ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Analysis of Energy Efficient Sensor Cloud

Sneha N.P

Assistant Professor, Dept. of Computer Science and Engineering, Academy for Technical and Management Excellence, Mysore, India

ABSTRACT: While discussing sensor networks, energy and the sensors' location is crucial information to be considered. Each sensor node is powered by a battery that is not rechargeable and is not possible to change. Sensor nodes deployed in hostile environments are vulnerable to attacks like wormhole attacks, pollution attacks etc. It is necessary to verify the sensors' location before they can be used by location based applications and to place sensing devices like heat monitoring devices at various places. Previous verification schemes either require group-based deployment knowledge of the sensor field or depend on expensive, dedicated hardware. In this paper we suggest how the battery life of the sensor can be increased and we uselight weight location verification system that performs both on-spot and in-region location verifications.

KEYWORDS: Wireless sensor networks, sensor nodes, sensor cloud, localization, verification, energy efficiency, on-spot and in-region.

I. INTRODUCTION

Knowing the location of sensor nodes is very important for many applications such as environment monitoring sound, temperature, pressure, motion, vibration, pollution and target tracking as well as geographical routing. [1],[2] Each node in a sensor network consists of a radio transceiver or any other wireless communication device, a small microcontroller and an energy source most commonly cell/battery. These batteries power the sensor nodes to carry out the required task. Therefore it is necessary to conserve the battery power so that it can perform for a longer duration of time. Sensor nodes basically consist of three parts: sensing, processing and communicating [3]. Accelerometer sensor, thermal sensor and microphone sensor are some of the most commonly used sensor devices deployed in sensor network as sensor nodes. Currently wireless sensor networks are used in several areas like healthcare, hazardous environment exploration, defence such as military target tracking and surveillance [4],[5], government and environmental services like natural disaster relief [6] and seismic sensing [7] and so forth. However, sensor networks have to face many issues and challenges. Sensors' localization is subjected to many malicious attacks like attackers can compromise sensors and inject false information; they can also interrupt signal transmission between sensors. Hence location estimated in localization process are not always correct even though some secure localization algorithms [8], [9], [10], [11], were proposed. Therefore, we classify previous location verification algorithms into two categories, namely, on-spot verification and in-region verification. On-spot verification is to verify whether a sensors' true location is the same as its estimated location. Most existing verification algorithms [12], [13], [14], [15], [16] belong to this category. Other than the on-spot verification some effort has been given to designing in-region location verification algorithm. A protocol named echo was proposed to verify if a sensor is inside a physical region such as a room, a building or even a stadium. The verification result will allow a decision whether to assign sensors the accessing right to some resources in that physical region. However sensor networks face many issues and challenges regarding their communication and resources. Wireless sensor network has its own resource and design constraints which are application specific and dependant on monitored environment. Fewer nodes are required to form a network for monitoring a small area, whereas huge numbers of sensor nodes are required for the coverage of larger area. While monitoring larger environment, there is a possibility of limited communication between nodes. The emergence of cloud computing is seen as a remedy. Cloud computing has been evolved as the future generations computing paradigm.

The US NSIT (national institute of Standards and technology) defines the concept of cloud computing as follows : cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable, computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with management effort or service provider interaction [17]. Cloud computing allows the users and systems to

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

use a Platform as a Service (PaaS) for e.g., operating systems (OS), infrastructure as a Service (IaaS), for e.g., application level programs, and so forth at a very low cost which are being provided by several cloud providers (e.g., Amazon, Google and Microsoft) on the basis of pay per use service[18]. Cloud computing platform dynamically provisions, configures and reconfigures the servers as needed by the end users. Servers in cloud can be in the form of virtual machines or physical machines. Cloud computing renders two major trends in IT: (1) efficiency achieved through highly scalable, and hardware and software resources, and (2) agility, which is achieved through parallel batch processing, using computer intensive business analytics and real time mobile interactive applications that respond to user requirements [19]. The benefits of cloud computing is that the end user need not worry about the exact location of servers. Sensor cloud has been evolved and proposed by several IT people. Sensor cloud infrastructure [20] is an extended form of cloud computing, sensor cloud service architecture is introduced as an integration of cloud computing into the wireless sensor network to innovate a number of other new resources. This integration overcomes shortfalls of wireless sensor networks like storage capacity of data collected in sensor nodes and processing of these data. Cloud computing provides a vast storage capacity and processing capabilities, hence it enables collecting huge amount of sensor data by linking the WSN and cloud through the gateways that is the sensor gateway and the cloud gateway. Sensor gateway collects information from the sensor nodes, compresses it and transmits it back to the cloud gateway which in turn recompresses it and stores it in the cloud storage server [21].

II. LITERATURE SURVEY

The localization schemes applied for wireless sensor networks are compromised by malicious attackers who can launch wormhole attack, range enlargement/reduction attacks. Sensor cloud is a new paradigm for cloud computing that causes physical sensor's to accumulate data and transmit all sensor data into a cloud computing infrastructure. The sensor cloud handles sensor data very efficiently.

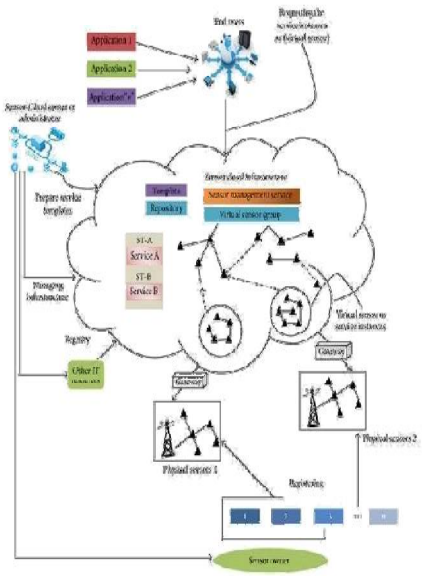

Fig 2.1: Sensor Cloud Infrastructure.

In fig 2.1, we can see how a sensor cloud works. Here, the physical sensor is owned by the sensor owner and these sensors sense the data during certain events.

The cloud has a virtual sensor to which these sensors will be mapped as the end user cannot access the physical sensor that is located in some unknown location. Hence the user need not know the actual location of the sensors. The virtual sensors are grouped so that the users can access other applications. The sensor cloud is managed by the sensor cloud owner.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Lazos et al proposed SeRLoc[L. Lazos and R. Poovendran, "SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks," Proc. ACM Workshop Wireless Security (WiSe), 2004.] which utilizes directional equipped on anchors to overcome wormhole attacks.

On further edition to SeRLoc they later introduced high resolution robust localization for wireless sensor networks HiRLoc [L. Lazos and R. Poovendran, "Hirloc: High-Resolution Robust Localization for Wireless Sensor Networks," Proc. IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 233-246, Feb. 2006] . This algorithm also makes use of directional antennas but the communication range of location is variable.

The location verification problem was first addressed , in which Sastry et al[N. Sastry , U.Shankar, and D.Wagner, "Secure Verification of Location Claims", Proc. ACM Workshop Wireless security,2003] proposed Echo protocol to verify if a device is inside some physical region, such as a room or a football stadium. The Echo protocol is mainly used to provide location-based access control, and cannot be directly applied for location verification in other applications.

Capkun and Hubaux [S.Capkun and J.P.Hubaux, "Secure Positioning of Wireless devices with Application to Sensor Networks", Proc. IEEE INFOCOM, 2005.] proposed a Verifiable Multilateration technique to verify whether a sensor's estimated location is at its true location using the distance bounding protocol.

Capkun and others proposed [S.Capkun, M.Cagalj, and M.Srivastava, "Secure Localization with Hidden and Mobile Base Station", Proc .[IEEE INFOCOM, 2006] Covert base station which can keep their existence and communications unknown to sensors.

Coming to sensor cloud, MicroStrain defines sensor cloud as follows "it is a unique sensor data storage ,visualization and remote management platform that leverage [sic] powerful cloud computing technologies to provide excellent data scalability, rapid visualization, and user programmable analysis . It is originally designed to support long-term deployments of MicroStrain wireless sensor, Sensor-Cloud now supports any web connected third party device, sensor, or sensor network through a simple OpenData API" [22].

A sensor cloud collects and processes information from several sensor networks, enabling information sharing. It also integrates several networks with the number of sensing applications and cloud computing platform by allowing applications to be cross-disciplinary that may span over multiple organizations[23]. In sensor network sensors are utilized according to the applications and this application handles both sensor data and the sensor itself such that other applications cannot use this, which causes wastage of valuable sensor resource. To overcome this virtualizing the physical sensor is necessary. These virtualized sensors on a cloud computing platform are dynamic in nature.

Within the Sensor-Cloud infrastructure, to obtain QoS , the virtual sensor are monitored regularly so users can destroy it when they become meaningless[24].

Nimbit is a free and social service that is used to record and share sensor data on cloud. Nimbit provides alert management mechanism, data compression mechanism etc.

Pachube is one of the first online database service provider which allows to connect sensor data to the web. This system provides free usage and has several number of interfaces for producing sensor or mobile based applications.

III. EXISTING SYSTEM

A large number of localization schemes were proposed in recent years for WSN. Localization schemes can be compromised by malicious attackers, who can launch wormhole attack, range enlargement/reduction attacks, many secure localization schemes are designed.Lazos et al. proposed SeRLoc , which utilizes directional antennas equipped on anchors to detect worm- holes. As an improvement to the SeRLoc, they later introduced High-resolution Robust Localization for WSNs (HiRLoc). Since these algorithms run on sensors that have limited resources, some improvement methods have been developed for fast computing of regional intersections.The energy consumed during data communication in a sensor cloud may drain the battery that powers each sensor node. This may lead to the death of the sensor node which needs to be changed. This becomes a problem during an emergency such as a bomb blast or natural disaster. This way the data is unresolved. So the sensed data can be compressed in order to save energy and uploaded to the sensor cloud to be used in future. In WSN LZW algorithm was used. Here we try using a simple lossless algorithm that is better than LZW when it comes to energy consumption.However, since sensors may not be innocent, that is, they can easily be compromised and tend to report false locations. Therefore location verification is necessary to defend against such attacks. Echo protocol was proposed to verify if a device was inside a physical region. The following section gives the solution for the above considered problem.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

IV. PROPOSED SYSTEM

The data must be transferred from the sensors to the sensor cloud platform. It has to be compressed and encrypted to secure the data and this data must then be sent from the sensor to the sensor cloud platform.

This paper proposes an algorithm to compress the data from the sensor to the sensor cloud platform. We use a commitment based scheme to provide security. The sensors and the sensor cloud application negotiate the key for every periodic interval of time. Here a simple lossless algorithm that uses the data from the Huffman coding table can be used which is as below,

encode(di, Table)
IF di=0 THEN
SET ni TO 0
ELSE
SET ni TO $\log_2(|di|)$
category
ENDIF
SET si TO Table[ni]
IF ni=0 THEN
SET bsi TO si
ELSE
IF di>0 THEN
SET ai TO $(di)|_{ni}$
ELSE
SET ai TO $(di-1)|_{ni}$
ENDIF
SET bsi TO <<si,ai>>
ENDIF
RETURN bsi

Table 4.1: Huffman Variable length codes

n_i	s_i	d_i
0	00	0
1	010	-1,+1
2	011	-3,-2,+2,+3
3	100	-7,..,-4,+4,...,+7
4	101	15,...-8,+8,...,+15
5	110	-31,...,-16,+16,..,+31
6	1110	-63,..,-32,+32,..,+63
7	11110	-127,..,-64,+64,..,+127
8	111110	-255,..,-128,+128,..,+255
9	1111110	-511,..,-256,+256,..,+511
10	11111110	-1023,..,-512,+512,..,+1023
11	111111110	-2047,..,-1024,+1024,..,+2047
12	1111111110	-4095,..,-2048,+2048,..,+4095
13	11111111110	-8191,..,-4096,+4096,..,+8191
14	111111111110	-16383,..,-8192,+8192,..,+16383

The number of bits that has to be transferred is reduced by applying the compression algorithm and hence less energy is spent on transferring the data to the sensor cloud. Hence the battery life of the sensor cloud is increased.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

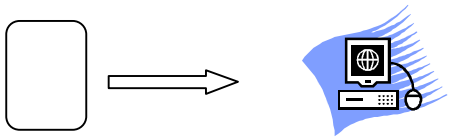

Fig 4.1: Sending data

In order to verify the sensors' location, we develop a mobile application which sends data such as latitude, longitude and vibration values to the sensor cloud which has to decrypt the message in order to receive the information sent by the android application.

A. Verification process

The first step in the verification process is that each sensor broadcasts its ID within its communication range and meanwhile overhears the IDs broadcast by other sensors. We denote sensor Si's neighbourhood observation by Oi. As an example, Fig. 4.2 shows a scenario where sensors are localized accurately with zero errors. The solid circles and the hollow circles represent sensors' true and estimated locations, respectively. Sensor S0's true location is L = (x_0, y0) and its communication range is the big dashed circle. Because sensor S1, S2, S3, S4 is in the communication range of sensor S0, their ID messages can reach S0. Hence, sensor S0's neighbourhood observation is O0 = (S1, S2, S3, S4). Then, each sensor sends its neighbourhood observation and its estimated location to the VC. The VC will analyze all the information collected from sensors and detect if there is any inconsistency.

The intuition is that when sensors are correctly localized with small localization errors, then their neighbourhood observations should be consistent with their estimated locations. For example, in Fig. 4.2, all sensors are localized with ZERO errors. The distance between the estimated locations of S0 and S1 is less than the radius R, which is consistent with the fact that they can observe each other. Based on this intuition, GFM algorithm organizes all the information in the form of matrix to find information inconsistencies. The GFM algorithm is as follows,

Algorithm GFT Algorithm

```
1: assign an initial trustability indicator 0.5 to all
sensors
2: for round k=1 to N
3:    for each sensor Si
4:     update Si's indictor from Ik-1 to Ik
5:       if Ik> threshold
6:            accept sensor Si and stop updating its
indicator
7:       if Ik – Ik-1< 0.05
8:            stop updating the indicator for Si in future
rounds
9: verify sensors with indicators greater than the
threshold
```

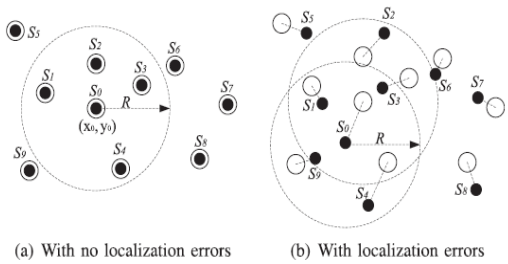

Fig 4.2: Snapshot of sensor field

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

B. In-Region & On-Spot Verification

Here we describe verification system in which the VC can effectively determine if sensors' estimated locations are trustable. According to the requirements of different applications, the system should provide either on-spot or in-region verification results.

On-spot verification is to verify whether a sensor's localization error is less than a certain distance. Let L_{true} and L_{est} denote the true location and the estimated location of a sensor, then the verification fails if the following condition holds true: $jL_{true} \_ L_{est}> D$, where D is named the Anomaly Degree. The value of D should be set properly with the considerations of the application requirements and the value of "normal" localization errors that are present in no-attack environment. In this paper, we consider D as an input parameter and assume its value has already been given to our system.

In-region verification is to verify whether a sensor is inside a physical region or not. The region may be different for each location-based application. Given an application, we define a physical region in which if a sensor can be verified, then the application goal can be achieved. Application goal is fulfilled, Li€Vi, where Li is the location of sensor Si, and Vi is the verification region.

The in-region verification algorithm is as follows:

Algorithm: In-region Verification Algorithm
1: Find confirmed neighbours for sensor S_i
2: Determine scored districts D_il, ..., D_{im}
3: **for** each district D_{ij}
4: calculate in-district probability Pr(D_{ij})
5: calculate pdf or pmf for continuous or discrete distribution
6: calculate in-region confidence
7: **if** continuous distribution
8: perform two-dimensional integral using pdf
9: **else**
10: perform addition on all points' probabilities using pmf

V. IMPLEMENTATION

In this paper we describe a method to reduce the battery power spent on the transfer of data in a low cost sensor network. The devices are registered and transfer of compressed data between the sensors is done using the LZW algorithm. A large amount of energy is saved and hence the proposed algorithm is found to be more energy efficient. The data to be transferred is compressed to maintain data security and the sensors' location is verified with on-spot and in-region verification algorithms with high detection rate and low false positive rate.

VI. CONCLUSION

In this paper we have proposed a light weight location verification system that performs both on-spot and in-region location verification of energy efficient sensor nodes using sensor cloud. Our proposed verification system is more light weight, effective, energy efficient and robust. We have also introduced a new way to expose platform capabilities as service blocks for developing applications on the top of application platform. It yields satisfactory verification results to a variety of applications and is resilient to malicious attacks and can be used in hostile environments.

REFERENCES

[1] K. Romer and F. Mattern, "The design space of wireless sensor networks," *IEEEWireless Communications*, vol.11,no. 6, pp. 5461, 2004.
[2] T. Haenselmann, "Sensor networks,"GFDL Wireless Sensor Network textbook 2006.
[3] I. F. Akyildiz,W. Su,Y. Sankarasubramaniam, and E.Cayirci,"A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, 2002.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

[4] G. Simon, G. Balogh, G. Pap et al., "Sensor network-based countersniper system," in *Proceedings of the 2nd InternationalConference on Embedded Networked Sensor Systems (SenSys '04)*, pp. 1–12, Baltimore,Md,USA,November 2004.
[5] S. K. Dash, J. P. Sahoo, S. Mohapatra, and S. P. Pati, "Sensorcloud: assimilation of wireless sensor network and the cloud," in *Advances in Computer Science and InformationTechnology.Networks and Communications*, vol. 84, pp. 455–464, Springer-Link, 2012.
[6] M. Castillo-Effen, D. H. Quintela, R. Jordan,W.Westhoff, and W.Moreno, "Wireless sensor networks for flash-flood alerting," in *Proceedings of the 5th IEEE International CaracasConference on Devices, Circuits and Systems (ICCDCS '04)*,pp. 142–146, November 2004.
[7] G. Werner-Allen, K. Lorincz, M. Welsh et al., "Deploying a wireless sensor network on an active volcano," *IEEE Internet Computing*, vol. 10, no. 2, pp. 18–25, 2006.
[8]. L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks," Proc. 11th Network and Distributed SystemSecurity Symp., 2003.
[9] Y. Hu, A. Perrig, and D. Johnson, "Packet Leashes: A Defenseagainst Wormhole Attacks in Wireless Ad Hoc Networks," Proc.IEEE INFOCOM, 2003.
[10] L. Lazos and R. Poovendran, "SeRLoc: Secure Range-IndependentLocalization for Wireless Sensor Networks," Proc. ACMmWorkshopWireless Security (WiSe), 2004.
[11] Z. Li, W. Trappe, Y. Zhang, and B. Nath, "Robust StatisticalMethods for Securing Wireless Localization in Sensor Networks,"Proc. Fourth Int'l Symp.Information Processing in Sensor Networks(IPSN '05), 2005.
[12] S. Brands and D. Chaum, "Distance-Bounding Protocols," Proc.Workshop the Theory and Application of Cryptographic Techniques onAdvances in Cryptology (EUROCRYPT '93), pp. 344C359, 1994.
[13] S. Brands and D. Chaum, "Distance-Bounding Protocols," Proc.Workshop the Theory and Application of Cryptographic Techniques onAdvances in Cryptology (EUROCRYPT '93), pp. 344C359, 1994.
[14] S. Capkun, M. Cagalj, and M. Srivastava, "Secure Localizationwith Hidden and Mobile Base Stations," Proc. IEEE INFOCOM, 2006.
[15] W. Du, L. Fang, and P. Ning, "LAD: Localization AnomalyDetection for Wireless Sensor Networks," Proc. IEEE Int'l Parallel and Distributed Processing Symp. (IPDPS '05), 2005.
[16] L. Lazos, R. Poovendran, and S. Capkun, "ROPE: Robust PositionEstimation in Wireless Sensor Networks," Proc. Fourth Int'l Symp. Information Processing in Sensor Networks (IPSN '05), 2005.
[17] S. K. Dash, J. P. Sahoo, S. Mohapatra, and S. P. Pati,"Sensorcloud: assimilation of wireless sensor network and the cloud," in *Advances in Computer Science and InformationTechnology.Networks and Communications*, vol. 84, pp. 455–464, Springer-Link, 2012.
[18] H. T.Dinh, C. Lee, D. Niyato, and P. Wang, *A SurveyofMobile Cloud Computing: Architecture, Applications, andApproaches*,Wireless Communications and Mobile Computing-Wiley Online Library, 2011.
[19] W. Kim, "Cloud computing: today and tomorrow," *Journalof Object Technology*, vol. 8, pp. 65–72, 2009.
[20] M. Yuriyama and T. Kushida, "Sensor-cloud infrastructurephysical sensor management with virtualized sensors on cloudcomputing," in *Proceedings of the IEEE 13th InternationalConference on Network-Based Information Systems(NBiS'10)*, pp. 1–8, September 2010.
[21] L. P. D. Kumar, S. S. Grace, A. Krishnan, V. M. Manikandan, R. Chinraj, and M. R. Sumalatha, "Data filtering in wireless sensor networks using neural networks for storage in cloud," in *Proceedings of the IEEE InternationalConferenceon Recent Trends in Information Technology(ICRTIT '11)*,2012.
[22] Sensor-Cloud, http://sensorcloud.com/system-overview.
[23] K. T. Lan, "What's Next? Sensor+Cloud?" in *Proceeding of the 7th International Workshop on Data Management for Sensor Networks*, pp. 978–971, ACM Digital Library, 2010.
[24] U. Varshney, "Pervasive healthcare and wireless health monitoring," *Mobile Networks and Applications*, vol. 12, no. 2-3, pp. 113–127, 2007.