International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

Signcryption Based Security for PSO-GD Localization in WSN

R. Latha, T. N. Prabakar

Abstract: ***A signcryption based security for localization using PSO-GD algorithm in WSN is proposed which combines particle swarm optimization (PSO) and gradient decent (GD) methods for secure localization. Initially, the beacon node signcrypt the message with the keys and broadcasted the information to the surrounding nodes so as to enable receiver to identify the sender. Then the received location information is unsigncrypted by each unknown sensor node and verified. If the unsignsryption is performed successfully, the unknown node accepts the message, otherwise discarded. From the location information gathered, the unknown node estimates its location coordinates through PSO-GD localization algorithm.***

Keywords: WSN; sensor; Security; PSO; Localization

I. INTRODUCTION

A. WSN

A large number of inexpensive sensor devices form an easily deployable self configurable network without any pre deployed infrastructure called Wireless ad hoc sensor networks (WSNs) [1, 6]. These sensor node nodes are both transmission and battery power-constrained and possess limited computation and communication capabilities and help WSN to aware of its physical location [2, 6]. WSN characteristics like flexibility, fault tolerance, high sensing fidelity, low cost, and rapid deployment open the path for a wide variety of applications. Hence, such networks can be employed in consumer applications such as emergency rescue, disaster relief, smart homes, and patient monitoring, as well as industrial applications such as distributed structural health monitoring and environmental control, and military applications such as target identification and tracking, geographic routing, security surveillance, and so on**.** Also WSN enable validating the integrity of the sensor network as well as the retrieved data [1, 2, 6]. As wireless sensor networks deployed in open environment, it is open to unexpected physical environment and attacks from some adversaries [3]. Sensor localization is an important issue in WSNs [5].

B. Localization in WSN

Localization is the process of finding the location of sensor nodes by itself i.e., discovering spatial relationships between objects [8].

Manuscript published on November 30, 2019.
* Correspondence Author
Dr. R. Latha*, Tiruchirappalli Engineering College, Tiruchirappalli (Tamil Nadu), India.
Dr. T. N. Prabakar, Tiruchirappalli Engineering College, Tiruchirappalli (Tamil Nadu), India.

Location awareness is the necessity for many sensor applications since many applications like environment monitoring, vehicle tracking and mapping depend on knowledge of sensor node locations. Energy can also be saved in location based routing protocols overcoming the route discovery requirement and also caching performance can be enhanced for location dependent applications. However, employing GPS receiver in a sensor network node is expensive hence a few location aware seed nodes and protocols enabling other nodes to estimate their location from the received messages are utilized. Location awareness also enhances the security requirements [5, 7].

As nodes in the sensor networks are employed in an unplanned infrastructure in a dynamic manner without prior knowledge of their location, determining the node positions with a given few anchor nodes and relative distance and angle information between the nodes is a problem namely position estimation or localization problem [9]. However, these localization techniques are susceptible to attacks under the hostile environment involving false position and range reports by internal attackers and position spoofing by external attackers. Malicious attacks like replay attack or compromise attack can disturb the localization procedure [5].

In addition localization techniques face problems as: its dependency on information from signal strength, time of arrival requires special hardware not available on sensor nodes and if added, cost will be increased. Also a large number of seed nodes are needed to cover the network as a whole but not possible in sensor networks [7].

C. Secure localization in WSN

Securing localization is essential for ensuring the WSN integrity and its associated services. Location aware security policies require trusted location information for deployment. Once the location dependent services are deployed, attackers and misuses target on the mechanism providing location information. Location infrastructures are prone to location specific attacks which could not be solved by traditional security services. Hence mechanisms are required to be integrated to protect localization techniques. The attacks can be defeated by focusing on nodes before localization or localizing even under attacks [13].Security requirements are Authentication, integrity, availability, non-repudiation, and privacy [8].

II. LITERATURE REVIEW

Pinaki Sarkar and Sarbajit Mukherjee [10] developed a deterministic merging block technique for overcoming the connectivity issue while an unique method based on localization scales any KPS in particular, the merged schemes.

However, full communication could not be given guarantee with random merging as merged pairs.

Ning Yu et al [11] proposed a BRS-based robust secure localization (BRSL) algorithm for minimizing the impact of the malicious attackers in WSNs. BRSL method comprises of two phases. Beta reputation system based trust evaluation framework was established in first phase. The weighed Taylor-series least squares method was weighted for estimating sensor node co ordinates in the second phase. However, the cost is not less.

III.PROPOSED SOLUTION

A. Overview

In this paper, a signcryption based security for localization using PSO-GD algorithm is presented. The beacon node signcrypt the message with the keys and broadcasted the information to the surrounding nodes so as to enable receiver to identify the sender. Then the received location information is unsigncrypted by each unknown sensor node and verified. If the unsignsryption is performed successfully, the unknown node accepts the message, otherwise discarded. In PSO-GD algorithm, the PSO based distance estimation technique is integrated with gradient descent approach. In this algorithm, the unknown nodes estimate their location coordinates by using the neighborhood beacon node set.

B. System model and assumptions

Te system model consists of a base station (BS) and a master node, which are assumed to be honest. It is also assumed that all sensors nodes cannot be localized using GPS device. Hence a set of anchor nodes are deployed with GPS device. The master node is responsible for secure localization and key distribution. The anchor node broadcasts its location information which contains its id and location coordinates.

C. Signcryption-based Security

The anchor

a. Signcryption

Signcryption [12] is a cryptographic process by means of which a receiver verifies the credentials of sender. The location information can be signcrypted by the anchor node using its private key and the group public key. The receiver recovers the location information from the signcrypted text, only when it belongs to the same group of sender. Thus it ensures secure localization of sensor nodes.

An anchor node performs signcryption which involves the following steps:

1. Randomly select a number k in the range [1,..q-1]
2. Compute the encryption and signing keys $(k1,k2)=H(Kp_{gi})$.
3. Compute the message authentication code (MAC) of the location information m by k1 as

$$r=HMAC(k_1,m)\ .$$

4. Compute $s=(k/(r+sA))mod\ q$.
5. Encrypt the message by k2 as

$$c=E_{k2}(m).$$

6. Broadcast the message

ES = $\{ID_A||r||s||c\}$.

b. Un-signcryption

The signcrypted location information can be unsigncrypted using the private key of the group and the public key of the anchor node.

The un-signcryption process involves the following steps:

1. For the received location information ES, comput

$$M = {}_{s}S_{gj}(rQ + P_A).$$

2. If $M \neq P_{gj}$

drop the massage

Mark the sender node as suspected

3. If $M = P_{gj}$,

Compute

$$(K_1,K_2)=H(M).$$

4. Decrypt the message m as

$$m=D_{K2}(c).$$

D Location Estimation using PSO-GD

Usually, once the location information is received from the trusted anchor node, other nodes estimate the distance between themselves and the anchor node using time difference of arrival (TDOA) measurement. In this paper, PSO with gradient descent method is applied, which is explained in the next section.

a. **Modified PSO with Gradient Descent Method**

The main principle of PSO is related individual particles of information and optimization of solution space.

The method of Gradient Descent (GD) [13][14] is also known as steepest descent, which is basically an optimization algorithm to determine the local minimum of a function. In this method, an arbitrary point x0 within a function's range is picked, and small steps are taken towards the direction of greatest slope changes, which is the direction of the gradient, and eventually, after many iterations, the minimum of the function can be determined.

In this section, a modified PSO-GD algorithm is developed. It considers straight and non-straight conditions and estimates the gradient of the objective function in the perspective of improving the accuracy.

In PSO, a group of particles are randomly initialized to solutions. In each iteration, the particles try to update the solution in search of optimal solutions.

In every iteration, the position of each particle is updated by considering the following values:

$P_{best}(i)$ is obtained from the particle itself and known as the individual extreme
$G_{best}(i)$ is obtained from the current population and known as the global optimum.

After estimating these best values, the velocity λ_i and location σ_i of the particle are updated as:

$$\lambda_i(t+1) = \Omega \times \lambda_{id}(t) + L_1 \times rand() \times [P_{best}(t) - \sigma_{id}(t)] + L_2 \times rand() \times [G_{best}(t) - \sigma_{id}(t)] \quad (1)$$

and

$$\sigma_{id}(t+1) = \sigma_{id}(t) + \lambda_{id}(t+1) \quad (2)$$

$1 \le i \le D, D$ is the number of initialized particles.

$1 \le d \le V, V$ is the dimension of searching space

$1 \le t \le D_{\max}, D_{\max}$ is the desired iteration of particle swarm

Ω is the inertia weight

L_1, L_2 are learning constants.

The local and global best solutions are estimated as follows:

$$P_{best}(i)(t+1) = \begin{cases} P_{best(i)}(t), if\ fitness(\sigma_{id}(t+1) \ge fitness(P_{best(i)}(t)) \\ \sigma_{id}(t+1), if\ fitness(\sigma_{id}(t+1) < fitness(P_{best(i)}(t)) \end{cases} \quad (3)$$

The gradient of the objective function is applied in each iteration to control the movements of the particles.

Hence the particle's velocity eqn. can be modified as

$$\lambda_i(t+1) = \Omega \times \lambda_{id}(t) + L_1 \times rand() \times [P_{best}(t) - \sigma_{id}(t)] + L_2 \times rand() \times [G_{best}(t) - \sigma_{id}(t)] + L_3 . g_{id}(f(\sigma_{id}(t))) \quad (4)$$

Where $g(f(\sigma_{id}))$ represents the partial derivatives of the objective function, and L_3 is the weight for the gradient term.

The objective function $f(\sigma_{id})$ is given by

$$f(\sigma_{id}) = \frac{1}{2}\sum_{k=1}^{N}(\|Z_k - Z\| - d_k)^2 \quad (5)$$

The gradient decent update rule is given by the following equation

$$\sigma_{id}(t+1) = \sigma_{id}(t) - \eta \nabla f(\sigma_{id}) \quad (6)$$

Here $-\eta \nabla f(\sigma_{id})$ is the negative gradient of the objective function at the current position, η is the learning rate which is equal to $L_3 dt$. ∇ (.) denotes the derivative with respect to Z.

b. PSO-GD Algorithm

The unknown node estimates its location coordinates by using the modified PSO-Gradient algorithm. The steps involved in the algorithm are as follows:

Algorithm

1) Initialize the search space Un
2) Initialize the particles r_j, j=1,2…D
3) Estimate $\hat{Z}(0)$ to some point in the deployment area.
4) For each particle r_j
5) For each iteration t , t=1,2….D_{max}
6) Find the local score $f(X_j)$ (t)
7) Evaluate the gradient $f(X_j)$ at current estimate using Eq.(5)
8) Update the estimated value using gradient decent update rule using Eq.(6)
9) Find the local best function $P_{best}(t)$ of $X_j(t)$
10) Find the global best function $G_{best}(t)$ of $X_j(t)$
11) If local score $f(X_j)(t) > P_{best}X_j(t)$, then
12) Put $P_{best}\ X_j(t) = f(X_j)$ (t)
13) End if
14) If local score $f(X_j)(t) > G_{best}X_j(t)$, then
15) Put $G_{best}\ X_j(t) = f(X_j)$ (t)
16) End if
17) Update the velocity and position of r_j using Eq. (1) and (2)
18) End For
19) End For

20) Repeat the steps from (4) to (18) until the best solution is attained.
21) Return the estimated position (x_n, y_n) corresponding to the best solution.

The position of r_i at iteration t in the solution search space is indicated by $\overrightarrow{X_i}(t)$.

Each position is associated with an error function. The local score of the current position is calculated using the fitness function $f(X_j)$. The local best P_{best} and global best G_{best} solutions are estimated for $f(X_j)$.
The gradient of objective function $f(X_j)$ is updated using the gradient decent rule. After checking the local score of $f(X_j)$ with P_{best} and G_{best}, the next position and velocity of r_j is updated.

Each iteration results in a new estimate that has a higher probability of being the true location of the node.

IV. Experimental Results

A. Experimental Parameters

The Signcryption based Security for PSO-GD Localization (SSPSO-GD) protocol is implemented in NS2 and compared with the BRS-Based Robust Secure Localization (BRSL) algorithm [11]. The performance is measured in terms of packet delivery ratio (PDR), communication cost, computational cost, localization delay and resilience against node capture metrics. The experimental settings and parameters are shown Table 1.

Table 1: Experimental parameters

Number of nodes	50,100,150,200 and 250
Topology size	50m X 50m
MAC Protocol	IEEE 802.11
Propagation model	Two Ray Ground
Antenna model	Omni Antenna
Transmission range	250m

B. Results

In this section, the results for varying the number of nodes from 50 to 250 are presented.

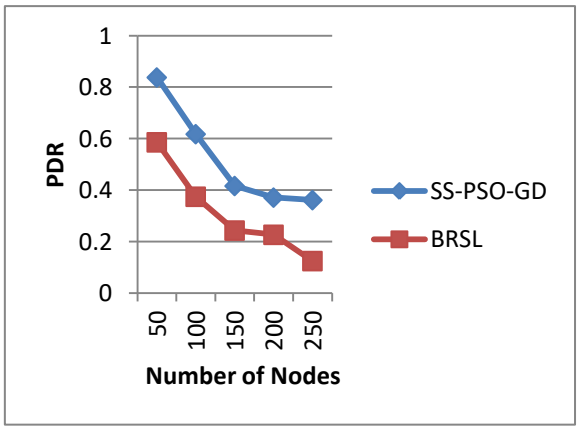

Figure 1: PDR for varying nodes

The graph showing the results of PDR for varying the nodes is shown in Figure 1. The figure depicts that the PDR of SS-PSO-GD ranges from 0.83 to 0.36 and PDR of BRSL ranges from 0.58 to 0.12. Ultimately, the PDR of SS-PSO-GD is 43% higher when compared to BRSL.

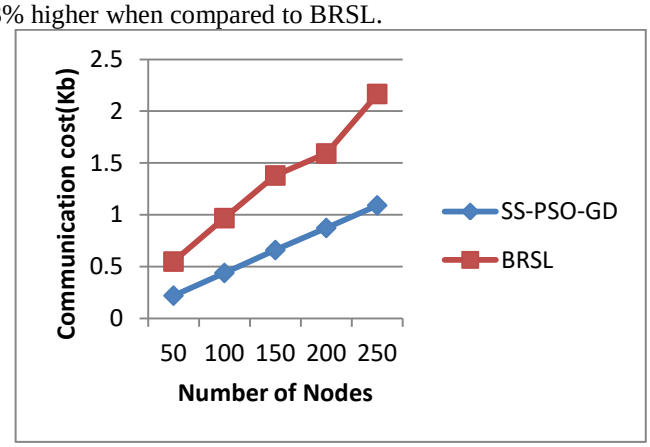

Figure 2: Communication cost for varying nodes

The graph showing the results of communication cost for varying the nodes is shown in Figure 2. The figure depicts that the communication cost of SS-PSO-GD ranges from 0.22 to 1.09 and communication cost of BRSL ranges from 0.54 to 2.2. Ultimately, the communication cost of SS-PSO-GD is 52% less when compared to BRSL.

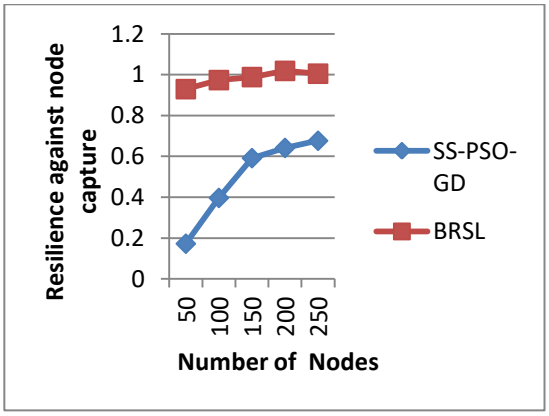

Figure 3: Resilience for varying nodes

The graph showing the results of Resilience for varying the nodes is shown in Figure 3. The figure depicts that the Resilience of SS-PSO-GD ranges from 0.17 to 0.67 and Resilience of BRSL ranges from 0.92 to 1.0. Ultimately, the Resilience of SS-PSO-GD is 50% less when compared to BRSL.

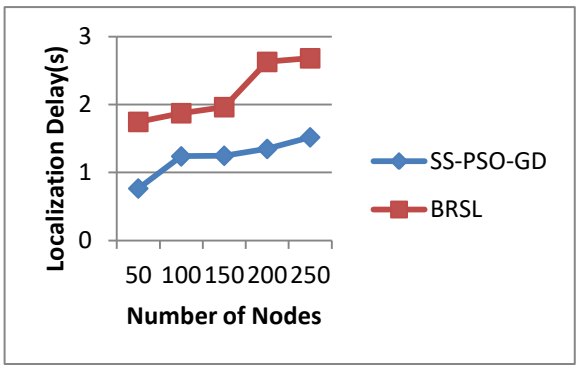

Figure 4: Localization Delay for varying nodes

The graph showing the results of localization delay for varying the nodes is shown in Figure 4. The figure depicts that the localization delay of SS-PSO-GD ranges from 0.76 to 1.5 and delay of BRSL ranges from 1.7 to 2.6. Ultimately, the localization delay of SS-PSO-GD is 44% less when compared to BRSL.

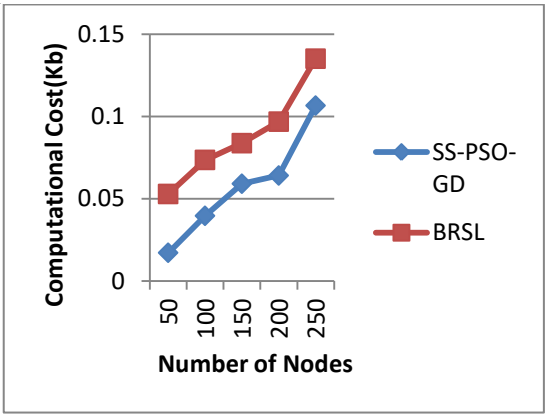

Figure 5: Computational cost for varying nodes

The graph showing the results of computational cost for varying the nodes is shown in Figure 5. The figure depicts that the computational cost of SS-PSO-GD ranges from 0.01 to 0.106 and computational cost of BRSL ranges from 0.05 to 0.14. Ultimately, the computational cost of SS-PSO-GD is 40% less when compared to BRSL.

V. CONCLUSION

A SS-PSO-GD algorithm for WSN is proposed in this paper which combines particle swarm optimization (PSO) and gradient decent (GD) methods for secure localization. Initially, the beacon node signcrypt the message with the keys and broadcasted the information to the surrounding nodes so as to enable receiver to identify the sender. Then the received location information is unsigncrypted by each unknown sensor node and verified. If the unsignsryption is performed successfully, the unknown node accepts the message, otherwise discarded. From the location information gathered, the unknown node estimates its location coordinates through PSO-GD localization algorithm. Experimental results shows that SS-PSO-GD achieves lesser localization delay with reduced communication and computational costs.

REFERENCES

1. Loukas Lazos and Radha Poovendran, “SeRLoc: Robust Localization for Wireless Sensor Networks”, ACM Transactions on Sensor Networks, Vol. 1, No. 1, August 2005, pp. 73–100.
2. Yanchao Zhang, Wei Liu, Yuguang Fang and Dapeng Wu, “Secure Localization and Authentication in Ultra-Wideband Sensor Networks”, IEEE Journal on Selected Areas in Communications, Vol. 24, No. 4, 2006.
3. Junbeom Hur, Yoonho Lee, Seongmin Hong and Hyunsoo Yoon, “Trust-Based Secure Aggregation in Wireless Sensor Networks”, 3rd International Conference on Computing, Communications and Control Technologies, Austin, USA. 2005.
4. Eric Sabbah, Adnan Majeed, Kyoung Don, Kang, Ke Liu, and Nael Abu Ghazaleh, “An Application Driven Perspective on Wireless Sensor Network Security”, Proceedings of the 2nd ACM international workshop on Quality of service & security for wireless and mobile networks, ACM, 2006.
5. Srdjan C apkun, Saurabh Ganeriwal, Farooq Anjum and Mani Srivastava, “Secure RSS-based Localization in Sensor Networks”,IEEE, 2006.
6. E. Ekici, S. Vural, J. McNair and D. Al-Abri, “Secure probabilistic location verification in randomly deployed wireless sensor networks”, Ad Hoc Networks, 2007.
7. Lingxuan Hu and David Evans, “Localization for Mobile Sensor Networks”, Proceedings of the 10th annual international conference on Mobile computing and networking, ACM, 2004.
8. Avinash Srinivasan and Jie Wu, “A Survey on Secure Localization in Wireless Sensor Networks", Encyclopedia of Wireless and Mobile communications, 2007.
9. V. Vijayalakshmi and Dr. T.G. Palanivelu, “Secure Localization Using Elliptic Curve Cryptography in Wireless Sensor Networks”, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.6, June 2008.
10. Pinaki Sarkar and Sarbajit Mukherjee, “Secure Connected Scalable Combinatorial KPS In WSN: Deterministic Merging, Localization”, 38th Annual IEEE Conference on Local Computer Networks, 2013.
11. Ning Yu, Lirui Zhang, and Yongji Ren, “BRS-Based Robust Secure Localization Algorithm for Wireless Sensor Networks”, Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks, 2013.
12. Ting Zhang, Jingsha He, Xiaohui Li and Qian Wei, “A Signcryption-based Secure Localization Scheme in Wireless Sensor Networks”, International Conference on Medical Physics and Biomedical Engineering, Physics Procedia, pp. 258 – 264, 2012.
13. Ravi Garg, Avinash L. Varna, and Min Wu, “An Efficient Gradient Descent Approach for Secure Localization in Resource Constrained Wireless Sensor Networks”, IEEE Transactions on Information Forensics and Security, pp- 717 – 730, 2012
14. Zahra Ansari,Reza Ghazizadeh and Zahra Shokhmzan, "Gradient Descent Approach to Secure Localization for Underwater Wireless Sensor Networks",24th Iranian Conference on Electrical Engineering (ICEE),2016.