Chapter 19

TENSOR: A Technique to Enhance IoT Data Security using Bluetooth Low Energy Network for Smart Home Environment

A. Dalvin Vinoth Kumar[1], A.Vithya Vijayalakshmi[1] and Dr. L. Arockiam[2]

Abstract

The Internet of Things (IoT) refers to the inter-connectivity of devices and is enabled by the technologies such as RFID, Bluetooth, NFC, Wi-Fi, and Mobile Network. It is a Modern paradigm, rapidly growing around wireless communications. The capacity offered by the IoT make possible of developing large number of IoT applications such as Smart home, Smart city, smart health etc…,The communication technology used in IoT differs from application to application. The end devices /sensors are not always connected directly to internet, instead they are connected through the gateway. The security is the challenging task in IoT due to heterogeneity of devices. All security algorithms are not energy efficient. The proposed technique deals with data security in smart health environment. The duplication of data is identified by the location of end devices. The results prove that the proposed technique enhances the data security.

Keywords: IoT, Data security, Bluetooth low energy, communication technology, end devices security, BLE- sensor network.

Introduction

As in standard data mining, the aim in web mining is to determine and recover useful and attractive patterns from a huge dataset. There has been enormous interest towards web mining. In web mining, this dataset is the massive web data. Web data contains different kinds of information, including, web documents data, web structure data, web log data, and user profiles data. Two different approaches are projected on the definition of web mining. One approach is process-based and the other is data-based. Data-based definition is more widely accepted today. In this perspective, web mining is the application of data mining techniques to extract knowledge from web data, where at least one of structure or usage data is used in the mining process. There are no differences between web mining and data mining compared in general. All of web data can be mined mainly in three different dimensions, which are web content mining, web structure mining, and web usage mining.

[1] *Ph.D. Scholar, Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli, Tamilnadu, India.*

[2] Associate Professor, *Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli, Tamilnadu, India*

S. Vignesh and A. Philip Arokiadoss (ed.), *Statistical Approaches on Multidisciplinary Research,* Volume I

Introduction

Internet of Things (IoT) is a new era which allows communication between electronic devices. It is a methodology connecting the virtual world with the real world. IoT world builds an interaction between all physical objects such as cars, doors etc. [Mahmud et al., 2015]. Smart connectivity with existing networks and context-aware computation using network resources is an indispensable part of IoT [Jayavardhana et al., 2013]. IoT has huge potential for developing more new creative application in many fields [Eleonora et al., 2014]. There are so many IoT applications existed such as smart city, smart home, smart healthcare, agriculture and breeding, augmented maps, assisted driving etc. There are some IoT elements which show the functionality of IoT, each includes various key technologies of IoT.

Nowadays wireless communication systems are arising for home, city, healthcare, transport, agriculture etc. to improve our life quality [Ala Al-Fuqaha et al., 2015]. The main objective of these applications are to obtain information from devices, environment and also energy consumption monitoring. Among many IoT applications, smart home requires power consumption for monitoring systems and also for other devices [Mats Anderson et al., 2016]. Also the data security of home appliances connected with internet is one of the major issues. In this paper, we use Bluetooth Low Energy for sensor communication in smart home environment. The proposed work ensures originality of data by verifying the location of the sender. It refers to a periodic transfer of data. It mainly used for sensors, actuators or other small devices that require low power consumption.

Review of Literature

Jin-Shyan Lee et al. discussed and compared the low power communication standards such asBLE and ZigBee for various metrics such as power consumption, transmission time, and delivery ratio. They suggested the engineers to choose a relevant low-power wireless protocol. However, this comparison did not conclude a clear solution about the choice of the low-power wireless protocol. An architecture and design of Bluetooth Low Energy Controller was described by PawelWiecha et al. They have explained the Bluetooth system specified with the Bluetooth host and the controller with the layers involved in it. This architecture involved the Bluetooth controller and proposed to reduce the power consumption and minimizing the hardware area[Aihou Chen et al., 2015]. They proved that the division of hardware gives more flexibility. Also, the working of the architecture was implemented and verified by newest and advanced techniques. Many authors used similar technologies in IoT [Mohamad et al., 2016][Danijel et al., 2015][Yanzhen et al., 2016].

Almog Benin et al. discussed the security of existing standards such as Zigbee and Bluetooth Low Energy. Low-power wireless devices are not fully secured, it may end with the man-in-the–middle attack. They proposed three essential aspects in attaining secure association for connected devices namely a user-interface primitive, a new Message Recognition protocol (MRP) and a robust definition for MRPs security. They also proved that their MRP named PEBIUS holds the strongest security definition. MattiSiekkinen et al. focused on low power communication mechanisms mainly, Bluetooth Low Energy. They discussed and proved that when compared with Zigbee, the energy consumption of BLE is efficient by using certain measurements. The energy consumption measurements were done between the master and slave on both connected and dis-connected states. These measured values were compared with 802.15.4. They concluded that these measurement can vary when there is a change in number of packets transfers between the connected devices.

Mario Collotta et al. discussed the components of the smart home such as monitoring, innovative metering etc. When all such devices use more energy, then there is a demand of energy. Here, they proposed a novel energy management scheme/methodology for smart homes by using Bluetooth Low Energy for connected home appliances. This reduces the energy consumption chargers and the high-power peak load. They also proved that this approach reduces the peak load demand and the electricity charges. Ye Ding et al. proposed a remote mobile medical home monitoring system for the rehabilitation patients with chronic diseases outside the hospital. Wearable detection device was used to detect the physiological signals. BLE technologies were used to transfer the physiological data. Smart phone was used to store the function of display, data storage and also act as an alarm for monitoring. They used sensor nodes to collect physiological parameter values such as Blood Pressure Detection, Infrared Ear Thermometer Detection, ECG Detection and Detection of Blood-Oxygen and Pulse-rate to detect and provide the physiological data.

Proposed Methodology: TENSOR

The proposed work TENSOR( ) uses three phases namely network topology construction, Location computation, and Trust validation. BLE communication technology is used in this scenario. The applications of IoT like smart home, smart health the sensor nodes are installed to sense various data like temperature, humidity, heart beat rate etc. The physical set up of these sensors are termed as network topology construction. The sensor/ end nodes are not capable of communicating with the internet directly. However, relay nodes are used as intermediate nodes to communicate with the internet. In a smart home environment the cctv cameras are used for surveillance. The camera nodes are connected with the power line communication to communicate with internet. These nodes are used to validate the data sent by the sensors. This phase is termed as trust validation. The location information of the sensor is used as the parameter to validate trust. The location of the sender node is computed dynamically in the location computation phase. The algorithm for proposed work is as follows:

TENSOR( )

Step 1: Construct the Network Topology
Step 2: If a Relay Node (r_i) receives data from end node (e_i).
Step 3: Compute the location of end node using Received Signal Strength (RRSI)Location (e_i)
Step 4: Validate the universal unique Identification (UUId) and Location of the end node.
Step 5: Forward the data to the Gateway
Step 6: Update the data in the cloud server

Construct ( )

The Network topology construction for IoT varies from Application to Application. In a smart home environment, the sensors are fixed in various locations. The sink node/gateway node acts as cluster head for sensor nodes. The sensor nodes are termed as end nodes, these end nodes sense the data and forward it to the parent node or directly to gateway node. The *Figure 19.1a* and *Figure 19.1b* show the topology construction for smart home environment. The end nodes are resource constrained nodes so they not connected directly to the internet, instead they are connected to the gateway (g_i).

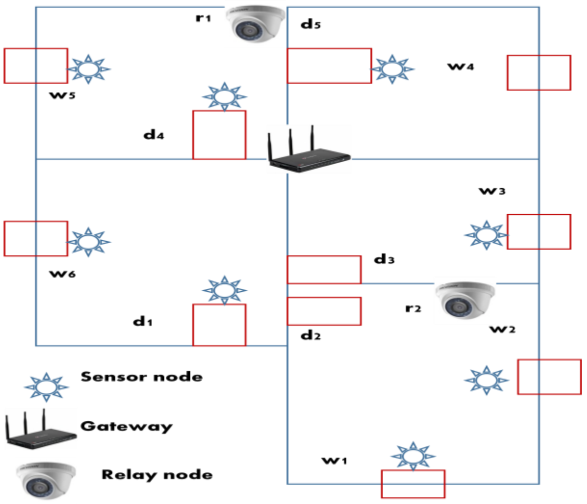


Figure 19.1a. Smart Home Environment

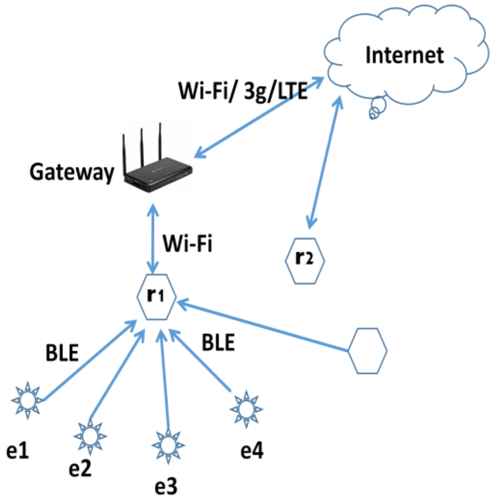


Figure 19.1b. Network Topology construction

The Relay node acts as intermediate node between end nodes. The relay node is not a router node. For example, the Surveillance camera with Power Line Communication (PLC) can act as a relay node. The node with PLC is not energy constrained so they are directly connected to the internet. In smart home environment, most of the nodes are static (mesh under routing). The physical location of the nodes are identified and stored in the gateway. The Universal unique Id (UUId) and location of the end device are maintained in a table as shown in the Table 19.1.

The location information of the end node calculated in two different environment namely in-door and out-door. The location in in-door is computed by the Received Signal Strength Indicator (RSSI) value. Out-door location is computed using reference node information. The RRSI value measured by the gateway is not exact received power in dBm. Whereas the RRSI value gives the condition of the received power level. It can be easily converted into received power by applying offset to compute the correct value. The obtained RRSI is converted by the processor into analog-to-digital (ADC).

Table 19.1. Neighbour Information Table in Gateway

Node	UUId	Location
e_i	$UUId_i$	$L(e_i)$
e_{i+1}	$UUId_{i+1}$	$L(e_{i+1})$
. .	. .	. .
e_{i+n}	$UUId_{i+n}$	$L(e_{i+n})$

$$P_r = 1/d^2 \tag{1}$$

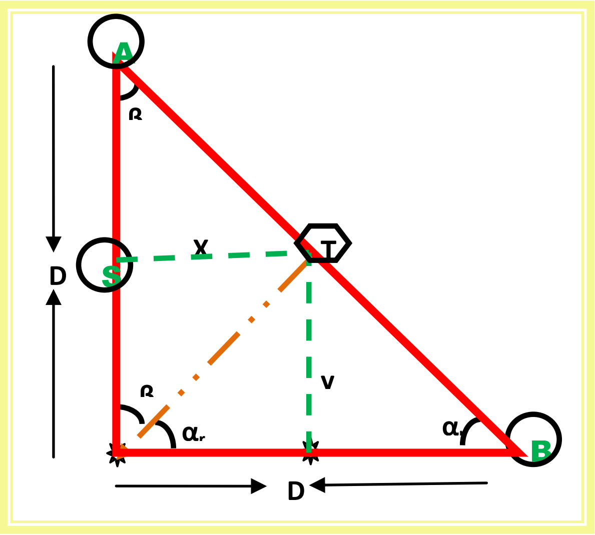
$$d^2 = 1/p_r \tag{2}$$

$$d = \sqrt{1}/pr \tag{3}$$

$$P_r(d) = pw_r(d0) - 10 * n * \log_{10} (d1/d0) \tag{4}$$

$$N_d = \frac{p_r(d1) - p_r(do)}{10 * \log_{10}(d1/d0)} \tag{5}$$

P is the power and d is the distance, the power loss Pr is inversely related to the distance square as shown in equation 1. Out-door node location calculation is performed using the reference of the neighbour node. The location information is computed with trigonometry formula as shown in *Figure 19.2*. Where T is the target node S is the server node and A & B are reference nodes.



$$X = \frac{d_y Sin(\beta r1) \; sin(\beta r2)}{d_y Sin(\beta r1 + \beta r2)} \tag{6}$$

$$Y = \frac{d_x \; Sin(\alpha r1) \; sin(\alpha r2)}{d_x \; Sin(\alpha r1 + \alpha r2)} \tag{7}$$

Figure 19.2. Location calculation using Reference node

The distance between source and target node is calculated using the trigonometry. The reference nodes are assumed in the triangular position. The value of X and Y are calculated as like equation 6 & 7. The acute angle of the triangle 1 is referred as α and obtuse angle of the triangle 2 is referred as β. The acute angle of triangle 2 is calculated by (Π – β). The location information of the node is validated. The data is updated only when the UUId and location are true. The proposed work increase the probability of updating the original data thus the data reliability is increased. The *Figure 19.3a* shows the probability of attacker node and *Figure 19.3b* shows when attacker node increases fake data rate increases.

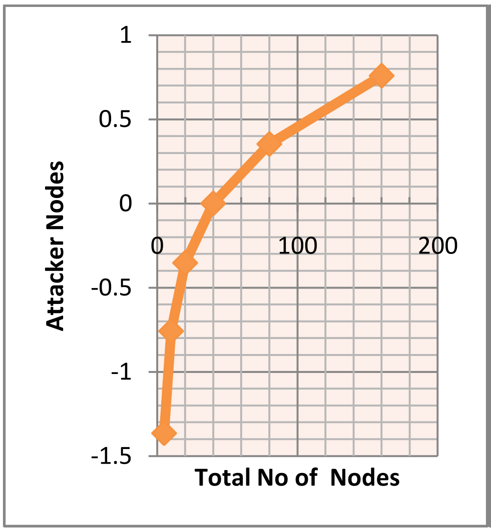


Figure 19.3a.Probability of Attacker node

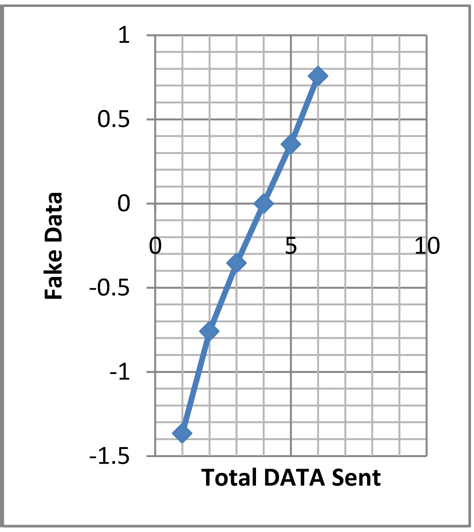


Figure 19.3b. Probability of Attacker node

Conclusion

IoT devices are resource constrained devices. The security algorithm like AES is not able to incorporate into these sensor nodes. The proposed work ensures the originality of the data. Trust of the data is ensured by the context information of sending node. The proposed work uses the location information of the sender as context to validate the data. It uses two different techniques to compute the location for in-door and out-door nodes. The probability of updating fake data is reduced and the quality of service in data security is enhanced.

References

Aihou Chen, Aurora Gil-de-Castro, Emilio J. Palacios-García, Jose M. Flores-Arias and Francisco J.Bellido-Outeirino, “In-Home Data Acquisition and Control System Based on BLE”, IEEE International Symposium on Consumer Electronics (ISCE), 2015, pp. 1- 2.

Ala Al-Fuqaha, Guizani, Mehdi Mohammadi, Mohammed Aledhari and MoussaAyyash, “Internet of Things: A Survey on Enabling Technologies, Protocols and Applications”, IEEE Communications Surveys & Tutorials, 2015, Vol.17, Iss. 4, pp. 2347 – 2376.

Almog Benin, Sivan Toledo and EranTromer, “Secure Association for the Internet of Things”, IEEE International Workshop on Secure Internet of Things, 2015, pp. 25 -34.

DanijelCabarkapa, Ivana Grujic and PetarPavlovic, “Comparative Analysis of the Bluetooth Low-Energy Indoor Positioning Systems”, IEEE, TELSIKS, 2015, pp. 76- 79.

Eleonora Borgia, “The Internet of Things vision: Key features, applications and open issues”, Elsevier, Computer Communications, 2014, pg. 1–31.

JayavardhanaGubbi, RajkumarBuyya, SlavenMarusic and MarimuthuPalaniswami, “Internet of Things (IoT) A Vision, architectural elements, and future directions”, Elsevier Future Generation Computer Systems, 2013, pg. 1645-1660.

Jin-Shyan Lee and Ming-Feng Dong, “A Preliminary Study of Low Power Wireless Technologies: ZigBee and Bluetooth Low Energy”, IEEE Conference on Industrial Electronics and Applications, 2015, pp. 135 – 139.

Mario Collotta and Giovanni Pau, "A Novel Energy Management Approach for Smart Homes Using Bluetooth Low Energy", IEEE Journal on Selected Areas in Communications, 2015, vol. 33, no. 12, pp. 2988 – 2996.

Mats Anderson, "Use Case Possibilities with Bluetooth Low Energy in IoT Applications", u-blox whitepaper, 2016, pp. 1- 16.

MattiSiekkinen, Markus Hiienkari, Jukka K. Nurminen and JohaanaNieminen, "How Low Energy is Bluetooth Low Energy? Comparative Measurements with ZigBee/802.15.4", Workshop on Internet of Things Enabling Technologies, Embracing Machine-to-Machine Communications and Beyond, 2012, pp. 232-237.

Md. Mahmud Hossain, MaziarFotouhi, and RagibHasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things", IEEE World Congress on Services, 2015, pg. 21-28.

Mohamad Omar Al Kalaa, WalidBalid, NaimBitar, and Hazem H. Refai, "Evaluating Bluetooth Low Energy in Realistic Wireless Environments", IEEE Wireless Communications and Networking, 2016, pp. 1- 6.

PawelWiecha, MarekCieplucha, PatrykKloczko and Witold A. Pleskacz, "Architecture and Design of a Bluetooth Low Energy Controller", International Conference on Mixed Design of Integrated Circuits and Systems (MIXDES), 2016, pp. 164 – 167.

YanzhenQu and Philip Chan, "Assessing Vulnerabilities in Bluetooth Low Energy (BLE) Wireless Network based IoT Systems", IEEE International Conference on Big Data Security on Cloud, IEEE International Conference on High Performance and Smart Computing, IEEE International Conference on Intelligent Data and Security, 2016, pp. 42 – 48.

Ye Ding, Shi Gang and Jiang Hong, "The Design of Home Monitoring System by Remote Mobile Medical", IEEE International Conference on Information Technology in Medicine and Education, 2015, pg. 278 – 281.