Light Weight Location Verification Algorithm in Wireless Sensors for Checking the Reliability of Data

Puneet Singhania
(Author)
Dept of Information Science and Engineering,
The National Institute of Engineering,
Mysore-570008,Karnataka,India
puneetsinghania2002@gmail.com

C. N. Chinnaswamy
(Author, Associate Professor)
Dept of Information Science and Engineering,
The National Institute of Engineering,
Mysore-570008,Karnataka,India
chinnaswamynie@gmail.com

Dr. T. H. Sreenivas
(Author, Professor)
Dept of Information Science and Engineering,
The National Institute of Engineering,
Mysore-570008,Karnataka,India
Sreeni_th@hotmail.com

Rahul Srivastava
(Author)
Dept of Information Science and Engineering,
The National Institute of Engineering,
Mysore-570008,Karnataka,India
rahulsrinie@gmail.com

Ravi Priya
(Author)
Dept of Information Science and Engineering,
The National Institute of Engineering,
Mysore-570008,Karnataka,India
ravibk9078@gmail.com

Shashi Raj
(Author)
Dept of Information Science and Engineering,
The National Institute of Engineering,
Mysore-570008,Karnataka,India
rajshashi3@gmail.com

***Abstract*—** Wireless sensors can be deployed in any environment, even if that is hazardous and they send back the data gathered to the verification center which is placed at some safe location. Since the data collected by these are very vital so any compromisation may lead to undesirable results. Sensors can be easily compromised by changing its actual position to some false position so there is need for some algorithm to verify the position and ensure that the data is unblemished. Since in previous scheme, heavy and expensive equipments were used along with the deployment knowledge required, it becomes inefficient for all cost range. Therefore, we have proposed a verification system which utilizes the concept of on-spot and in-region location verification. In on-spot verification, we calculate the distance of the wireless sensor from its actual deployed position. In-region verification depends upon neighbouring sensors. Along with that, once a sensors gets out of its tolerable region, even for once, its data gets discarded. Putting the sensors back to its original position after the discarding of the data won't make it trusted and the sensor will still be considered compromised. This additional feature ensures that the data received in the verification center is from a trusted device and is true.

Keywords- *Wireless sensor network; Verification*

++++

I. PREAMBLE

Wireless sensor networks consist of numerous portable sensors which can be deployed at any environments and are used to measure the values based on the significant parameters. They can be used in various monitoring systems. For example, they can be used forests for monitoring purposes where the movements of elephants are recorded base on the vibration values. They sense it, record the values and send it to the verification centre. It helps in effective monitoring. It can be used in mining locations also where the vibration value plays a very vital role. Any minor change in vibration values can lead to significant change in further processing and values can be affected vastly. A system can be used where encryption can be made on sensor itself, which is a very unique feature. Later it can be decrypted through IMEI at the verification centre.

II. SYSTEM STUDY AND ANALYSIS

a) EXISTING SYSTEM

In recent years, the location verification of the wireless sensors has been the main issue because the data collected from such sensors should be trustful and correct. The existing systems includes directional antennas but they could not screen the sensors from the malicious attack.Lazos et al proposed SerLOC[11] where directional antennas with worm-hole detection anchors are used.With further advancement the SerLOC was introduced with high resolution robust Localisation whose primary work is to remove the false location data. These sensors have very limited computational power so several different techniques of regional overlapping is used. If a sensor is not functioning from correct location or not optimal the data centre is addressed about it. The Localization problem as first conveyed by Shastry et al [] proposed to verify the position of the system within boundaries. The echo protocol mainly to provide location based access control and cannot be used for verification of the location.

b) PROPOSED SYSTEM

We proposed to develop a system that will be applicable for all cost range sensor networks with very high accuracy of the location of all sensors within a particular network.We will register the data and keep track of its location and once the sensor is out of tolerance region,the data received from that node will be considered as compromised.The verification of the sensor device will be done by on-spot and in-region verification methods.

III. LTERATURE SURVEY

- The localization schemes applied for wireless sensor networks are compromised by malicious attackers who can launch wormhole attack, range enlargement/reduction attacks.

- So 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 which directional antennas equipped on anchors to detect wormholes.

- As an improvement 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.

IV. SYSTEM DESIGN

a) ARCHITECTURAL DESIGN

Software architecture is used to project business and functional identity by higher architecture levels into application. It is the structure of the system which comprises software components, the externally visible properties of these components and the relationship between them. It is high levels abstract and logical design.

Fig.4.1 Architectural Design

Fig.4.1 shows Architectural Design of the lightweight location verification system .one unique feature is that data is encryption is done at the sensors nodes itself. Then it is sent to the verification centre where it is decrypted using IMEI number. Here, If the node exists or is already registered at the verification centre, it checks whether the node is from a trustable location or not. The data is decrypted only if it is from a trusted location and the algorithm being used is GFM algorithm. If it is not from a trusted location, then the entire data is discarded and it indicates clearly that the node has been compromised even it is moved away from the trusted location for even a few nanoseconds.

b) HIGH-LEVEL DESIGN

High-level design provides an overview of entire system, identifying all its elements at some level of abstraction. This contrasts with low level design which exposes the detailed design of each of these elements.

 ISSN: 2321-8169
3074 - 3078

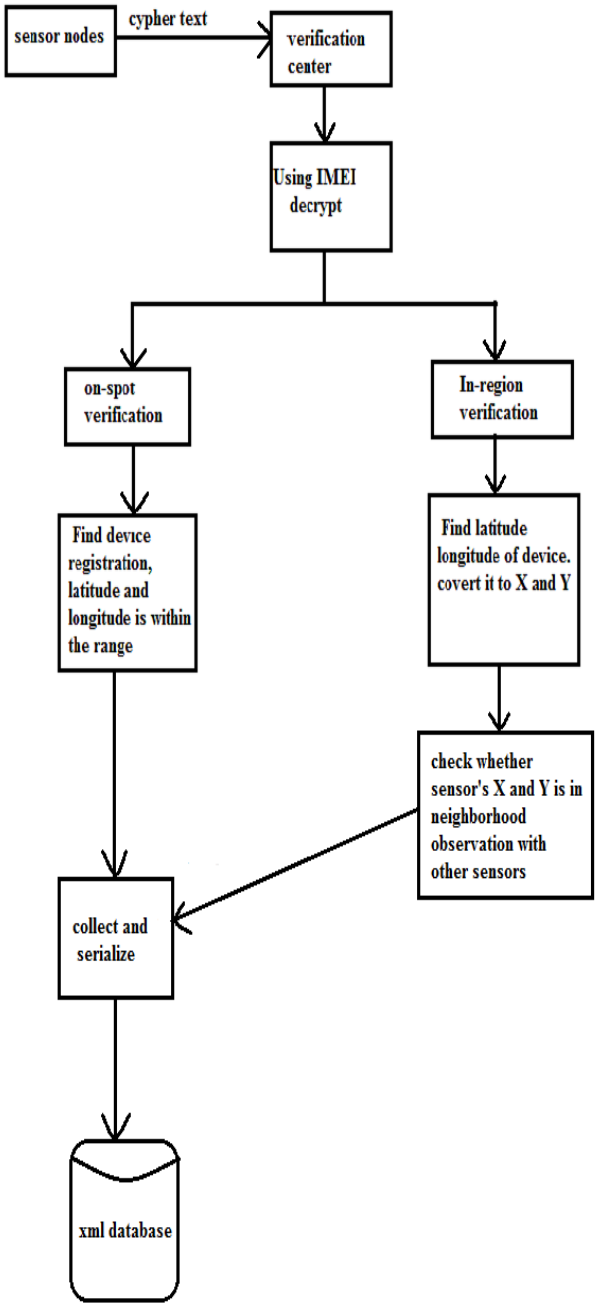

Fig.4.2 High-level Design

From the above fig 4.2 it is clear that our project has an application user. These application users interact with the xml database.

c) FLOW CHARTS

It's a diagram of sequence of movements or actions of people or things involved in a complex system or activity. Flow chart is a formalized graphic representation of a logic sequence, work or manufacturing process, organization chart, or similar formalized structure. The purpose of flow chart is to provide people with a common language or reference point when dealing with a project or process.

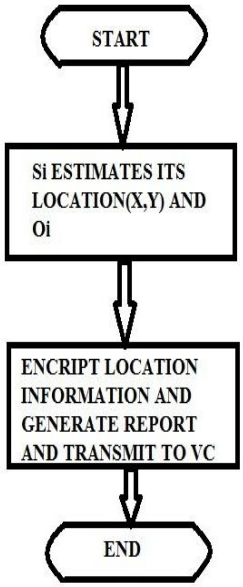

Fig.4.3 Flowchart of the sensor

Fig.4.3 shows each sensor reports its estimated location and its neighbourhood observation to the VC. We assume each sensor shares a pair wise key with the VC, so they can encrypt the message and authenticate themselves. Such pair wise keys can either be preloaded offline into sensors memories, or distributed online using some existing key distribution algorithms.

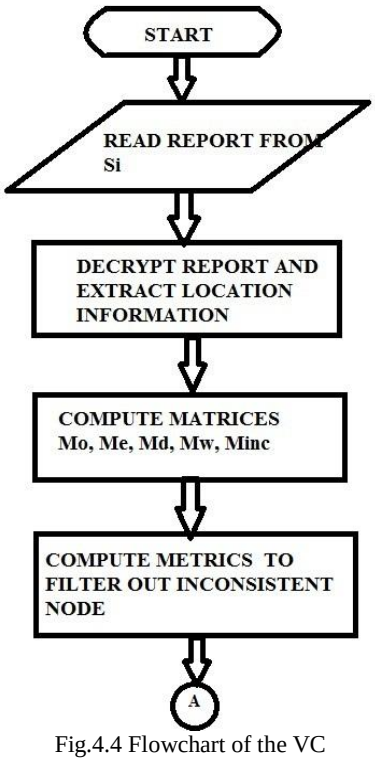

Fig.4.4 Flowchart of the VC

Fig.4.4. shows the flow diagram of the verification centre. In verification centre the VC reads the information's sent from the sensors. Five n* n square matrixes are calculated based on the reported information from sensors. The five matrices are Observation matrix, Estimation matrix, Difference matrix, Weight matrix, Inconsistency matrix. These matrices are

 ISSN: 2321-8169
3074 - 3078

computed and the inconsistent node is filtered out using GFM algorithm.

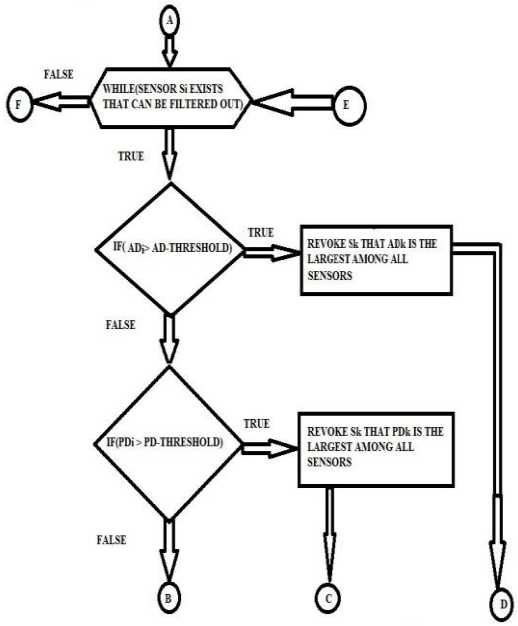

Fig.4.5 Flowchart of GFM algorithm

In fig.4.5 GFM algorithms calculate sall the above matrixes and utilizes filtering metrics to greedily filter out abnormal locations. In the first round, VCcomputes matrix Minc and metrics ADi, PDi, and ASi for alli is any natural number.

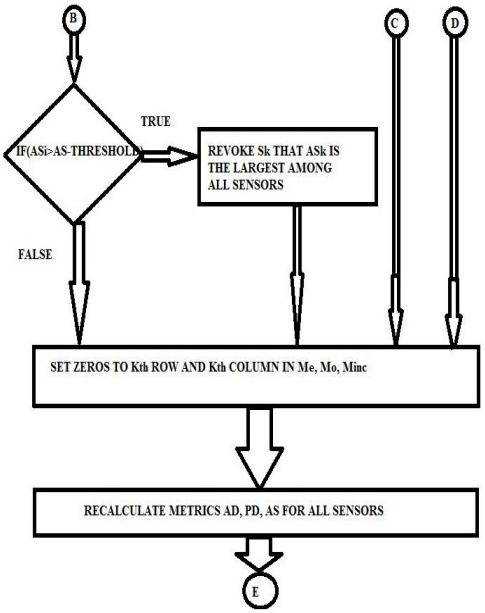

Fig.4.6 Flowchart of GFM algorithm

If there is any sensor whose metric value exceed that metric's threshold, VC revokes the sensor that has the largest metric value (say node Sk), and sets all zeros to the *k*th row and the *k*th column in matrixes Me, Mo, and Minc. This process repeats until no more sensors can be filtered out.

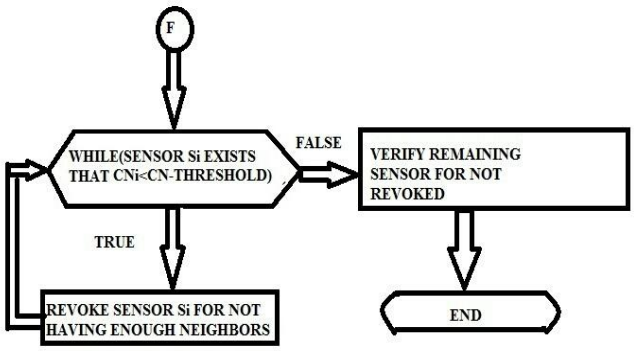

Fig.4.7 Flowchart of GFM algorithm

Then the metric *CN*i is considered: sensors that do not have enough number of consistent neighbours are revoked. Finally, the remaining sensors are accepted by the VC as correctly localized sensors.

d) SEQUENCE DIAGRAM

A sequence diagram in a Unified Modelling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. A sequence diagram shows object interactions arranged in time sequence. It depicts the objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario. Sequence diagrams typically are associated with use case realizations in the Logical View of the system under development.

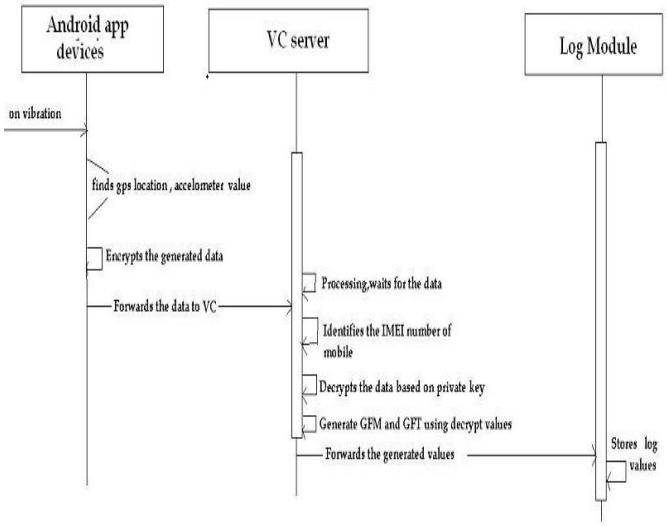

Fig:4.8 Sequence diagram

The above is the sequence diagram which gives us a brief flow. Initially the latitude and the longitude values are found out using the android mobile app which in turn is directed to the verification centre which is in encrypted form, when this message is forwarded to VC it in turn processes the data and decrypts the message using the private key. It also generates the GFM and GFT values in order to find the trustable locations. The log module is used to store the log values.

V. CONCLUSIONS

We are implementing a system where we are not using any hardware which may be expensive or which in any deployment knowledge is required .There is no use of any directional antennas or any such heavy equipments. So this system can be considered lightweight and expensive.The system is designed that is completely robust precise and when implemented and the output is recorded, we get the desired and correct results. Also ,it has the number of instances detected by the system divided by the total number of instances present, which is very high.Moreover it has the number of normal patterns as attacks is divided by total number of normal patterns which is very low. The system which we are proposing us very efficient in many aspects.

REFERENCES

[1] W. Du, J. Deng, Y.S. Han, and P.K. Varshney, "Pairwise Key Pre-Distribution Scheme for Wireless Sensor Networks," *ACM Trans. Information and System Security*, vol. 8, pp. 42-51, 2003.

[2] W. Du, J. Deng, Y.S. Han, S. Chen, and P.K. Varshney, "Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge," *Proc. IEEE INFOCOM*, 2004.

[3] D. Liu and P. Ning, "Improving Key Pre-Distribution with Deployment Knowledge in Static Sensor Networks," *ACM Trans. Sensor Networks*, vol. 1, no. 2, pp. 204-239, 2005.

[4] Z. Yu and Y. Guan, "Key Pre-Distribution Scheme Using Deployment Knowledge for Wireless Sensor Networks," *Proc. Fourth Int'l Symp. Information Processing in Sensor Networks (IPSN '05)*, pp. 261-268, 2005.

[5] S. Brands and D. Chaum, "Distance-Bounding Protocols," *Proc. Workshop the Theory and Application of Cryptographic Techniques on Advances in Cryptology (EUROCRYPT '93)*, pp. 344C359, 1994.

[6] S. Capkun and J.P. Hubaux, "Secure Positioning of Wireless Devices with Application to Sensor Networks," *Proc. IEEE INFOCOM*, 2005.

[7] A. Kerckhoffs, La cryptographie militaire, Journal des sciences militaires. IX(1):5¨C38, IX(2):161¨C191. 1883.

[8] S. Capkun, M. Cagalj, and M. Srivastava, "Secure Localization with Hidden and Mobile Base Stations," *Proc. IEEE INFOCOM*, 2006.

[9] W. Du, L. Fang, and P. Ning, "LAD: Localization Anomaly Detection for Wireless Sensor Networks," *Proc. IEEE Int'l Parallel and Distributed Processing Symp. (IPDPS '05)*, 2005.

[10] E. Ekici, J. McNair, and D. Al-Abri, "A Probabilistic Approach to Location Verification in Wireless Sensor Networks," *Proc. IEEE Int'l Conf. Comm. (ICC)*, 2006.

[11] http://issuu.com/raghurajan1/docs/3_ijiarec