Mobility Aware Displacement Approximation Technique Based LSS and Privacy Preservation for Effective Data Routing in WSN with IoT Devices

S S Rajasekar (rajasekarss1009@yahoo.com)
Bannari Amman Institute of Technology

C. Palanisamy
bannari amman institute of technology

K. Saranya
Bannari amman institute of technology

Research Article

Keywords: WSN, Mobility Displacement Approximation, LSS, Privacy Preservation, MADA-LSS, DSRM, THM.

Posted Date: November 3rd, 2021

DOI: https://doi.org/10.21203/rs.3.rs-1025973/v1

Mobility Aware Displacement Approximation Technique Based LSS and Privacy Preservation for Effective Data Routing in WSN with IoT Devices

[1*]Dr. S S Rajasekar, (corresponding author)

Assistant Professor, Department of Computer science and Engineering, Bannari Amman Institute of Technology, Sathyamangalam. ORCID ID:0000-0001-9591-5833. EMAIL : rajasekarss1009@yahoo.com

[2]Dr.C.Palanisamy,

Professor, Department of Information technology, Bannari Amman Institute of Technology, Sathyamangalam. Palanisamy123456@hotmail.com

[3]Dr. K.Saranya,(**Third author**)

Assistant Professor, Department of Computer science and Engineering, Bannari Amman Institute of Technology, Sathyamangalam. ORCID ID: 0000-0002-8849-9605 EMAIL : SaranyaSaranyaSaranya123@hotmail.com

Abstract:

The Location based Service Selection (LSS) in WSN has been well studied. Towards effective LSS, an efficient Mobility Aware Displacement Approximation (MADA-LSS) based approach is presented in this article. The model monitors the mobility of mobile device and predict the possible location at different future time stamp. According to the future time stamp, the list of service locations are identified at different possible locations. According to the possible locations and service set, the method discover set of routes to reach each of the service points. For each of the route, the method estimates Data Arrival Rate (DAR), Data Claim Rate (DCR) and Data Rate Support Measure (DRSM) for both Access Point as well as route identified. Also, the method ranks the service points according to DRSM value and estimates the Trusted Handover Measure (THM) for the routes according to IoT (Internet of Things) devices of any route. By considering both THM and DSRM values an optimal service point as well as route has been selected to perform data transmission. Also, the privacy preservation is performed by using the same set of displacement approximation scheme which selects optimal encryption based on mobility parameters and time complexity and security of different encryption schemes. The proposed method improves the performance of LSS and secure routing.

Index Terms:

WSN, Mobility Displacement Approximation, LSS, Privacy Preservation, MADA-LSS,DSRM, THM.

1. Introduction:

The use of wireless sensor network (WSN) has been increasing at every second as the mobile users accesses various services through their device. The services available at different service point or Access Point (AP) are accessed through number of sensor nodes in the network. The mobile users access the available services through various routes available in the WSN to complete their data access. The sensor network has number of sensor nodes to support data access and service access. The mobile nodes have the freedom to move on any direction and speed. This would change the topology and introduces number of link failure which challenges the protocol to handle the data packets and delivering to the user. Also, like any network, there are many threats can be identified which challenges the delivery of data packet to the exact legitimate node and service point.

In general, the routing in WSN is performed by discovering the routes available. It has been performed in two ways, one by broadcasting the route request throughout the network and collecting the routes available through set of reply being received. Another one is using the topology of the network. However, identified routes cannot be used for the entire transmission, as there will be set of link failure would occur due to many factors. If the sensor nodes lose their energy and would become dead this introduces link failure. Also, when the mobile node moves to a location where there is no other sensor node located within the transmission range, then there will be link failure which encourage the increased frequency of route discovery. This would affect the performance of entire network and lifetime as well.

In recent times, the IoT (Internet of Things) devices has become unavoidable part of WSN which is being used by different organizations and homes. Even though the IoT devices are not part of the network, they can be used in transmitting the data efficiently and to complete the transaction. But, the IoT devices cannot be trusted in transmitting sensitive data between the service point and users. If there exist a malicious node in the route in form of IoT devices, then they would steal the data and would involve in various threats. The selection of secure route is

done by choosing a route based on the trust of nodes, behavior of nodes and so on. However, they suffer to achieve expected security performance.

The selection of secure route has great impact on the privacy of user data. The data transmission would be done over the user data which is more sensitive. If the data has been exposed, then the service trustworthy on the network as well in the market would get degrade. However, it is necessary to preserve the user data and privacy preservation is the process of hiding sensitive user data from external world. It has been performed by enforcing different approaches of access restriction as well as data encryption schemes. Towards the scope, this article presents an mobility aware displacement approximation scheme which involves in the selection of secure route and enforces privacy preservation. The approach is focused on how the IoT devices can be used in transmitting the service data effectively.

On the other side, the article considered the Location based service selection (LSS) which is the most dominant entity in achieving higher QoS performance in WSN. However, the mobile node moves on various directions, it is necessary to provide the seamless service to the user. The same service would be available in various locations and to provide seamless service, it is necessary to choose the optimal service access point for the user. The selection of LSS has been performed based on various constraints like mobility, speed, direction and so on. However the method does not meet the requirements. The proposed model MADA-LSS is focused on selecting the service based on various parameters. The detailed approach is presented in the next sections.

2. Related Works:

The problem of LSS in WSN has been approached with several techniques. Also, the privacy preservation has been handled by various researchers. This section details set of methods related to the problem.

In [1], the author proposes a proxy source node selection mechanism by constructing the candidate region. According to the energy, a least hop route is selected to perform data transmission. A concept of user/service location information and locality-sensitive hashing (LSH) is presented towards location aware recommendation to achieve higher privacy-preservation [2]. A dual privacy preserving (DPP) scheme is presented to protect the user

location where the method combine Shamir threshold mechanism, dynamic pseudonym mechanism, and K-anonymity technology in improving the content privacy.

In [4], a novel privacy-preserving and scalable service recommendation scheme is presented which works based on SimHash, named $SecRec_{SimHash.}$ In [5], the same is enforced with distributed recommendation of services, which consider multi dimensions named $SerRec_{multi\text{-}qos}$, Similarly, an instance of Locality-Sensitive Hashing (LSH), into service recommendation is presented named MinHash which works on two stage as $SerRec_{two\text{-}LSH\ and}$ generates recommendation in two stages [6].

The privacy preservation with edge computing is presented in [7], where the ECO method enforce privacy preservation on vehicle to vehicle communication and V2V routing [7] A random walk approach is presented in [8], which combines collaborative filtering to perform privacy preservation and location strategy to perform LSS. A distributed locality sensitive hashing scheme based service recommendation is presented in [9], where Distri-LSH approach focused on service recommendation. In [10], propose a location privacy protection method to satisfy users' personalized privacy needs with reasonable protection of their privacy. Firstly, we define a normalized decision matrix to describe the efficiency and privacy effects of a route, and establish a multi-attribute utility function to quantify the utility of different routes for route selection. Then, according to users' personalized privacy protection need, we allocate the privacy budget for each query location on the selected route based on the distance between it and his nearest sensitive location.

In [11], they propose a Skyline point which divides the entire service set into regions. According to that, the method performs service selection. In [12], propose noise-added selection algorithm, a location privacy protection method that satisfies differential privacy to prevent the data from privacy disclosure. In [13], propose a cooperative edge caching scheme, which allows vehicles to fetch one content from multiple caching servers cooperatively. In [14], the author propose dedicated short-range communication (DSRC) standard, with three original contributions. The method works on probability and uses the spatial relationship to perform location based service selection. In [15], develop a privacy preserving protocol to predict missing QoS values and thereby providing Web service recommendations based on past QoS experiences and locations of users. In [16], propose a privacy preserving user-based CF

technique based on homomorphic encryption, which is capable of determining similarities among users followed by generating recommendations without revealing any private information.

In [17], propose a location-aware personalized CF method for Web service recommendation. The proposed method leverages both locations of users and Web services when selecting similar neighbors for the target user or service. In [18], propose a privacy-preserving task recommendation scheme (PPTR) for crowdsourcing, which achieves the task-worker matching while preserving both task privacy and worker privacy.

In [19], A customer-aware power regulatory model is proposed that provides awareness to the consumer regarding the usage of electrical energy, in a secure and reliable solution that combines the features of electrical engineering with cloud computing to ensure better performance in notifying issues, which is done based on location, and enhances the execution of smart grids.

In [20], the author present a efficient approach towards privacy preservation is presented by considering different parameters of mobile node in secure routing. In [21], proposed an energy-aware QoS-guaranteed workflow management mechanism. In [22], propose a secure and efficient privacy-preserving data aggregation algorithm (SECPDA) based on the original clustering privacy data aggregation algorithm. In [23], an efficient mobility aware directional service fetching algorithm (MADSF) is presented in this paper. The algorithm performs lookup about different services available around the user location. By fetching the trust are relation on verified route selection represents the directional approach based on the services identified, services present in the direction of user and estimates data pickup rate (DPR) for each service based on different properties of the route and service. Finally, user selected the current meet by the point single service selection and produces result to the user.

In [24], propose a proxy source node selection mechanism by constructing the candidate region. Secondly, based on the residual energy of the node, we propose a shortest routing algorithm to achieve better forwarding efficiency. Finally, by combining the proposed proxy source node selection mechanism with the proposed shortest routing algorithm based on the residual energy, we further propose a new, anonymous communication scheme.

All the methods suffer to achive the expected performance in LSS and privacy preservation.

3. Mobility Aware Displacement Approximation Based LSS and Privacy Preservation:

The proposed mobile aware displacement approximation model monitors the network and mobility of nodes. According to that, the method discovers the list of access points and routes available according to the topology of Manet. Further, from the list of access points and by approximating the mobility details of node, the method estimates Data Arrival Rate (DAR), Data Claim Rate (DCR) and Data Rate Support Measure (DRSM) for both Access Point as well as route identified. Also, the method computes the value of Trusted Handover Measure (THM) towards route selection and DSRM is used for service selection. The detailed approach is presented in this section.

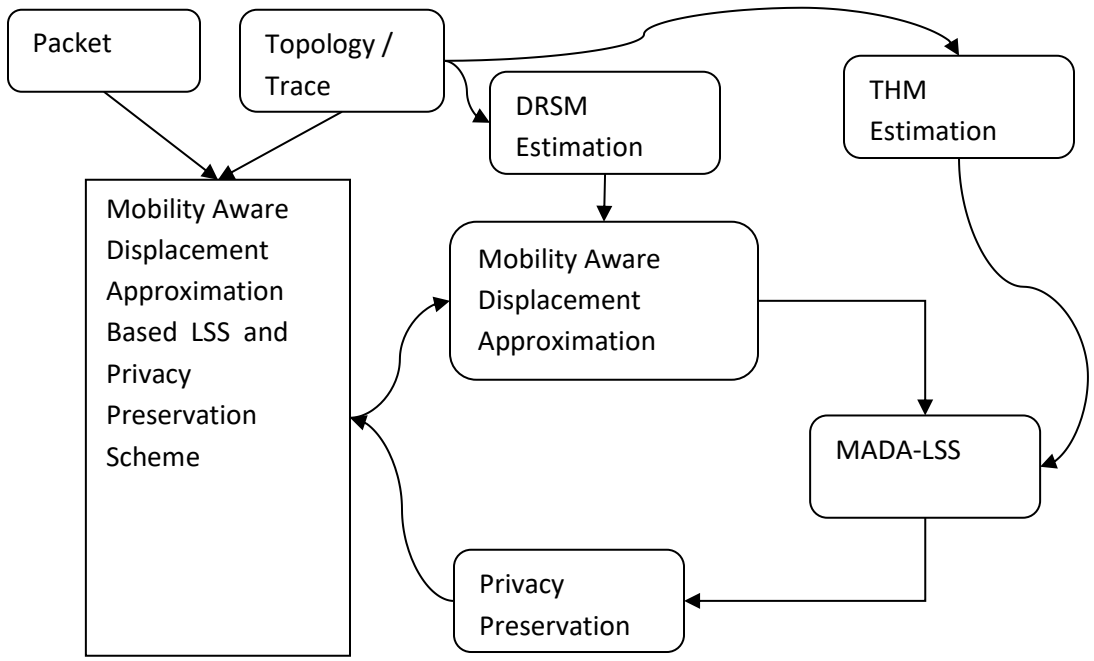

Figure 1: Architecture of Proposed MADA-LSS Model

The functional model of proposed MADA-LSS model is presented in Figure 1, and the functional properties are detailed in this section.

3.1 Mobility Aware Displacement Approximation:

The mobility aware displacement approximation algorithm monitors the location of the mobile node. According to the mobility, speed, direction of the mobile node, the method approximates different locations would be moved by the node in different time stamp. The possible locations to which the node would move have been used in identififying set of services and routes to reach the service access points. The routes identified are used in MADA-LSS towards the selection of service. Let us consider, the node M_i located in a geographic location Gl_k at the time stamp T_t, then if the mobility speed of M_i is x then, the possible location of the node M_i at the time stamps $\{T_{k+1}, T_{k+2,} T_{k+3}\}$ can be measured by approximating the speed and direction with the location to be of $\{l_k, l_{k+1,} l_{k+2}\}$. Once, the location of the mobile node has been predicted, then the set of service points around the location l can be identified and routes to reach the service point Ap, can be identified towards successful service selection.

Algorithm:

Given: Mobile Node Location L, Node ID Nid, Speed X

Obtain: Location Set Lset, Access Point Set Sps, Route-List Set Rlist

Start

Read L, Nid, X.

Initialize Time T_k = Current Time.

At each Time T_r

At each angle Mangle

Compute Displacement Mdisp = $Location(\ \ (X \times Tr) \times Mangle)$ -- (1)

Add Mdisp to location set Ls.

Initialize Service point list Spl.

$$\text{Spl} = \sum_{i=1}^{size(SPS)} Sps(i).location < Region \;\&\&\; Dist(Mdisp, Sps(i).location) < Th > \quad \text{-- (2)}$$

Add to access point set of specific location.

For each service point sp_i

Identify set of routes $\text{Rs} = \sum Routes \rightarrow \quad Spi$

Add to route list set Rlist.

End

End

End

Stop.

The above discussed algorithm computes the mobility displacement would occur on any mobile node and based on that set of service points and routes to reach the service points are identified. Identified routes and access points are added to concern set to support location based service selection.

3.2 DRSM Estimation:

The routes identified to reach any service access point has many features in terms of number of hops, number of IoT devices, traffic in each hop, number of bytes claimed per second and so on. According to all these, the data rate support measure (DSRM) is measured. The above mentioned factors are much essential in identifying the exact route for the data transmission. In order to provide seamless service, the data rate in the route towards the specific application must be achieved. For example, when a user access the video file through the service, the playback of video must be done without interruption and requires seamless delivery of data packets. This is in turn needs specific data rate required by the application must be maintained. Also, the service point must be capable of delivering such required data rate according to the user needs as well as service requirements. By maintaining such data rates, the service performance and application performance can be maintained. So, the selection of route must be done by considering all these.

According to this, for any given route R, the method estimates the Data Arrival Rate (DAR) and data Data Claim Rate (DCR) for the route. According to these two values, the Data Rate Support Measure (DRSM) of the route has been measured. Similarly, the same DRSM value can be measured for Access Point towards LSS.

The value of DAR is measured as follows:

$$DAR = \frac{\sum_{i=1}^{size(Ts)} Sumof\ (BytesTransfered(Ts(i)))}{size(Ts)} \quad \text{-- (3)}$$

The above equation represent the value of DAR which is computed by summing the total bytes transferred through the route at different transmission and computes the average value.

Similarly, the data claim rate (DCR) is measured by computing the average claim value in bytes. It has been measured as follows:

$$DCR = \frac{\sum_{i=1}^{size(Ts)} Sumof\ (BytesClaimed(Ts(i)))}{size(Ts)} \quad \text{-- (4)}$$

Now using DAR and DCR values, the value of DRSM is measured is measured as follows:

$$DRSM = {}^{DAR}/_{DCR} \quad \text{-- (5)}$$

Estimated value of DRSM is used in LSS and privacy preservation.

3.3 THM Estimation:

The trusted handover measure (THM) is the value which represents the trustworthy of the route in data transmission. It has been measured according to the number of IoT devices present in the route and number of transmission done through the route in success manner. By computing the value of THM, the trustworthy of the route can be measured. It has been measured as follows:

$$THM = \frac{\sum_{i=1}^{size(Ts)} Ts(i).Route==R \;\&\&\; State==1}{\sum_{i=1}^{size(Ts)} Ts(i).Route==R} \times \sum IoT \in R \quad \text{-- (6)}$$

In the above equation, the value TS represent the trace set and the equation identifies the number of IoT devices present in the route and number of transmission and number of success transmission. Estimated value of THM is used in service selection.

3.4 MADA Location Based Service Selection:

The mobility aware displacement approximation algorithm receives the service request from the mobile node. According to that, the service available based on the location of the node are identified. Further, the method performs mobility aware displacement approximation which identifies routes and service points as list. From the list, for each access point and for each route available, the method computes the DRSM value and THM values. Using both of them, the method select a most DRSM valued service point. For the service point selected, the method estimates the THM value for the routes identified. Finally, a route with higher THM is identified to perform data forwarding. The data forwarding is done by performing privacy preservation.

Algorithm:

Given: Request Req, Trace set Ts, Network Topology NT.

Obtain: Null

Start

Read Req, Ts, NT.

Identify service requested Sreq = Service $\in Req$

Identify mobile node location, speed [Mloc,x] = Location, speed $\in$Req

[Spl, Rlist] = Perform Mobility aware displacement approximation (Mloc,x)

For each service point s

For each route R

Compute DSRM.

End

End

Choose the service point with maximum DSRM.

For each route R

Measure THM.

End

Route R =Choose route with maximum THM.

Perform Privacy Preservation on data D.

Transmit data through route R.

Stop

The above discussed algorithm represents how the overall mobility aware displacement approximation based LSS is working.

3.5 Privacy Preservation:

The privacy preservation in this approach is performed by choosing an effective data encryption scheme according to the data. The method classifies the encryption schemes according to the complexity of the algorithm and time complexity. By considering the mobility of the node, the method selects a optimal method for data encryption. Further, the selected method has been used in data encryption and data has been transmitted through the route selected. If the node moves on less speed, then the method choose a moderate time complex algorithm for data encryption, otherwise if the nodes mobility is higher, then the least time complex scheme is selected for data encryption. But it is not done intentionally, because the selection at the least mobility is done on random manner but when mobility is higher then only least time complex method is selected.

4. Results and Discussion

The proposed mobility aware displacement approximation based location based service selection is implemented in advanced java. The method tracks the nodes mobility by fetching the GPS location and based on the mobility speed the service selection has been optimized. The method has been evaluated for its performance under various parameters. Obtained results are compared in this section.

Simulation Constraint	Value
Tool Used	Advanced Java
Number of Nodes	200
Number of service points	20
Number of IoT devices	40

Table 1: Details of Evaluation

The parameters and factors considered for the performance evaluation is presented in Table 1. According to this, the results obtained has been presented in this section.

LSS Performance			
	50 Services	100 Services	200 Services
KBPC	67	71	74
SECPDA	73	76	79
Distri_LSH	76	79	82
MADSF	83	86	89
MADA-LSS	85	88	97

Table 2: Analysis on LSS Performance

The performance of the methods are measured on location based service selection and compared with other methods. The proposed MADA-LSS algorithm has improved the performance in location based service selection than other methods.

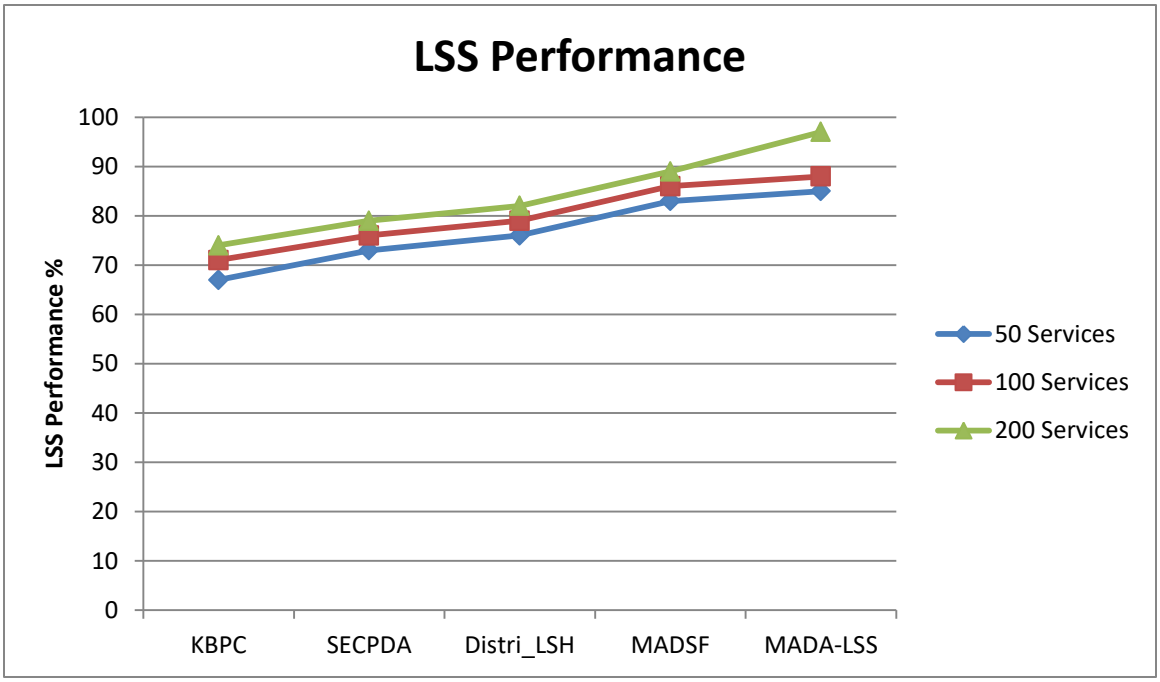

Figure 2: Analysis on LSS Performance

The performance of LSS has been measured for various approaches and presented in Figure 2. The proposed MADA-LSS algorithm has produced higher performance than other methods.

Privacy Preservation Performance			
	50 Users	100 Users	200 Users
KBPC	65	69	73
SECPDA	69	75	77
Distri_LSH	73	78	81
MADSF	81	85	85

MADA-LSS	84	87	96

Table 3: Analysis on Privacy Preservation Performance

The performance of the methods are measured on privacy preservation and compared with other methods. The proposed MADA-LSS algorithm has improved the performance in privacy preservation than other methods.

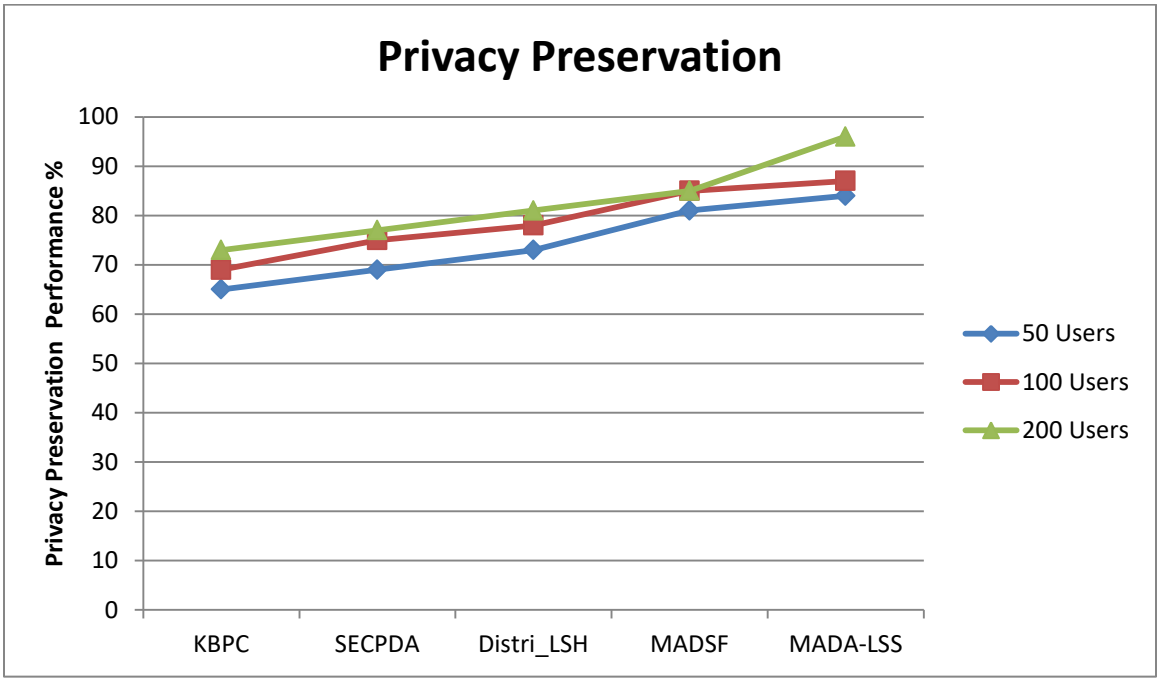

Figure 3: Analysis on Privacy Preservation Performance

The performance of privacy preservation has been measured for various approaches and presented in Figure 2. The proposed MADA-LSS algorithm has produced higher performance than other methods.

Secure Routing Performance

	50 Nodes	100 Nodes	200 Nodes
KBPC	69	72	74
SECPDA	71	74	76
Distri_LSH	74	78	81
MADSF	82	86	89
MADA-LSS	85	89	98

Table 4: Analysis on Secure Routing Performance

The performance of the methods are measured on secure routing and compared with other methods. The proposed MADA-LSS algorithm has improved the performance in secure routing than other methods.

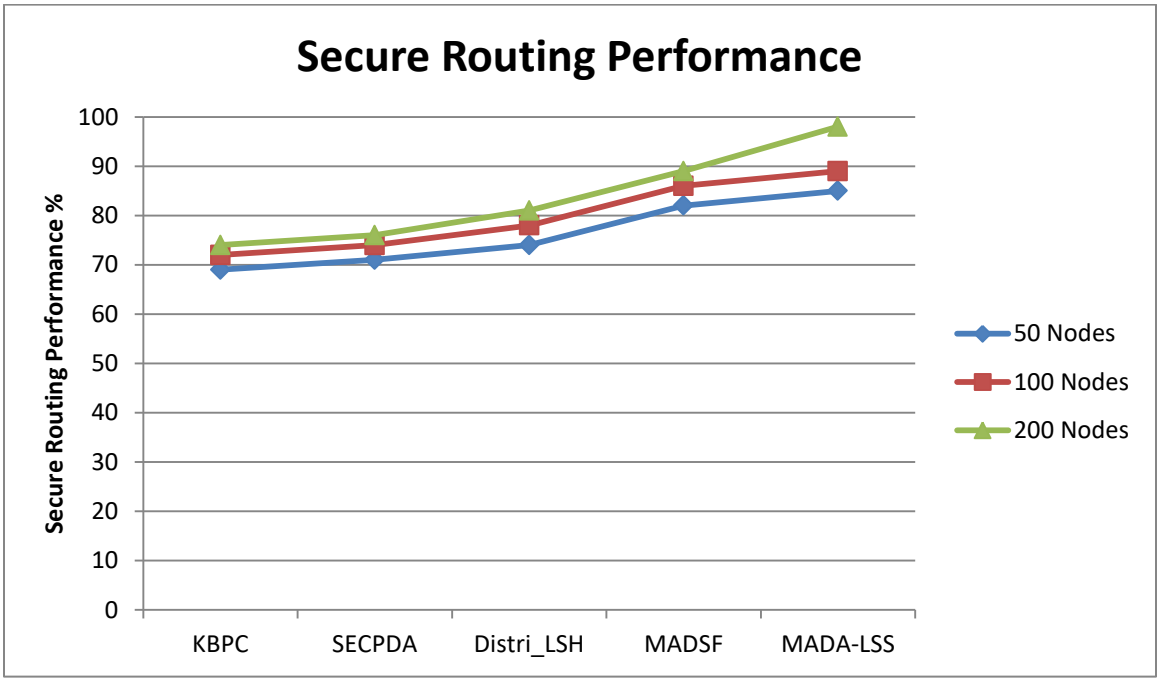

Figure 4: Analysis on Secure Routing Performance

The performance of secure routing has been measured for various approaches and presented in Figure 4. The proposed MADA-LSS algorithm has produced higher performance than other methods.

5. Conclusion

This article presents a novel mobility aware displacement approximation based location based service selection (MADA-LSS) towards QoS development in WSN. The method performs mobility aware displacement approximation according to the mobile location to predict the possible feature locations. According to the locations, the method finds the service points and routes towards each service points. Further, for each route the method computes the DSRM and THM values to perform efficient LSS and privacy preservation. The proposed MADA-LSS approach has produced higher performance on location based service selection and privacy preservation than other approaches.

1. Funding

No funding

2. Conflicts of interest

No conflict of interest

3. Availability of data

Data availability

Using dataset in this paper not using

4. Code availability

Advanced java

5. Authors' contributions

Based on the classification results produced the Data Rate Support Measure (DRSM) is taken to build the crop recommendation model.

References:

1. Fengyin Li, Pei Ren, Guoyu Yang, Yuhong Sun, Yilei Wang, Yanli Wang, Siyuan Li, Huiyu Zhou, "An Efficient Anonymous Communication Scheme to Protect the Privacy of the Source Node Location in the Internet of Things", Security and Communication Networks, vol. 2021, Article ID 6670847, 16 pages, 2021.

2. W. Lin et al., "Location-Aware Service Recommendations With Privacy-Preservation in the Internet of Things," in IEEE Transactions on Computational Social Systems, vol. 8, no. 1, pp. 227-235, Feb. 2021, doi: 10.1109/TCSS.2020.2965234.

3. S. Zhang, G. Wang, M. Z. A. Bhuiyan and Q. Liu, "A dual privacy preserving scheme in continuous location-based services", IEEE Internet Things J., vol. 5, no. 5, pp. 4191-4200, Oct. 2018.

4. Y. Xu, L. Qi, W. Dou and J. Yu, "Privacy-preserving and scalable service recommendation based on SimHash in a distributed cloud environment", Complexity, vol. 2017, pp. 1-9, Dec. 2017.

5. W. Gong, L. Qi and Y. Xu, "Privacy-aware multidimensional mobile service quality prediction and recommendation in distributed fog environment", Wireless Commun. Mobile Comput., vol. 2018, pp. 1-8, Apr. 2018.

6. L. Qi, X. Zhang, W. Dou, C. Hu, C. Yang and J. Chen, "A two-stage locality-sensitive hashing based approach for privacy-preserving mobile service recommendation in cross-platform edge environment", Future Gener. Comput. Syst., vol. 88, pp. 636-643, Nov. 2018.

7. X. Xu et al., "An edge computing-enabled computation offloading method with privacy preservation for Internet of connected vehicles", Future Gener. Comput. Syst., vol. 96, pp. 89-100, Jul. 2019.

8. M. Tang, X. Dai, B. Cao and J. Liu, "WSWalker: A random walk method for QoS-aware Web service recommendation", Proc. IEEE Int. Conf. Web Services, pp. 591-598, Jun. 2015.

9. L. Qi, X. Zhang, W. Dou and Q. Ni, "A distributed locality-sensitive hashing-based approach for cloud service recommendation from multi-source data", IEEE J. Select. Areas Commun., vol. 35, no. 11, pp. 2616-2624, Nov. 2017.

10. C. Xu, L. Luo, Y. Ding, G. Zhao and S. Yu, "Personalized Location Privacy Protection for Location-Based Services in Vehicular Networks," in IEEE Wireless Communications Letters, vol. 9, no. 10, pp. 1633-1637, Oct. 2020, doi: 10.1109/LWC.2020.2999524.

11. X. Liang, Q. Lu and M. Li, "Research on Web Service Selection Based on Improved Skyline Algorithm," 2019 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom), 2019, pp. 1323-1328,

12. Zhimin Li, Noise-added selection method for location-based service using differential privacy in Internet of Things, SAGE Publications, Advances in Mechanical Engineering, 2019.

13. J. Chen, H. Wu, P. Yang, F. Lyu and X. Shen, "Cooperative Edge Caching With Location-Based and Popular Contents for Vehicular Networks," in IEEE Transactions on Vehicular Technology, vol. 69, no. 9, pp. 10291-10305, Sept. 2020, doi: 10.1109/TVT.2020.3004720.

14. B. Liu, W. Zhou, T. Zhu, L. Gao, T. H. Luan and H. Zhou, "Silence is Golden: Enhancing Privacy of Location-Based Services by Content Broadcasting and Active Caching in Wireless Vehicular Networks," in IEEE Transactions on Vehicular Technology, vol. 65, no. 12, pp. 9942-9953, Dec. 2016, doi: 10.1109/TVT.2016.2531185.

15. S. Badsha et al., "Privacy Preserving Location-Aware Personalized Web Service Recommendations," in IEEE Transactions on Services Computing, vol. 14, no. 3, pp. 791-804, 1 May-June 2021, doi: 10.1109/TSC.2018.2839587.

16. S. Badsha, X. Yi, I. Khalil and E. Bertino, "Privacy preserving user-based recommender system", Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst., pp. 1074-1083, 2017.

17. .J. Liu, M. Tang, Z. Zheng, X. F. Liu and S. Lyu, "Location-aware and personalized collaborative filtering for web service recommendation", IEEE Trans. Serv. Comput., vol. 9, no. 5, pp. 686-699, Sep./Oct. 2016.

18. J. Shu, X. Jia, K. Yang and H. Wang, "Privacy-preserving task recommendation services for crowdsourcing", IEEE Trans. Serv. Comput., 2018.

19. Sivapragash Chidambaram, Location Based Optimized Service Selection for Secure and Reliable User Perspective Data Management with Cloud Computing For Increased Performance of Smart Grids, Energies, 2019.

20. Ashween, R., Ramakrishnan, B. & Milton Joe, M. Energy Efficient Data Gathering Technique Based on Optimal Mobile Sink Node Selection for Improved Network Life Time in Wireless Sensor Network (WSN). Wireless Pers Commun 113, 2107–2126 (2020).

21. E. Tong, L. Chen and H. Li, "Energy-Aware Service Selection and Adaptation in Wireless Sensor Networks with QoS Guarantee," in IEEE Transactions on Services Computing, vol. 13, no. 5, pp. 829-842, 1 Sept.-Oct. 2020, doi: 10.1109/TSC.2017.2749227.

22. Dou, H., Chen, Y., Yang, Y. et al. A secure and efficient privacy-preserving data aggregation algorithm. J Ambient Intell Human Comput (2021). https://doi.org/10.1007/s12652-020-02801-6.

23. Rajasekar, S. & Palanisamy, C. & Saranya, K.. (2021). Privacy-preserving location-based services for mobile users using directional service fetching algorithm in wireless

networks. Journal of Ambient Intelligence and Humanized Computing. 12. 10.1007/s12652-020-02361-9.

24. Fengyin Li, Pei Ren, Guoyu Yang, Yuhong Sun, Yilei Wang, Yanli Wang, Siyuan Li, Huiyu Zhou, "An Efficient Anonymous Communication Scheme to Protect the Privacy of the Source Node Location in the Internet of Things", Security and Communication Networks, vol. 2021, Article ID 6670847, 16 pages, 2021.