Survey on Intrusion Detection Security Management System using Internet of Things Devices

Yogesh Nagar [1], Gagan Sharma [2], Rajesh Sharma [3]
[1,2,3]Department of Computer Science & Engineering,
RKDF University, Bhopal, India

Abstract: Internet of Things (IoT) is a modern perspective which incorporate the Internet and daily life physical object related to several domains like home automation, office, human health, industrial process and environmental monitoring. Using Internet of things and modern sensors, the implementation of security management system, have been popularizing now a days for smart city development. In this paper, a comprehensive survey on intrusion detection management system using Internet of things (IoT) devices are presented. This survey presents various challenging issues, strategies and technical aspects with respect to IoT based intrusion detection system. Finally, future aspects of modern intrusion detection system in smart city development is presented.

Keywords: Intrusion Detection, Internet of Things, Ultrasonic Sensors

I Introduction

Internet of things (IoT) offers various electronic security systems which frequently include surveillance, access control and intrusion detection devices that are permanently installed at the protected premises for smart city development [1]. They usually require substantial capital outlay for their design, components and commissioning which nevertheless enable later savings in security personnel costs [2, 3].

This high capital outlay is not justifiable for some premises that, for example, temporarily house exhibitions or high value cargo, and infrequent public events. In these cases the cost of IoT based sensing devices and security arrangements can be reduced by using easily installable and programmable low cost autonomous proximity sensors [4, 5]. These sensors could be set on guard for specific times only, discreetly cordoning off particular perimeters without obstructing the view of the exhibits or causing inconvenience during work hours. If an intrusion was detected, the sensor would report it wirelessly to the security personnel reducing the number of security staff required otherwise. Each proximity sensor in such a system should be of low cost and low power consumption, capable of broadcasting secure messages across [6, 7].

In this paper we present a conprehensive survey on low cost IoT based sensing devices for distributed security system that utilizes ultrasonic transducers operating in the pulse echo mode for intrusion detection, can be easily installed, can operate unattended for days and reports an intrusion wirelessly.

II Intrusion Detection System using Modern IoT based Sensors

Various active and passive IoT based sensor technologies can be used for proximity sensing in security applications. Passive sensors (e.g., acoustic, seismic or thermal infrared sensors) use the energy received from the environment to detect the presence of the intruder [8]. For example, widely used passive infrared (PIR) sensors detect changes in infrared radiation caused by movements of the intruder which has different temperature compared to the surroundings [9, 10]. However, these sensors have shown a high miss rate when the intruder moves at a slow speed or use heat insulating closes.

Active sensors include infrared (IR), inductive, capacitive, and ultrasonic sensors [11–13]. The active IR sensors sense either the intensity or phase shift of the IR light back-scattered by the intruder. The IR intensity sensors frequently give inaccurate ranging results because of their nonlinear sensitivity and dependence on the reflectance of surrounding objects. The phase shift option can offer medium resolution at long ranges, but at high cost [14].

Inductive and capacitive sensors are not convenient for proximity sensing in security applications for several reasons. First, they require a ratio between the maximum operating distance and the sensor diameter of about 0.5; therefore, they have very small operating range for portable sensors. Second, their sensitivity is highly dependent on the physical nature of the intruding object. Third, inductive devices operate only in the presence of a magnetic field so that a magnetic target or some permanent magnet has to be used in the system [15, 16].

Active ultrasonic sensors seem preferable for this application for the following reasons. First, they can operate in various open space environmental conditions, in the presence of fog, dust, dirt, lighting or strong electromagnetic interference (EMI). Second, ultrasonic sensors can be used for relatively accurate distance measurements by estimating the time-of-flight (TOF) of the emitted ultrasonic wave. Comparing to laser or microwave emissions propagating at the speed of light, ultrasonic sensors require much simpler and cheaper electronics because of low speed of sound in air (around 340 m/s at 200C). Third, ultrasonic sensors can be fabricated at a low cost using electrostatic or piezoelectric principles [9]. There are suitability various sensor technologies for low cost intrusion detection security networks.

III Related Work

Loukas *et al.* [17] presented the landscape of IDSs for vehicles which is fragmented into isolated families of research ideas employed on a single type of vehicle, and usually evaluated on generalist network simulators. By proposing a single IDS taxonomy for all types of vehicles and identifying areas of future research, they aimed to help researchers from a diverse range of backgrounds identify where they can contribute in the overall architecture of a vehicle's IDS, adopt ideas tried previously on different types of vehicles, as well as extend existing solutions with both cyber and physical audit features, more diverse design architectures, and evaluation in more realistic conditions and against a greater range of realistic attacks.

Khelifi *et al.* [18] presented a survey of different approaches, techniques and technologies of the localization systems in WSN and their application in Internet of Things. We classified the localization approaches into centralized, distributed, ant iterative. Centralized algorithms generally provide more precise positions and can handle a large amount of data. However, they are energy consuming and present a single point of failure, which reduces their use in power-sensitive or large-scale applications. Distributed localization mechanisms are based on message exchange between nodes and several anchors. These systems do not dependent on central entity and have potentially better scalability, but lower precision. Iterative approaches are used by a distributed algorithms to improve the initial location estimation, which is obtained by adding more range measurements or spatial relationship information. However, these systems are usually costly in terms of computing.

Sonbul *et al.* [19] described the architecture, operation, design and experimental performance of a low cost ultrasonic distributed security system for intrusion detection. All the constituents of the system were fully prototyped and successfully tested. They selected ultrasonic sensors operating in the pulse echo mode to achieve medium range detection from a single sensor node. The nodes were networked using ZigBee that enabled secure, reliable, low cost, long battery life and simple networking. A simple PIC microcontroller was used for design of the node which enables the low cost and low power operation for the nodes. A node consists of an ultrasonic transducer, a microcontroller, a DC–DC converter, a ZigBee module and semiconductor switches with the low cost.

IV Proposed Approach

The proposed architecture of intrusion detection system integrates several autonomous battery operated IoT based sensor nodes. Every node consists of an ultrasonic proximity sensor, a network adapter and a microcontroller. The microcontroller wirelessly receives the operating parameters and reports intrusion when it is detected. Fully autonomous low cost nodes can be installed using quick fasteners (magnets or screws), and require no extra wiring. The nodes can go to sleep if not in use or between the consecutive transmissions consuming down to very low power only.

This feature allows reducing the number of nodes comparing to conventional proximity sensors because there is no need for separate transmitter and receiver as represented in Figure 1. Another advantage of ultrasonic proximity sensors relates to their wider beam (60° typical) comparing to, for example, optical transmitter-receiver pair. Ultrasonic Sensors are specifically made to sense the object proximity or range with the help of ultrasound reflection, just like a radar, which helps in calculating the time taken to reflect ultrasound waves between the sensor and a solid object. It consists of three units, one or more transmitters, receiver and control unit. The transmitters emit a high frequency ultrasonic sound waves which reflect back from any nearby solid object and then received by the receiver and further processed by the control unit to calculate the time taken. Using this time, the distance between the object and the sensor can be calculated using some calculations. Thus this distance can be used for specific purposes.

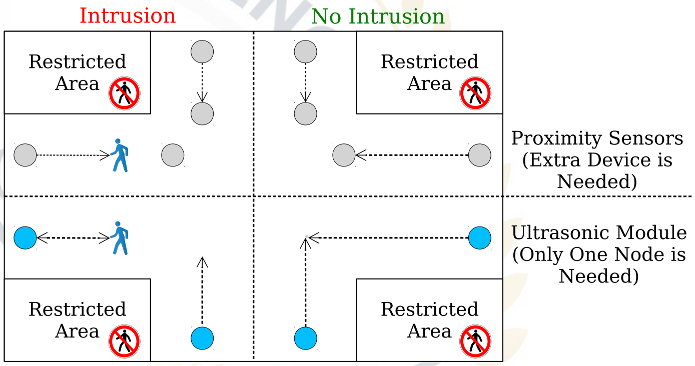
Intrusion
No Intrusion
Restricted Area
Restricted Area
Proximity Sensors (Extra Device is Needed)
Ultrasonic Module (Only One Node is Needed)
Restricted Area
Restricted Area

Figure 1: Proposed Model of Intrusion Detection System

In this survey, we are proposing this sensor to capture any motion within a specific range. We use “HC–SR04” ultrasonic sensor in this project. It has four pins: 5V power supply (Vcc), Trigger Pulse Input (TRIG), Echo Pulse Output (ECHO) and ground (GND). Through raspberry pi, we send an input signal to TRIG which then triggers the sensor to send ultrasonic pulse. ECHO remains low until sensor is triggered. When the sensor receives the waves it measures the time and then sends a 5V signal to ECHO. We have used a voltage divider to feed the signal coming from

ECHO to the GPIO pin of raspberry pi as it is rated at 3.3V but ECHO is rated at 5V. After this sensor detects a distance reduced more than a particular threshold distance, as specified in the code (i.e. due to an obstruction in the path), it sends a high bit to the attached Raspberry Pi.

V Conclusion

We surveyed and described various architecture, operation, design, and experimental performance of a low cost ultrasonic distributed security system for intrusion detection. Further, model was proposed using IoT based devices which can be easily expanded to include various additional features, functionalities and services. For example, the password/deactivation mechanism could be replaced from the current button-input style to a traditional PIN based system or even a voice-command based activation/deactivation of certain part of this security system. Also, in order to completely monitor all activity near the home premises, multiple Raspberry Pi computers can be integrated instead of just one. Such Raspberry Pi computers would be located outside possible entry points into the house such as windows, vents, etc., and not just the main door. Since the Raspberry Pi single board computers operate independently of the microcontroller based unit in our implementation, such expansion would be extremely easy.

REFERENCES

[1] M. L. R. Chandra, B. V. Kumar, and B. SureshBabu, “Iot enabled home with smart security,” in *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, Aug 2017, pp. 1193–1197. [Online]. Available: https://doi.org/10.1109/ICECDS.2017.8389630

[2] B. Chung, J. Kim, and Y. Jeon, “On-demand security configuration for iot devices,” in *2016 International Conference on Information and Communication Technology Convergence (ICTC)*, Oct 2016, pp. 1082–1084. [Online]. Available: https://doi.org/10.1109/ICTC.2016.7763373

[3] H. Geng, *SMART HOME SERVICES USING THE INTERNET OF THINGS*. Wiley, 2017. [Online]. Available: https://doi.org/10.1002/9781119173601.ch37

[4] W. Qin, B. Li, J. Zhang, S. Gao, and Y. He, “Design and implementation of iot security system towards campus safety,” in *Advanced Technologies in Ad Hoc and Sensor Networks*, X. Wang, L. Cui, and Z. Guo, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 299–312.

[5] P. K. Madupu and B. Karthikeyan, “Automatic service request system for security in smart home using iot,” in *2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, March 2018, pp. 1413–1418. [Online]. Available: https://doi.org/10.1109/ICECA.2018.8474684

[6] T. T. Brooks, *A Secure Update Mechanism for Internet of Things Devices*. IEEE, 2017. [Online]. Available: https://doi.org/10.1002/9781119193784.ch3

[7] S. Evdokimov, B. Fabian, O. Günther, L. Ivantysynova, and H. Ziekow, *RFID and the Internet of Things: Technology, Applications, and Security Challenges*. now, 2011. [Online]. Available: https://doi.org/10.1561/0200000020

[8] L. Dong, L. Wang, and Q. Huang, “Effects of metal plane in lc passive wireless sensors,” *IEEE Sensors Letters*, vol. 2, no. 1, pp. 1–3, March 2018. [Online]. Available: https://doi.org/10.1109/LSENS.2017.2788432

[9] P. Gamba, E. Goldoni, P. Savazzi, P. G. Arpesi, C. Sopranzi, J. Dufour, and M. Lavagna, “Wireless passive sensors for remote sensing of temperature on aerospace platforms,” *IEEE Sensors Journal*, vol. 14, no. 11, pp. 3883–3892, Nov 2014. [Online]. Available: https://doi.org/10.1109/JSEN.2014.2353623

[10] A. Bereketli and O. B. Akan, “Communication coverage in wireless passive sensor networks,” *IEEE Communications Letters*, vol. 13, no. 2, pp. 133–135, February 2009. [Online]. Available: https://doi.org/10.1109/LCOMM.2009.081691

[11] M. Steffanson and I. W. Rangelow, “Microthermomechanical infrared sensors,” *Opto-Electronics Review*, vol. 22, no. 1, pp. 1–15, Mar 2014. [Online]. Available: https://doi.org/10.2478/s11772-014-0176-0

[12] R. Ma, F. Hu, and Q. Hao, “Active compressive sensing via pyroelectric infrared sensor for human situation recognition,” *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 47, no. 12, pp. 3340–3350, Dec 2017. [Online]. Available: https://doi.org/10.1109/TSMC.2016.2578465

[13] E. H. Sargent, “Solution-processed infrared optoelectronics: Photovoltaics, sensors, and sources,” *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 14, no. 4, pp. 1223–1229, July 2008. [Online]. Available: https://doi.org/10.1109/JSTQE.2008.925766

[14] L. Korba, S. Elgazzar, and T. Welch, “Active infrared sensors for mobile robots,” *IEEE Transactions on Instrumentation and Measurement*, vol. 43, no. 2, pp. 283–287, April 1994.

[15] B. George, H. Zangl, T. Bretterklieber, and G. Brasseur, “A combined inductive–capacitive proximity sensor for seat occupancy detection,” *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 5, pp. 1463–1470, May 2010. [Online]. Available: https://doi.org/10.1109/TIM.2010.2040910

[16] B. George and H. Zangl and T. Bretterklieber and G. Brasseur, “A combined inductive-capacitive proximity sensor and its application to seat occupancy sensing,” in *2009 IEEE Instrumentation and Measurement Technology Conference*, May 2009, pp. 13–17. [Online]. Available: https://doi.org/10.1109/IMTC.2009.5168409

[17] G. Loukas, E. Karapistoli, E. Panaousis, P. Sarigiannidis, A. Bezemskij, and T. Vuong, "A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles," *Ad Hoc Networks*, vol. 84, pp. 124–147, 2019. [Online]. Available: https://doi.org/10.1016/j.adhoc.2018.10.002

[18] F. Khelifi, A. Bradai, A. Benslimane, P. Rawat, and M. Atri, "A survey of localization systems in internet of things," *Mobile Networks and Applications*, Aug 2018. [Online]. Available: https://doi.org/10.1007/s11036-018-1090-3

[19] O. Sonbul and A. N. Kalashnikov, "Low cost ultrasonic wireless distributed security system for intrusion detection," in *2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS)*, vol. 01, Sept 2013, pp. 235–238. [Online]. Available: https://doi.org/10.1109/IDAACS.2013.6662679