SECURING AND MANAGING ARMY CANTONMENT IN INDIA USING INTERNET OF THINGS

Tarun Kumar¹, Pawan Kukreja², Dharmender Singh Kushwaha³, Sanjeev Pippal⁴

¹Computer Science and Engineering Department, GL Bajaj Institute of Technology and Management Greater Noida, U.P. 201306
²,³Computer Science and Engineering Department, Motilal Nehru National Institute of Technology Allahabad, Allahabad, U.P. 211004, India

¹ertarun123@gmail.com, ²pawangargi@gmail.com, ³dsk@mnnit.ac.in, ⁴sanpippalin@gmail.com

https://doi.org/10.26782/jmcms.2020.06.00034

Abstract

Internet of Things (IoT) is newfangled area of development that can lead to tremendous efficiency improvement in terms of expensive manpower saving, cost cutting, round the clock availability and modular structure to continuously improve processes and things. This paper proposes an application of the IoT in security and management of the army cantonment area. In the context of security, this paper proposes three kind of integrated applications. The Access control system ensures entry of the authorized vehicles using RFID and Automatic Number Plate Recognition techniques. Intrusion detection based on passive infrared, camera and thermal imaging is proposed at the next level. Gun fire detection in residential blocks of the army campus by using sound sensors ensures any intrusion, attack or any other undue situation. Apart from security, this paper also proposes intelligent use of water flow sensors for smart monitoring of underground drainage and water level sensors to reduce the wastage of water in tank overflow conditions. The proposed system is reliable, efficient in terms of accuracy, response time of the various modules, round the clock capability and economical in terms of operational and maintenance cost.

Keywords: Vehicle detection, Automatic number plate detection, Radio frequency identification, Sensors

I. Introduction

Since past few years, India is facing internal security challenges in various states. The current situation becomes more aggravated as terrorist are targeting base camps of the security agencies. Currently physical security in a military cantonment
is generally ensured using walls, fencing, and obsolete tech solution viz. CCTV cameras, combination of manual processes like regulated entry and issue of temporary passes. Dependent upon extent of area and its layout, certain entry and exit points are decided. Based on these parameters, other resources like budget, manpower, time available are allocated. Threat perception also dictates allocation of these resources in terms of manpower, gates construction, manning of these gates to regulate entry and exit and various processes are implemented. Typical differences are that military has its own sensors, GIS, Private Communication architecture with Redundancy, Manpower and other important resources like PCs, Electricity, buildings and organizational structure. The current security scenario issues, reasons and problem areas are considered for a typical military cantonment in peace area. Cantonment generally has complete facilities of a town and is self sufficient for most of the civic functions. Scenario assumed within scope of this research proposal is that of peacetime issues. During wartime (also referred to as operational time), there are a variety of different requirement. Also extremely robust infrastructure, detailed validation and testing of all systems are essentially required for IoT based solutions to be used during war. This is highly unlikely to be used in near future and therefore not dealt in this document.

Case Study of Pathankot Incident is discussed here in brief. On 2nd Jan 2016 attack at Pathankot airbase, there was total commotion. Casualties incurred were 4-6 attackers, 1 civilian, 7 security personnel (5 DSC, 1 IAF commando, 1 NSG). One of the reasons highlighted by Indian Express was glaring deficiencies in security which had facilitated the attackers, including trees, tall grass and shrubbery surrounding the walls of the air base [III]. Other Possible causes were:

- Dense civilian environment around IAF base.
- Complacency of security persons and systems.
- Lack of latest processes and technology and their adaptability.
- Lack of coordination.
- No use of sensors to monitor blind areas, neglect of dead grounds and non-removal of vegetation around base.
- Terrain around Air Base

Certain obvious problems of current scenario are sub-optimal resource utilization, inefficiency, human fatigue/error, lack of complete area / periphery coverage & slow response both from info dissemination and action point of view.

II. Related Work

Current technology can help us turn the Internet of Things (IoT) into a hard-working asset to facilitate growth with advantages like Data-driven operational efficiencies that reduce inventory, downtime, and time to deploy. We can get a
greater ability to support our process evolution from a reliable, transparent technology foundation that is compatible with future technology releases. We can aim for reduced risk from a holistic, more easily managed security approach to address physical and cyber vulnerabilities. Our decision making can be faster and better through informed prioritization. Many researchers are exploring the scope of these leading edge techniques in different domains. Ghayvat et al. [II] proposed application of IoT sensors in the development of smart building that are capable to monitoring the movements of the objects. Singh and Kushwhaha [XV] proposed an automatic intrusion detection system based on IP camera and microcontroller. Proposed system detects the presence of the human and tracks the movements of detected person. Maisonneuve et al. [XII] proposed application of the sound sensors measure the level of noise pollution. Zanella et al. [XIX] use GPS based systems for estimation of real-time traffic congestion data. Kumar et al. [X] proposed automatic number plate recognition based on image processing techniques. Kumar and Kushwaha[XI] extends the scope of RFID techniques in real time vehicle tracking. The researchers are extending scope of IoT in various areas such as smart parking[XIII], smart grids[XVIII], smart fire detection system[XIV], traffic surveillance using aerial images and thermal images[VIII],[XVI] etc. These IoT based applications are reliable and have low maintenance cost. The intent of this research proposal is to extend the scope of IoT in safety of life of the soldiers.

III. Proposed Work

This paper proposes smart and intelligent techniques for securing and managing army cantonment area. It focuses to secure the army contentment by implementing RFID based access control system and smart intrusion detection at boundary walls of the camps. This paper also proposes smart drainage management in army cantonment since, it is a gray area for intrusion. Figure 1 illustrates the placement of various kinds of sensors to secure the army cantonment area. In this figure, the Passive Infrared (PIR) sensors and cameras are proposed to be installed on the boundary region of the cantonment to ensure the intrusion detection round the clock. All the cameras monitor the boundary in day time while the PIR sensors are capable to detect the presence of any human at night also. A thermal sensor is also proposed at the canal / drainage outlet of the cantonment area to detect any possible intrusion through these. The entry gate of the army cantonment is equipped with two RFID readers and a camera. All the sensors and cameras are connected to the centralized processing server. The centralized processing server has different servers for processing the information sensed.
This paper proposes three main modules for ensuring complete security of army cantonment from any types of intrusion. These modules are as follows:

1. Access Control System based on (RFID) and (ANPR),
2. Intrusion detection system based on Computer Vision and Passive Infrared Sensors,
3. Gun fire detection and alert system based on sound sensors&
4. Smart Cantonment upkeep and maintenance.

Access Control System

The proposed system provides a secure access control system for the cantonment area. In this system, entry of the each vehicle in army cantonment area is based on either RFID or ANPR authentication. This paper proposes two different approaches for authentication of any vehicles. The first approach is based on RFID readers and another one is based on ANPR.

RFID Based Access Control System

In the proposed security system, the RFID based techniques are used to secure the base station of security forces by deploying the RFID based access control system at entry points. RFID reader with processing device is attached to the gate control system at all the entry points of the base camps of security forces. This requires RFID tag to be installed in all the vehicles. RFID based access control system provides the access to the vehicles having authorized RFID tags only.
In this system, there is a centralized server that maintains the records of all the vehicles with their tag information and their privileges to entry in various base camps. All the vehicles that belong to security forces and their family members can be tracked at centralized server. When any vehicle wants to access into this surveillance area, RFID reader detects the tags of the vehicle. The processing device transfers the tag information to the centralized server and request for the privileges of the vehicles. The centralized server extracts the vehicle privileges and replies to the requesting device. On the basis of the vehicle privileges, process device sends the signal to gate control devices. Working of the proposed system is illustrated in figure 2.

**ANPR Based Access Control System**

There is a possibility of certain vehicles not equipped with RFID tags. These could be vehicles from suppliers, other cantonments or belong to a personal that has just arrived here on transfer. In this proposed system, verification of the vehicles is carried out using number plate recognition. ANPR based access control system read the image of the vehicle and identified its number. The system is required for those vehicles that do not have RFID tag equipped. In this module, ANPR system capture image of the vehicle and recognized its license plates. Entry is granted to the vehicle after verification of its authenticity by using recognized license plate as shown in figure 2.

![Illustration of working of access control system](image)

**Intrusion Detection System**

The intent of this module is to detect the intrusive activities on boundary walls of the army cantonment area around the clock. Computer vision based approach is used during day time environment and PIR for night surveillance. A pair of PIR and
camera is installed alongside of complete boundary wall. Each pair is connected with microcontroller device to transfer this information to the centralized server. Centralized server process the image obtained from the camera to detect presence of any human in the boundary zone. The PIS sensor sense the presence of the human based on the heat emission of human body. The microcontroller acquires the data and send to the centralized server. Each microcontroller is connected with the centralized server with wireless radio communication system. A REST full API is designed for communication between microcontroller and centralized server. The centralized server alerts the base camps in case of the intrusion in the cantonment area along with location of the intrusion. Thermal imaging sensor is placed at drainage outlet to detect the possible intrusive activity from canal / drainage out let in the cantonment area as happened in Sunjuwan army camp (JAMMU) on February 2018 in India[V]. This thermal sensor is also connected with the microcontroller. The sensor acquires thermal image of the drainage outlet continuously and microcontroller transfer acquire images to the centralized server.

During day time environment, vision based human detection system will work for possible surveillance. To detect the humans, a hybrid approach is developed based on the frame differencing and Histogram of Oriented Gradients (HOG) features[VII] of the image. For this proposed approach, assumption is made that the surveillance zone near the boundary wall is no-man's land area. Background subtraction technique is used to detect the presence of any object in surveillance area. The HOG feature based approach is used to confirm the presence of the human in the surveillance zone. A feed forward back-propagation artificial neural network is designed to classify the detected object as human or non-human objects. The presence of the human in the surveillance area alerts the army.

**Gun Fire Detection**

Most of the army cantonment area has a residential area for army personnel. The incidents of general gun fire in such area are very rare except any intrusive attacks. To detect such type of incidents in residential area, this work proposes use of sound sensors with intelligent microcontroller device. In general, gun fire has sound pressure above 130db and the sound pressure decrease 3db by increasing the distance twice between sound source and sound sensor [VI]. This property of sound waves is utilized in estimation of the possible distance sound sensors installation. In the proposed configuration, the sound sensors are deployed in fixed distance around the buildings. These sensors continuously monitor the sound pressure and programmed microcontroller identifies the pressure level and compares the same with the threshold. The microcontroller alerts the base station with its location in case of gun fire detection.

Apart from security issues of cantonment area, functioning of the cantonment with minimum manpower is also challenging. Maintenance of underground drainage involves multiple tasks such as detection of the choke points, excavation of roads,

---

Copyright reserved © J. Mech. Cont.& Math. Sci.

Tarun Kumar et al
repair work and patch work on road etc. This article also proposes automatic monitoring, choke detection and prevention technique by using IoT sensors. The next section describes the smart drainage management system.

**Smart Drainage Management Using IoT**

Each Cantonment has open and underground drains, and most of these being age old. It is virtually impossible to manually track cleaning, overflowing and periodic maintenance of these drains. There is no single solution that is foolproof in this regard. Currently, system used is complaint and resolve by sending physical manpower / mechanical means. This is very inefficient system due to duplicity of control among various agencies, area overlaps, lack of resources, slow human reaction. As a result, unhygienic cantonment, related health issues emerge. This paper makes an effort to propose a smart drainage monitoring system by using water flow sensors. Water flow sensors monitor the flow of water in the underground pipe. The water flow sensor consists of a rotator embedded with magnetic strip. Rotation of this rotator generates pulses for Hall Effect sensor. Water flow rate is measured by using flow sensors. In the proposed solution, each flow sensor is connected with a controller to collects the water flow information. Solution is to install these flow sensors at critical choke points. Centralized dash board monitoring helps proactively monitor complete network of drains. Solution is proactive since 24x7x365 monitoring is possible by utilizing integrated sensors and by less manpower. Monitoring of wider areas can thus be coordinated in a much better way. Certain process changes to log complaints and seasonal prioritization can improve efficiency further.

**Smart Water Overhead Monitoring**

Water treatment source to Overhead storage is a stable system, albeit treatment of water based on various chemical parameters can be automated, remotely monitored, recorded and proactively controlled. Lack of effective monitoring of overhead tanks at homes and central overhead tanks can be easily done with sensors thus preventing water wastage, excess power wastage due to extra pumping. A smart and intelligent use of water level sensors to control the water pumps is proposed. The installation of these sensors in various water tanks reduces the wastage of water and electricity without manpower.

**IV. Results and Analysis**

To establish feasibility of the proposed security and management system, cost and performance analysis of each sensors and application is carried out. A three layered architecture for securing and managing the army cantonment area is proposed as illustrated in figure3. IP cameras and PIR sensors performs preventive measures against any intrusive activity from the boundary walls. At the second layer, thermal sensors and sound sensors work continuously for detection of any intrusive entry from the drainage / canal outlets in the cantonment area. The sound sensors are installed in residential area for proactive measure to detect the location of the gun.
fire. The situation in which the terrorist any how breaches the first layer and starts gun fire in the campus, the sound sensors will detect the position of the terrorist based on in sound pressure and alert the control room. The layer third provides the smart management of the underground drainage and the water tanks by using the flow sensors and water level sensors.

Fig. 3: Layered architecture for securing and managing army cantonment

Through the implementation of the proposed layered architecture, the army cantonment can mitigate the several types of the risk and threats and reduce the manpower requirement in management of the overall security requirements and underground drainage and sever points. Table 1 illustrates the overall risks and threats that can be minimize by using the proposed system.

Table 1: Location wise impact of the sensors in proposed system

| Sensors Location | Camera | RFID Reader | PIR | Thermal | Sound | Flow Sensor | Water level Sensor | Impact |
|------------------|--------|-------------|-----|---------|-------|-------------|-------------------|--------|
| Entry Gates      | Yes    | Yes         | No  | No      | No    | No          | No                | Restricted Entry to only authorized vehicles |
| Boundary Walls   | Yes    | No          | Yes | No      | No    | No          | No                | Detection of intrusive activity round the clock |
In the proposed system, the accuracy of the image processing techniques needs to be measured for automatic number plate detection and human detection. The ANPR proposed in [X] is used for the access control system at entry gate and the approach for human detection is proposed in this article.

The accuracy and the response time of the APN are tested on the images of the vehicles captured in different environmental conditions. The table 2 illustrates the accuracy of the vehicles license plate recognition.

**Table 2: The Accuracy of the ANPR in different environment conditions**

| S. No. | Total Number of Vehicles | Environment | Accuracy (%) | Avg. Response time per vehicle (in Sec.) |
|--------|--------------------------|-------------|--------------|----------------------------------------|
| 1      | 50                       | Morning     | 97.6         | 1.12                                   |
| 2      | 50                       | Afternoon   | 98.1         | 1.08                                   |
| 3      | 50                       | Evening     | 96.4         | 1.47                                   |
| 4      | 50                       | Night       | 83.1         | 2.01                                   |
| 5      | 50                       | Cloudy      | 94.3         | 1.23                                   |
The average accuracy of license plate recognition in the proposed system is 96.6% excluding night surveillance data. The accuracy of license plate recognition decreases during the night environment and can be improved further by placing flood lights at the entry gates.

The approach for human detection is tested on the INRIA Person Dataset[IV]. The neural network is trained for 70 images of human and 70 images of non-human. During the training, neural network achieves 100% accuracy. During testing the same, the proposed approach achieves 97.4% accuracy in detection of human. The figure shows the confusion matrix of the training of neural network. Figure 4 shows the cross entropy of the neural network in each iteration of the training session.

The proposed neural network for human detection achieves 97.7% accuracy at 10 hidden layers.

Performance of the RFID based vehicle identification does not vary with changes in environmental conditions but may be affected when multiple RFID enabled vehicles are detected at the same time instance. This phenomenon is called collision of RFID tags. The proposed approach demands that the RFID reader must have quick response time and the module should not be vulnerable for collision of tags. During the simulation, performance of the RFID reader to handle the collision and the response time is measured for different scenarios. At present various algorithms exist for collision resolution in RFID techniques. In this article, an experiment is carried out to measure the performance of the RFID readers in collision like scenario. For the experiments, the topology including one RFID reader and multiple passive RFID tags enabled nodes is designed in NS-2 simulator.
Topology

While simulating in ns2, the proposed topology comprises of one RFID reader agent. The performance of the RFID reader is evaluated against the different number of mobile nodes with unique tag identifier. The numbers of the mobile tag nodes are 10, 20, 30, 40, 50 and 100. The speed of the mobile nodes is set to be random. The topology is constructed using the parameters given in the table 3.

Table 3: Parameters used for RFID Simulation

| Parameters                           | Values                              |
|--------------------------------------|-------------------------------------|
| Antenna Type                         | Omini Antenna                       |
| Transmit power (pt)                  | 0.2 (Approx. 15dBm)                 |
| Received power threshold             | 7.64097e-06 (Approx. 5 meters)      |
| Interface queue type (ifq)           | Queue                               |
| Max ifq size                         | 1000                                |
| Reader Type                          | Singularization                     |
| Service type (Algorithm)             | Q/DFSA/NEDFSA                       |
| Time to wait for collision           | 0.009                               |
| Algorithm constant                   | 0.2                                 |

Performance Evaluation

The objective of the simulation is to measure the average response time for a single tag. The simulation is carried out for 10, 20, 30, 40, 50 and 100 mobile nodes with unique identifier. In the simulation three existing algorithm such as Q-Algorithm[XI], Dynamic Framed Slotted ALOHA (DFSA) Algorithm[I] and Novel Estimated Dynamic Framed Slotted ALOHA (NEDFSA) Algorithm[XVII] are used.
Table 4: Average response time of the system for different number of tags

| S.N o. | No. of Tags | Average response time in seconds | Q – Algorithm | DFSA | NEDFSA |
|-------|-------------|---------------------------------|---------------|------|--------|
| 1     | 10          | 0.3667                          | 0.2701        | 0.2107 |
| 2     | 20          | 0.2780                          | 0.2432        | 0.2342 |
| 3     | 30          | 0.2668                          | 0.2332        | 0.2047 |
| 4     | 40          | 0.2527                          | 0.2657        | 0.2319 |
| 5     | 50          | 0.2892                          | 0.2698        | 0.2413 |
| 6     | 100         | 0.3102                          | 0.2863        | 0.2839 |

Fig.5: Average response time of RFID module for different anti-collision algorithms

Plot in figure 5, illustrates the response time of the RFID module for different algorithm respectively. In the simulation of the RFID module, all the tags are identified by RFID reader and the proposed simulation achieves 100% accuracy. The above figures show the efficiency and the average response time of the system. The average response time to identify a tag is 0.29 second in Q-Algorithm, 0.26 second in DFSA and 0.23 second in NEDFSA as shown in table 5. The above results illustrate that RFID modules have average response time < 0.3 second. The timeout time based on the simulation is set to 0.5 second for RFID module. The anti-collision efficiency of the system is 0.2447 for Q-Algorithm, 0.2264 for DFSA and 0.2112 for NEDFSA. The average efficiency of the system is <1, means system is capable to handle the collision.

Copyright reserved © J. Mech. Cont.& Math. Sci.
Taran Kumar et al
Cost Analysis

In this section, cost analysis of the required sensors and other devices is carried out. The objective of this analysis is to provide basic information for estimation of the total cost of the proposed system as shown in table 6. The cost of the each type of sensor and machines is given in the table 6.

Table 5: Cost list of equipment and sensors used in proposed system

| S.No. | Sensor / Device         | Price          |
|-------|-------------------------|----------------|
| 1     | IP Camera               | ₹2000 - ₹15000 |
| 2     | RFID Reader             | ₹2000 - ₹30000 |
| 3     | PIR Sensors             | ₹425 - ₹10000  |
| 4     | Thermal Sensors         | ₹50000 - ₹100000 |
| 5     | Flow Sensor             | ₹200 - ₹5000   |
| 6     | Water Level Sensor      | ₹200 - ₹5000   |
| 7     | Microcontroller (Arduino)| ₹800 - ₹2000  |
| 8     | Server Machine          | ₹70000 - ₹150000 |
| 9     | Networking Equipments   | ₹100000 - ₹500000 |

The installation of the proposed system incurs only one time cost. The operational cost and maintenance cost is negligible of the proposed system. The manual surveillance and management of the existing army cantonment area is the much more expensive and vulnerable to loss of military personals and other threats as compared to proposed system.

Total cost that shall incur for installation of these devices and sensors over a one square kilometer army cantonment is much less as compared to the loss incurred when an army personal loses his life. Although, we don’t dare to evaluate cost of life, but the cost incurred on training salaries and other benefits is much more.

V. Conclusion

A three layered architecture for securing and managing the army cantonment area is proposed comprising of IP cameras and PIR sensors that perform preventive
measures against any intrusive activity from the boundary walls. The access control system based on RFID is 100% accurate and efficiently detects multiple vehicles at the same time instance. ANPR system achieves 96.6% accuracy in license plate recognition. Human detection at the no-man’s land area based on image processing achieves 97.7% accuracy. Experimental results establish that the proposed system is not only reliable, but also very economical to implement for a developing nation like India. The operational and maintenance cost of the system are negligible as compared to manual surveillance and management. Another advantage of proposed system is that it maintains logs of the events. These logs can be utilized in post analysis of the security vulnerabilities as well as evaluating and planning of various kinds of activities in cantonment area. India is facing proxy war from last few decades either in Kashmir or many naxalite states. In such kind of conditions, implementation of proposed system can prevent various attacks and saves life of our beloved soldiers.

References

I. Cha, J.-R. and Kim, J.-H. Dynamic framed slotted ALOHA algorithms using fast tag estimation method for RFID system. Proc. IEEE CCNC, 2006, 768–772.

II. Ghayvat H., Mukhopadhyay S., Gui X., Suryadevara N. (2015). WSN-and IOT-based smart homes and their extension to smart buildings. Sensors. 4;15(5):10350-79.

III. http://indianexpress.com/article/india/india-news-india/pathankot-terror-attack-something-seriously-wrong-with-our-security-establishment-parliament-panel/.

IV. http://pascal.inrialpes.fr/data/human/ (2018)

V. http://www.firstpost.com/india/jammu-attack-by-entering-fortified-sunjuwan-army-camp-from-rear-afzal-guru-squad-exploited-security-lapse-4344775.html (2018)

VI. http://www.sengpielaudio.com/calculator-SoundAndDistance.htm (2018)

VII. Iamsa-at S and HorataP.. Handwritten Character Recognition Using Histograms Of Oriented Gradient Features in Deep Learning of Artificial Neural Network. In IEEE International Conference on IT Convergence and Security (ICITCS), pp. 1-5.
VIII. Krishnan, D., Muthaiah, R., Tapas, A., & Kannan, K. (2018). Evaluation of Local Feature Detectors for the Comparison of Thermal and Visual Low Altitude Aerial Images. Defence Science Journal, 68(5), 473-479. https://doi.org/10.14429/dsj.68.11233

IX. Kumar T. & Kushwaha, D. S. An Intelligent Reconnaissance Framework for Homeland Security. Def. Sci. J. 69, 4 (2019). doi: https://doi.org/10.14429/dsj.67.10286

X. Kumar, T., Gupta, S. & Kushwaha, D. S. An Efficient Approach for Automatic Number Plate Recognition for Low Resolution Images. In The fifth International Conference on Network, Communication and Computing (ICNCC) 2016 53–57.

XI. Maguire, Y. and Pappu, R. An optimal Q-algorithm for the ISO 18000-6C RFID protocol. IEEE transactions on automation science and engineering, 2009 6, 1, 16–24.

XII. Maisonneuve M. Ortiz et al. (2014). The cluster between Internet of Things and social networks: Review and research challenges, IEEE Internet Things J., vol. 1, no. 3, pp. 206–215, Jun. 2014

XIII. Rao Y. R. Automatic smart parking system using Internet of Things (IOT). Int J EngTechnolSci Res. 2017 May;4(5).

XIV. Rathore M. M., Ahmad A., Paul A., Rho S. Urban planning and building smart cities based on the internet of things using big data analytics. Computer Networks. 2016 Jun 4;101:63-80.

XV. Singh, D. K. & Kushwaha, D. S. Automatic Intruder Combat System: A way to Smart Border Surveillance. Def. Sci. J. 67, 50 (2017). doi: https://doi.org/10.14429/dsj.67.10286

XVI. Verma, K., Kumar, A., & Ghosh, D. (2018). Robust Stabilised Visual Tracker for Vehicle Tracking. Defence Science Journal, 68(3), 307-315. https://doi.org/10.14429/dsj.68.12209

XVII. Wensheng S. and Chenmin J. A Novel Dynamic Frame Slotted ALOHA Algorithm for Anti-Collision in RFID Systems in Journal of Information and control, 2012, (2): 233-237.

XVIII. Yun M., Yuxin B. Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid. In Advances in Energy Engineering (ICAEE), 2010 IEEE International Conference on Jun 19 (pp. 69-72).

XIX. Zanella A. et al. (2014). Internet of Things for smart cities, IEEE Internet Things J., vol. 1, no. 1, pp. 22–32.