Secure and Safe Surveillance System Using Sensors Networks - Internet of Things

Fazlullah Khan[1](✉), Mukhtaj Khan[1], Zafar Iqbal[2], Izaz ur Rahman[1], and Muhammad Alam[3]

[1] Department of Computer Science, Abdul Wali Khan University Mardan, Mardan, Pakistan
{fazlullah,mukhtajkhan,izaz}@awkum.edu.pk

[2] Department of Computer Science, City University of Sciences and IT, Peshawar, Pakistan
zafariqbal@cusit.edu.pk

[3] Instituto de Telecomunicações, University of Aveiro, Aveiro, Portugal
alam@av.it.pt

Abstract. Sensor network is a network of autonomous devices that consist of sensors which are spatially distributed to sense the physical environment for certain parameters like temperature, humidity and pollution etc. There are various applications of sensor network, like volcanic eruption, inventory tracking system, military surveillance, homes and industrial automation and automobiles. Different sensors use for specific purpose such as temperature sensor, humidity sensor, light sensor, ultrasonic and multimedia sensor, and all these sensors are used for their own task. In this system, we use ultrasonic sensor for defense and security purpose. The ultrasonic sensor constantly transmits ultrasonic sound (Transmitter) which on striking with an obstacle bounces back and that bounced wave is also received by sensor (Receiver) and from this reflection the distance between sensor and obstacle is calculated. So when a person come close to dangerous area like electric field, river side and explosive material, the system will detect the person and will sound an alarm to inform the authorities. The proposed scheme is implemented and the generated results validates its functionalities.

Keywords: Internet of things · Security · Surveillance · Wireless sensor networks

1 Introduction

The "IoT" heralds the connection of a nearly countless number of devices to the internet thus promising accessibility, boundless scalability, amplified productivity and a surplus of additional paybacks [1]. Current real-world deployments of large-scale IoT systems are not limited to some well-bounded application domains. Sensor networks is one of the key network that will play a vital role to achieve the desired goals. Sensor networks uses in various areas because of

J. Ferreira and M. Alam (Eds.): Future 5V 2016, LNICST 185, pp. 167–174, 2017.
DOI: 10.1007/978-3-319-51207-5_16

their unique characteristic that ranges from low level like mobile sensor (use in mobiles for call) to high level applications as nuclear plant monitoring. In sensor networks we deploy sensors in a field that is to be monitored for various parameter like temperature, humidity, pollution, light etc. the deployment criteria depends on application, it may be random or pre-planned [2]. The deployment in any hostile environment and in large geographical areas is usually random while in normal situation or limited areas we use pre-planned deployment technique.

Life of every human being is precious and the safety is a challenge for us. But the safety can be achieved by the use of various technological applications that do exist in this modern world. One of the techniques is through the deployment of sensor network. Therefore, we use ultrasonic sensor as a source of measuring the distance between human and the network. When a person approaches to define threshold the network will give a signal (alarm) to avoid the danger area. In this paper, the deployment of our network nodes are pre-planned as we have to monitor a specific area. The network can be deployed to any environment which can cause harm or threat to human life like electric field, border crossing, and huge water sides.

The reminder of this paper is structured as follows: the next section gives a short overview of relevant related work. Section 3 describes the proposed scheme. The implementation is described in Sect. 4. Section 5 gives an overview concerning the tests setup and the measurements results. In the last section, we draw the conclusions and some outlines for future work.

2 Related Work

We can find a number of related works focusing on the surveillance system using sensors networks such as a detail survey on multi-media can found it [3], a detail work on the energy efficient servilance system in [4]. The Australian Defense Force has IMAP and JMAP to perform planning prior to the deployment of forces, but there is a knowledge gap for on-ground forces during the execution of an operation [5]. Multi-agent based sensor systems can provide on-ground forces with a significant amount of real-time information that can be used to modify planning due to changed conditions. The issue with such sensor systems is the degree to which they are vulnerable to attack by opposing forces. This paper explores the types of attack that could be successful and proposes defense that could be put in place to circumvent or minimize the effect of an attack.

In [6], the authors state that it is practically impossible to construct a truly secure information system. Communications are secure if transmitted messages can be neither affected nor understood by an adversary, likewise, information operations are secure if information cannot be damaged, destroyed, or acquired by an adversary. They go on to define software challenges for a future combat system including (but not limited to) network security and accessibility; fault tolerance; and information analysis and summary of large data streams from the network. Further, author in [8] claim that most software is insecure. This could be because, as [9] have observed, security requirements are often omitted from requirements specifications altogether. This has been noted as being particularly problematic in other safety-critical domains such as automotive control software [10].

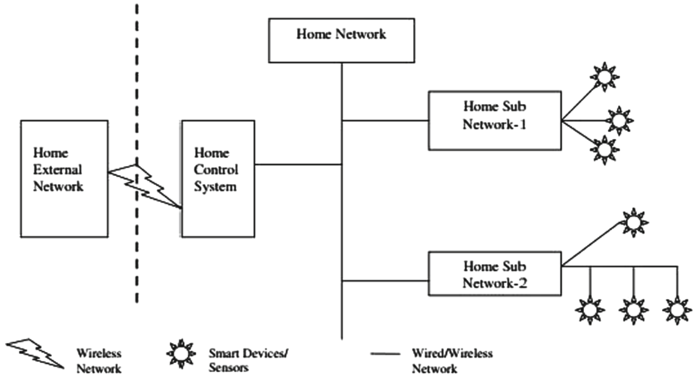


Fig. 1. Proposed system overview

In terms of the problem domain (military operations), wireless sensors of various types can be distributed on ground before a battle, whilst being connected to autonomous software agents in a multi-agent system to give an on-field tactical advantage, provided that the communications between the sensors cannot be subverted. A public key infrastructure is an obvious solution to the integrity problem, however issues of secure storage for the private key and over-the-air transmission of either public or private keys will still prove problematic. The issue of key management is perhaps further complicated by the ever-decreasing cost of the hardware required to conduct a brute-force attack [11].

3 Proposed Scheme

Our proposed model is focusing on the defense and security of individuals rather than a team. As stated, the basic application is to comfort and ease in life of general public as it can be installed in almost all places with low-cost and operation facilities. The previous work in this field were about high level security i.e. on state level surveillance but our model will provide the security in our routine work. In this model, we define an threshold and permitted area, where if someone tries to get into that particular area the alarm system will invoke the security officials as well as the individuals living or staying in that particular area on that particular time.

The proposed algorithm for the scheme is working on the principle that when the sound signal is generated by ultrasonic sensor and it echo back receive by the receiver of ultrasonic sensor and send to micro controller, the micro controller calculate the time. The time at which sound is produced and which it is received are also recorded. The distance is calculated on the bases of this time. The formula for the distance is

$$D = \frac{\frac{time\,in\,\mu\ \mathrm{sec}}{73.746}}{2}\,inches \qquad (1)$$

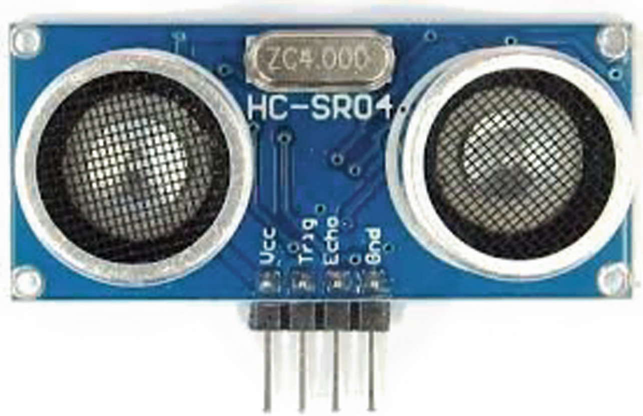


Fig. 2. An HC-SR04 type ultrasonic sensor

Using the above distance formula, we calculate threshold "t" value, where as for t < 24 in., it will display warning massage to the base station and will sound an alarm. An overview of the proposed system is presented in the Fig. 1. The figure shows that sensor network is integrated with the home sub-network and that is further connected with the home networks. Inside home, wireless and wireless networks can be used to connect with the external networks. For instance, if the users want to save the events in a server they can use the in-house networks to store the activities in the server.

4 Implementation

This section overviews the variety of hardware and software used to implemented the proposed scheme and generating results.

4.1 Ultrasonic Sensor

This type of sensors generates high frequency sound waves and evaluates the echo which is received back by the sensor. The frequency of sound wave is about 20 KHz or above. The time interval between sending the signal and receiving the echo determines the distance of object. Figure 2 depicts the sensor that has been used in the tests.

Fig. 3. Micro-controller chip used.

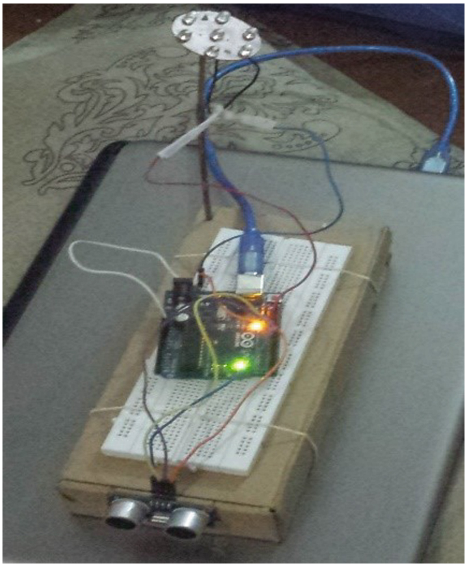


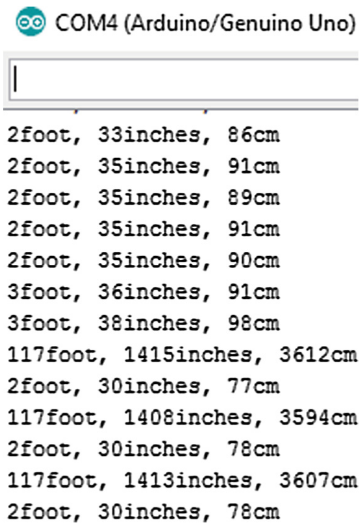
Fig. 4. Proposed system overview

4.2 Micro Controller

A micro controller is a small computer as it has a single IC. The micro controller has its own processor core, memory. The function of micro controller is to process the data (Fig. 3).

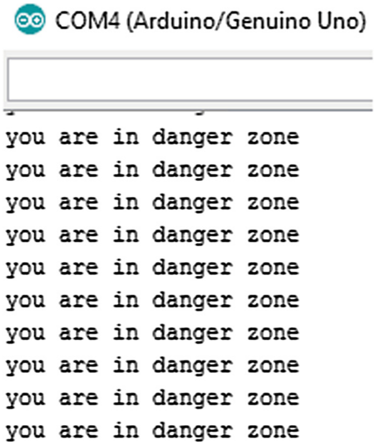
4.3 Bread Board and Jumper Wires

A bread board is used for making an experimental model of an electric circuit. As micro controller can support only a few devices therefore we use bread board



```
2foot, 33inches, 86cm
2foot, 35inches, 91cm
2foot, 35inches, 89cm
2foot, 35inches, 91cm
2foot, 35inches, 90cm
3foot, 36inches, 91cm
3foot, 38inches, 98cm
117foot, 1415inches, 3612cm
2foot, 30inches, 77cm
117foot, 1408inches, 3594cm
2foot, 30inches, 78cm
117foot, 1413inches, 3607cm
2foot, 30inches, 78cm
```

Fig. 5. Output in normal condition



```
you are in danger zone
you are in danger zone
you are in danger zone
you are in danger zone
you are in danger zone
you are in danger zone
you are in danger zone
you are in danger zone
you are in danger zone
you are in danger zone
```

Fig. 6. Output at the time of intruder detection

to connect multiple devices with the micro controller through jumper wires for initial test at laboratory level.

4.4 Software

We have used the open source Arduino Integrated Development Environment (IDE). The open-source Arduino Software (IDE) makes it easy to write code and upload it to the board. It can run on Windows, Mac OS X, and Linux.

5 Installation of Tools and Results

As stated earlier, the different devices are interconnected with micro controller through bread board. The connection was provided by jumper wires. The micro controller is further connected to laptop to display the result. The system is shown in Fig. 4.

When the network is in off state, it does not sense any movement and does not generate any data or information. Initially, the system is tested for normal condition and the situation when there is someone near the in vicinity. In normal condition, the system will sense the data through sensors; the micro controller will process it and will pass the output to the base station. The micro controller processes the data (calculate the distance) and take a decision on the calculated data. In normal condition when the threshold is not reach network will not take any action. As depicted in Fig. 5, the system shows the result of detection at various distances from the system.

When the defined threshold is reached i.e. the distance between network and intruder is less than defined threshold the system will sound an alarm and lights will start blinking and the message shall be displayed as “danger area” as depicted in Fig. 6. It should be noted that based on the scenario and application, we can change the defined threshold.

6 Conclusions and Future Work

In this paper, we presented a scheme based on sensor networks for surveillance system. In a nut-shell, the presented system is based on sensor network which use ultrasonic sensor and it take decisions based on sensed data at define threshold. The proposed system is implemented and validated. In future, we are committed to use the ultrasonic sensor in other applications as auto door’s opening, and home automation.

References

1. Alam, M., Ferreira, J., Fonseca, J.: Introduction to intelligent transportation systems. In: Alam, M., Ferreira, J., Fonseca, J. (eds.) Intelligent Transportation Systems. SSDC, vol. 52, pp. 1–17. Springer, Heidelberg (2016). doi:10.1007/978-3-319-28183-4_1
2. Alam, M., Rodriguez, J.: A dual head clustering mechanism for energy efficient WSN. In: Proceedings of the 2nd International Conference on Mobile Lightweight Wireless Systems - MOBILIGHT, Barcelona, Spain, May 2010
3. Cucchiara, R.: Multimedia surveillance systems. In: Proceedings of the Third ACM International Workshop on Video Surveillance and Sensor Networks, pp. 3–10. ACM (2005)
4. Tian, H., Krishnamurthy, S., Stankovic, J.A., Abdelzaher, T., Luo, L., Stoleru, R., Yan, T., Gu, L., Hui, J., Krogh, B.: Energy-efficient surveillance system using wireless sensor networks. In: Proceedings of the 2nd International Conference on Mobile Systems, Applications, and Services, pp. 270–283. ACM (2004)

5. Johnstone, M.N., Thompson, R.: Security aspects of military sensor-based defence systems. In: 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, pp. 302–309. IEEE (2013)
6. Wysopal, C., Nelson, L., Dai Zovi, D., Dustin, E.: The Art of Software Security Testing. Addison Wesley, Upper Saddle River (2007)
7. RFC 2828: Internet security glossary. Internet Engineering Task Force (2016). http://www.ietf.org/rfc/rfc2828.txt. Accessed 22 June 2016
8. Lozano, A., Jindal, N.: Transmit diversity vs. spatial multiplexing in modern MIMO systems. IEEE Trans. Wirel. Commun. **9**(1), 186–197 (2010)
9. Puthal, D., Nepal, S., Ranjan, R., Chen, J.: A dynamic key length based approach for real-time security verification of big sensing data stream. In: Wang, J., Cellary, W., Wang, D., Wang, H., Chen, S.-C., Li, T., Zhang, Y. (eds.) WISE 2015. LNCS, vol. 9419, pp. 93–108. Springer, Heidelberg (2015). doi:10.1007/978-3-319-26187-4_7
10. Jan, M.A., Nanda, P., He, X., Liu, R.P.: A lightweight mutual authentication scheme for IoT objects. IEEE Trans. Dependable Secure Comput. (TDSC), pp. 670–676 (2016)
11. Puthal, D., Nepal, S., Ranjan, R., Chen, J.: A dynamic prime number based efficient security mechanism for big sensing data streams. J. Comput. Syst. Sci. **83**(1), 22–42 (2016)