Secured GPS based Localization Protocol

Himani Joshi
M. Tech GRD
Rajpur Road
Dehradun, Uttarakhand

Ankur Chaudhary
Asst Professor
GRD, College
Rajpur Road, Dehradun

Anuj Saxena
CEO, Institute de Informatica
Subhash Nagar, Clement Town
Dehradun, Uttarakhand

ABSTRACT
Smart cities, smart villages, everything getting smart and so are the hackers. Networking has an important significance in the modern world of technology and securing it is as important as implementing it. The authors have proposed a Secured GPS Localization(SGPSL) protocol for the purpose of securing the location of the sensor nodes without compromising the resources. SGPSL provides two level security, first at the network authentication level and other at sensor level. To minimize the resource utilization mitigation is carried out. SGPSL is compared with existing GDOP[17] technique. It is observed that the bandwidth, and the energy consumed by the proposed work is 16%, and 19% respectively lesser then GDOP. The time secured is 5.3% lesser too.

General Term
Secured GPS Localization Protocol.

Keywords
GPS, Localization, WSN, GDOP, Encrypt, Secured Localization

1. INTRODUCTION
Technology has gone miles and with it the requirement for robust and secured network too. Services like Navigation through maps, and Internet-of-Things(IOT) devices have also brought everything in the palms of the people. Localization(finding location of a sensor)of a Wireless Sensor Networks(WSNs) poses an uphill task mainly as the extended community cost, bad localization, accuracy and restrained nodes are not addressed properly. Various models for Indoor localization[1], Surveillance[2] and outdoor localization[3-17] have already been presented but the main concern is Quality of Service(QOS) which includes accurate but secured location detection. A network could easily be attacked using man-in-the-middle[1] attack, Brute force[1] or social networking[1]. Hackers are smart but the designers have to be well equipped to counter the attacks.

Technology is a blessing but with it comes the threat of sharing personal information and also location which at times can be very dangerous especially for the rich and famous. Otherwise also no one would like to share its personal details and location with any unknown person. Deploying of wireless sensors can help Trains to navigate even in challenging situations and even help army to locate its personnel and also get the pin point location of the target by just airdropping some wireless sensors in the enemy area. With the exact position known Army can easily destroy the target sitting at safer distance. But, if the sensors are detected by the enemy and hackers are able to get into them and manipulate the signals wrong information would be received and wrong target would be hit, could be a very dangerous scenario. Even in case of train navigation tempered sensors can cause lot of damages. All this implies that the sensor locations need to be secured but at the same time minimum resource utilization should be there. The paper proposes a two tier secured localization technique for the purpose.

[1] Favourite attacks of the hackers

2. LITERATURE SURVEY
Since the inception of WSNs, localizing and securing it is always on the priority list. Distance separating nodes play a vital role in WSNs when it comes to finding them, to assure safety of the Euclidian distance estimation, in 2005 a signature based localization technique was proposed[3]. The method could only tolerate 50 outliers. A mean squared estimation(MMSE)[4], a technique for estimations, identification and removal of malicious location information was proposed in the same year. In 2006, based on features of the object location and trekking system, a hierarchical taxonomy was proposed[5]. Same year, two lightweight algorithms namely, Greedy Filtering by Matrix(GFM) and Trust Indicator(TI) for location verification were proposed [6]. A model was proposed in 2008 in [7], it presented how a vulnerable WSN could be attacked. To secure the nodes Secured Localization System(SLS) was proposed in 2008[8] to reduce distance attack. A strong defense system was proposed that worked both on distance reduction and enlargement. To provide greater accuracy on a larger foot-prints of mobile with lesser resources was proposed in [9]. Three parameters; consistency, location of the neighbor and secured positioning including detection of wormhole attack were put as a model and presented in [10] in 2010. SLMB technique for securing sensor locations was presented in 2011 in [11] the focus was on reducing overall energy. In 2013 a novel indoor localization algorithm was proposed[12], the algorithm focused on Bayes filtering and gave the prior and posterior probability of target location. RSSI measured the distance. In 2014 a Genetic Algorithm(GA) based model to secure the location of the nodes was proposed[13], no mitigation was carried out. In 2015 a model was proposed in which a mobile localization algorithm focused on game strategies[14]. Feature extraction was done assuming that the mobile sensor network was on attack and the mapping relation between the attack level and the trust level was established. In 2016 an indoor stationary localization based on radio waves was proposed[15], originally based on WiFi signals. Evaluation was based on the weighted *k*-Nearest Neighbours in Signal Space algorithm. In 2016 a method which model was proposed that focused on low-cost and high-accuracy for the localization of WSNs[16]. The authors presented a comprehensively improvised DV-Hop algorithm, which decreased the localization errors maintaining the hardware and communication costs. In the same year a model was proposed[17] that focused on a range-based beacon placement

model for an indoor floor plan for WSNs system. The proposed algorithm was Geometric Dilution of Precision(GDOP).

3. EXPERIMENTAL SETUP

3.1 Setup proposed SGPSL (Secured Geographical Positioning System Localization Protocol)

1. Place sensors randomly

2. Allocate equal energy to each sensor

3. Allocate equal bandwidth to each sensor

3.2 Parameters

The following Table describes the parameters used to perform secure localization.

Table 1 List of parameters

Transportation protocol	MFAP
Network protocol	UDP
Network interface type	PHY
Antenna model	OMNI
Routing protocol	DSDV
Data rate	11 Mb
Basic rate	0.5 Mbps
Traffic	20 Mbps
Energy	**3.5 j**

4. Research Methodology

4.1 Algorithm for securing node's location

Step1. loop through 1 to max

Simulate the signal received from each sensor

Store the direction of arrival of signal i.e., angle at which the sensor is located from the signal received from GPS device. Get the geographical location of the sensor using GPS

Step2. Set timer to record time

Step3. Perform Mutation

Step4. Perform Crossover using L value

Step5. Encrypt sensor and mark sensitive using improvised genetic algorithm

Step6. Display the angle of unencrypted sensors

Step7. Store time

Step8. Calculate remaining bandwidth and energy

4.2 Encryption Algorithm

Step1. bb← generate128 bit matrix

Step2. New_matrix ← add location of the sensor to bb an create a new matrix

Step3. l ← get length of the matrix;

Step4. loop k from 1 through l

Step5. new_matrix(k) ← new_matrix(k) + new_matrix(k)^2

end loop

Step6. flip the new_matrix

5. MATHEMATICAL Formulations

To test the proposed model for n number of nodes following mathematical formulations were used.

5.1 Energy Requirement

$$E_r = \left(\frac{E_i - \Delta E_j}{n} \right) .....eq(1)$$

Here,

E_i is the initial energy

ΔE_j is change in energy

E_r is energy required

5.2 Bandwidth Requirement

$$bw_r = \left(\frac{bw_i - \Delta b_j}{n} \right) .....eq(2)$$

Here,

bw_i is initial bandwidth

Δb_j is change in bandwidth

bw_r is bandwidth required

5.3 Total energy consumed

$$E_t = \sum_{i=1}^{n} E_{ri} .....eq(3)$$

Here,

E_{ri} is energy consumed in every iteration

E_t is total energy consumed

5.4 Total Bandwidth Consumed

$$BW_t = \sum_{i=1}^{n} bw_{ri} .....eq(4)$$

Here,

bw_{ri} is bandwidth consumed per iteration

BW_t is total bandwidth consumed

5.5 Total Time Consumed

$$Time_{taken} = \sum_{i=1}^{n} end_i - sart_i .....eq(5)$$

Here,

end_i is time one iteration ended
$start_i$ is start time of iteration
$Time_{taken}$ is the total time taken

5.6 Results and Discussion

5.6.1 Location Detected Through Google Map of Unsecure Node

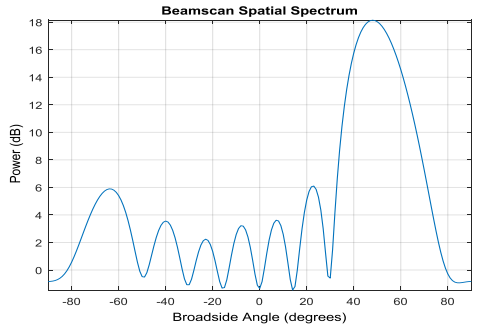

Fig 1 GPS Signal received to locate the sensor.

GPS receives the signals from the sensor, as shown in fig 1, the location of the sensor is estimated only if the sensor is not secured, secured sensors won't be detected. The location of the detected sensors is plotted along with a satellite view as shown in 2

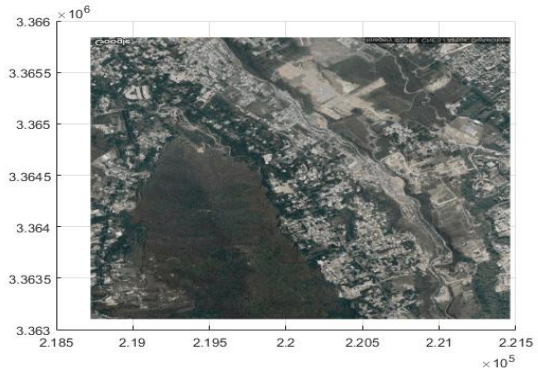

Fig 2 A satellite view of the location detected through google map of unsecure node.

5.6.2 Resource Management

The proposed algorithm effectively locates the sensors, secures them and also manages the resources like Bandwidth and energy and also manages the time.

5.6.3 *Bandwidth Consumption*

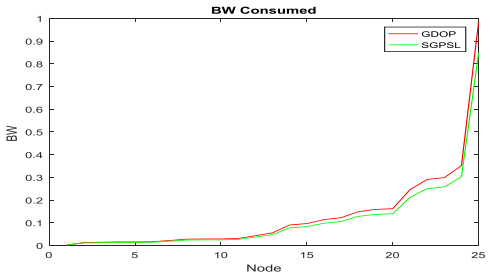

Fig. 3 Shows the consumption of Bandwidth of GDOP and SGPSL

From figure 3 it can be conclude the bandwidth consumption of the proposed model is much lesser than standard GDOP model. The total bandwidth consumed is shown in table 1.2 shows that the proposed model was able to save 16% bandwidth.

Table 1.2 Shows the total Bandwidth consumed by GDOP and proposed algorithm

Total BW GDOP	Total BW Proposed
3.378	2.91

5.6.4 Energy Consumption:

As can be seen from the following graph energy consumption in SGPSL approach is lower than GDOP algorithm. Figure 4 shows how the energy is consumed by both the algorithms as the execution progresses. Table 2 shows the total energy consumed by both GDOP and proposed model. The energy consumed by the proposed algorithm is 19% lesser than the GDOP olgorithm.

Table 2 Shows the total energy consumed by GDOP and proposed algorithm

Total energy GDOP	Total energy SGPSL
3.04	**2.45**

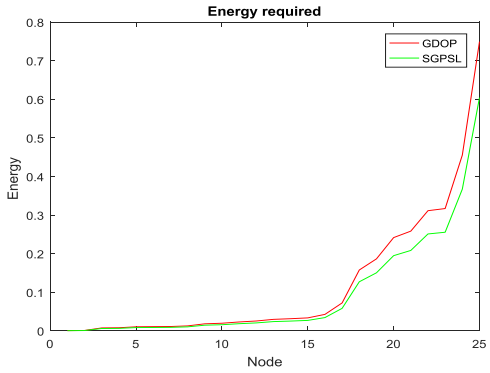

Fig. 4 shows plot of energy consumed by the proposed and GDOP model.

5.6.5 Time

As can be seen from the time graph in figure 5 the time taken by the SGPSL approach is lesser than GDOP algorithm. The

plot shows the progress of the time consumed with passing of vehicles, table 3 shows the total time consumed. It is observed that the time consumed by the proposed algorithm is 5.3% lesser than the existing GDOP algorithm.

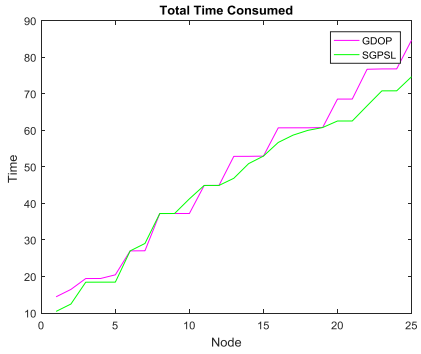

Fig 5 Shows the total time consumed by GDOP and the proposed algorithm

Table 3 Shows total time consumed by GDOP and proposed algorithm

Total Time GDOP (in ms)	Total Time Proposed (in ms)
16052.2384	15235.54

5.6.6 Quantitative Analysis in terms of different constraints.

Table 4 shows the quantitative analysis of the proposed and the standard GDOP algorithm in terms of different constraints. The observation indicated that the proposed algorithm outperforms the standard GDOP algorithm.

Table 4 Qualitative Comparison of GDOP and Proposed

Approach	SGPSL	GDOP
Objective	Deploy sensors Locate sensor using GPS signals Locate Geographical location using google map Secure the sensors Mitigate resources like energy, bandwidth and time	Deploy sensors Localize using GDOP. Record energy, bandwidth consumption and time taken.
Security	Two level security based on Reputation and Observation.	Single level security designed on reputation.
Design Consideration	Design to be executed on 802.11a/g	Designed on 802.11a
Adaptation to Topology changes	Adaptation is good as the protocol is flexible.	Average adaptation
Scalability	Minimum overhead	Average overhead
Packet Overhead	Minimum overhead	Average overhead
Processing	Very Low processing	Low processing

5.6.7 Quantitative Comparison of algorithm for different parameters

Table 2, 3 and 4 shows quantitative comparison of Bandwidth, Energy and time consumption of SGPSL Protocol using the proposed and standard GDOP algorithm. The graph shown in Fig 3 shows how the energy is consumed as the network progresses, even after the traffic increases the energy consumed by SGPSL Protocol remains consistently low and the overall energy consumed is lesser than the GDOP algorithm, table 2 supports that the total energy consumed by the proposed algorithm is lesser. Similarly, Fig 4 shows how the bandwidth consumed is managed with the progress of the network. Table 3 supports that the total bandwidth consumed by the proposed algorithm is lesser. The time consumed graph shown in Fig 5 and the supporting table 3 of the total time consumed shows that than even after securing the nodes the time consmed is consistently lower than GDOP and overall time consumed is also lesser.

6. CONCLUSION

The demand of the day to experiment with technology to make human life simpler has led the authors to design a Secured GPS Localization Protocol (SGPSL Protocol). The work focused on minimizing the resources utilization without compromising the location of the sensors. Hackers are known to penetrate the security of the networks and misuse the information gathered. A standard network with a known algorithm is vulnerable and easy to crack. The proposed work has double layer security at the MAC layer and at the information level of the sensors. The proposed work has been compared with existing GDOP localization technique. It has been observed that the bandwidth, energy consumed by the proposed work is 16% and 19% lesser respectively. The time consumed is lesser by 5.3%. The proposed work secures 11 sensors out of 25 sensors deployed, after the testing of network authentication, it has been observed that all the 11 secured locations remained secured and only 14 unsecured locations could be accessed by the network. From the results it can be concluded that overall life span of the network would also be better than GDOP as all the three parameters tested have given better results. The author in the future propose to use a predictive modelling technique to localize the sensors. In future various attacks can be carried out for testing the network for its robustness. The future work can also focus on further improvement of energy and bandwidth consumed. A new Machine Learning based algorithm can be designed for the mitigation purpose.

7. REFERENCES

[1] L. Location and W. S. Network, “Chapter 2,” pp. 12–33.

[2] B. Nemade, “Automatic Traffic Surveillance Using Video Tracking,” Procedia Comput. Sci., vol. 79, pp. 402–409, 2016.

[3] Z. Li, W. Trappe, Y. Zhang, and B. Nath, "Robust statistical methods for securing wireless localization in sensor networks," in 2005 4th International Symposium on Information Processing in Sensor Networks, IPSN 2005, 2005.

[4] D. Liu, P. Ning, and W. K. Du, "Attack-resistant location estimation in sensor networks," IPSN 2005. Fourth Int. Symp. Inf. Process. Sens. Networks, 2005., 2005.

[5] E. D. Manley, H. Al Nahas, and J. S. Deogun, "Localization and Tracking in Sensor Systems," IEEE Int. Conf. Sens. Networks, Ubiquitous, Trust. Comput. - Vol 2 - Work., vol. 2, pp. 237–242, 2006.

[6] Y. Wei, Z. Yu, and Y. Guan, "Location Verification Algorithms for Wireless Sensor Networks," pp. 0–7, 2007.

[7] A. Boukerche, H. A. B. F. Oliveira, E. F. Nakamura, and A. A. F. Loureiro, "Vehicular Ad Hoc Networks: A New Challenge for Localization-Based Systems," Comput. Commun., vol. 31, no. 12, pp. 2838–2849, 2008.

[8] D. He, L. Cui, H. Huang, and M. Ma, "Design and verification of enhanced secure localization scheme in wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 7, pp. 1050–1058, 2009.

[9] I. Amundson and X. D. Koutsoukos, "A Survey on Localization for Mobile Wireless Sensor Networks," Mob. Entity Localization Track. GPS-less Environnments, pp. 235–254, 2009.

[10] H. Guo, "Research on a new secure localization technology," ICCET 2010 - 2010 Int. Conf. Comput. Eng. Technol. Proc., vol. 6, pp. 527–530, 2010.

[11] T. Zhang, J. He, and H. Yu, "Secure localization in wireless sensor networks with mobile beacons," Int. J. Distrib. Sens. Networks, vol. 2012, 2012.

[12] R. Dwlrq et al., "The Research and improvement of Indoor Localization Algorithm Based on RSSI," pp. 178–181, 2013.

[13] R. Sharma and R. Sushil, "Security Framework in WSNs : Location," vol. 9, no. May, pp. 1–8, 2014.

[14] T. Bao, J. Wan, K. Yi, and Q. Zhang, "A game-based secure localization algorithm for mobile wireless sensor networks," Int. J. Distrib. Sens. Networks, vol. 2015, 2015.

[15] P. Kriz, F. Maly, and T. Kozel, "Improving Indoor Localization Using Bluetooth Low Energy Beacons," Mob. Inf. Syst., vol. 2016, 2016.

[16] Y. Liu and Y. Zhang, "A Better Range-Free Localization Algorithm in Wireless Sensor Networks," 2016 Int. Symp. Comput. Consum. Control, pp. 132–135, 2016.

[17] G. Laveti, G. S. Rao, D. E. Chaitanya, and M. N. V. S. S. Kumar, "TDOA Measurement Based GDOP Analysis for Radio Source Localization," Procedia Comput. Sci., vol. 85, no. Cms, pp. 740–747, 2016.