizzichini, S. Spinsante, S. Squartini, and R. Gavazzi, "Smart water grids for smart cities: A sustainable prototype demonstrator," in *2014 European Conference on Networks and Communications (EuCNC)*, 2014, pp. 1–5.

[29] W. Atmadja, J. Yosafat, R. A. Setiawan, and I. I. Irendy, "Parking guidance system based on real time operating system," in *2014 International Conference on Industrial Automation, Information and Communications Technology (IAICT)*, 2014, pp. 5–8.

[30] A. Saad, M. I. M. Roseli, and M. S. Zullkeply, "A Smart e-Voting System Using RFID Authentication Method for a Campus Electoral," in *Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication*, New York, NY, USA, 2014, pp. 31:1–31:7.

[31] F. Gustafsson and F. Gunnarsson, "Positioning using time-difference of arrival measurements," in 2003 IEEE International Conference on Acoustics, Speech, and Signal Processing, 2003. Proceedings. (ICASSP '03), 2003, vol. 6, p. VI-553-6 vol.6.

[32] K. C. Ho and W. Xu, "An accurate algebraic solution for moving source location using TDOA and FDOA measurements," IEEE Transactions on Signal Processing, vol. 52, no. 9, pp. 2453–2463, Sep. 2004.

[33] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," presented at the Advances in Neural Information Processing Systems.

[34] F. N. Iandola, S. Han, M. W. Moskewicz, K. Ashraf, W. J. Dally, and K. Keutzer, "SqueezeNet: AlexNet-level accuracy with 50x fewer parameters and <0.5MB model size," *arXiv:1602.07360 [cs]*, Feb. 2016.

[35] O. Abdel-Hamid, A.-R. Mohamed, H. Jiang, L. Deng, G. Penn, and D. Yu, "Convolutional Neural Networks for Speech Recognition," *IEEE/ACM Trans. Audio, Speech and Lang. Proc.*, vol. 22, no. 10, pp. 1533–1545, Oct. 2014.

[36] N. Dalal and B. Triggs, "Histograms of Oriented Gradients for Human Detection," in Proceedings of the 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05) - Volume 1 - Volume 01, Washington, DC, USA, 2005, pp. 886–893.

[37] S. Baker and I. Matthews, "Lucas-Kanade 20 Years On: A Unifying Framework," *International Journal of Computer Vision*, vol. 56, no. 3, pp. 221–255, Feb. 2004.

[38] OpenCV, "OpenCV: Optical Flow," *Open Source Computer Vision*. [Online]. Available: http://docs.opencv.org/trunk/d7/d8b/tutorial_py_lucas_kanade.html. [Accessed: 25-Dec-2016].

[39] Federal Aviation Administration, "Summary of Small Unmanned Aircraft Rule (Part 107)," FAA, Washington, DC 20591, Jun. 2016.