International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-2, December, 2019

Towards Developing Secure Data Aggregation with Integrity Verification Model (SDA-IV) in People Centric Sensing Systems

K.R.Jansi, S.V.Kasmir Raja

Abstract*: In present scenario of vast developments in wireless communication methods, embedded device based operations and mobile communications, sensor based techniques are widely adopted. Such systems are termed as People Centric Sensing Systems, which become very popular and acquires greater attention of researchers recently. However, security and privacy in transmitting data has been the major issue in People Centric Sensing Network (PCSN). For handling that problem efficiently, this paper presents a model called Security Data Aggregation and Integrity Verification (SDA-IV) model for providing privacy preserved data sharing between devices in PCSN. A new peer-to-peer oriented secure data sharing is achieved with the proposed model by making the user to shares their data randomly with other nodes along with the incorporating of integrity checking conceit. Moreover, the work comprises four phases: Initial Setup, Data Division and Encryption, Data Aggregation and Integrity Verification. Homomorphic Message Authentication Code is user for privacy preserving process and Hashing Functions are incorporated for integrity verification of shared data. Furthermore, the efficiency of the proposed SDA-IC model is evidenced using simulation results and comparative evaluations.

Keywords: People Centric Sensing Network, Privacy Preserving, Secure Data Aggregation, Integrity Verification, Homomorphic Encryption and MAC.

I. INTRODUCTION

In the current decade, with the enormous increase of smart phones and mobiles, an efficient network is required for effective sensing of the corresponding environment and providing communication between the people. This can be achieved with the People Centric Sensing Networks (PCSN) [1], which involves in performing sensing based computations, storage and interaction between people and the environment with appropriate data collection, processing and data transmission functions. The advanced networking model PCSN are used in environmental observation [2], congestion control [3] and network traffic managements [4]. Moreover, the systems of people centric sensing networks are technically different from the typical sensor networks that only concentrate on environmental monitoring and data accumulation. Here, the devices are not administrated or managed by single authorities that are belonging to individual users. Another main difference is the devices do not have any energy or power constraints, since it gets charged periodically. Unlike sensor nodes, the devices of people centric sensing networks are highly mobile in nature and hence, the topology for communication is dynamic. Then, the sensing data are dependent to provide communications between the humans and their environment.

Though there are several benefits in PCSN, still there are some security oriented issues remains unsolved. When analyzing and processing with the sensitive information of people, privacy preservation of data sharing is to be focused effectively. So, providing privacy preserving in data transmission in PCSN is a very challenging issue in present scenario of wireless communications [5]. For example, in health care applications, the data comprises the details about the blood pressure, weight, age, etc. The people does not want to provide their personal content to any other parties for ensuring that their content are private and safe. In some other application like CarTel [6], traffic data are used for making optimal route plan. When there exist any malicious nodes that may collapse the process, results in road congestion. These instances indicate the significance of privacy preserving and secure data aggregation in PCSN. There are several chances for the attackers to hack the shared data during the aggregation process. Henceforth, there is a wide requirement on secure data sharing model for efficient data aggregation in PCSN. The framework of People Centric Sensing Network with their components is presented in Fig 1.

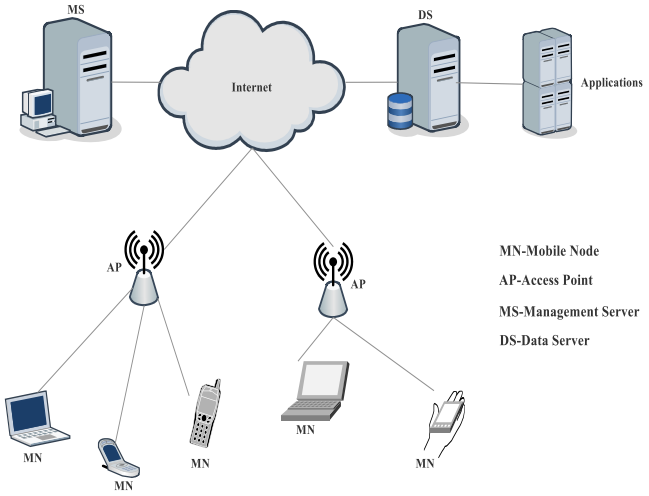

Fig .1. People Centric Sensing Network Framework and Components

Revised Manuscript Received on December 30, 2019.
* Correspondence Author
Mrs.K.R.Jansi*, Assistant Professor, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India. Email: jansik@srmist.edu.in
Dr.S.V.Kasmir Raja, Adjunct Professor,Department of IQAC, SRM Institute of Science and Technology, Chennai, India Email: svkr@yahoo.in

A. *Components of PCSN*

As given in Fig. 1, the system model of people centric sensing network mainly contains Management server, data server, Access Points and mobile devices or nodes. For performing seamless communication functions, the management and data severs involve in effectively managing and storing the data. The responsibility of aggregator is to combine the received data into one and transmitting that aggregated data to the server. The MNs are the mobile nodes that may be any kind of communication device that are having higher mobility, such as PDA, smart phones, PDA, cameras and so on. It is assumed that the mobile nodes can access the common access points, which are further connected through the internet. Each mobile node has distinctive identity and their work is to sense the environment for reporting the observed data to the access point or for processing data aggregation. The Management Server (MS) handles Identity related information and registration of entities in the network. The Data Server (DS) is responsible for storing the aggregated data or sensed data.

B. *Security Requirements*

In any process of data aggregation model, there are possibilities of adversaries can attack and access the data. For solving this issue, it is very significant to develop a new model for secure data aggregation in PCSN. Though the PCSNs are very much developed and focused in recent days, the model has to be designed in such a manner to solve link failures and security issues and also to handle the robustness. In previous works of privacy preserving in people centric sensing networks, there are limitations are noted which are focused to be solved using some cryptographic functionality. Moreover, developing a privacy preserving data aggregation and data sharing model is a complicated and challenging process. It is to be assured that the shared data through the network has not been revealed to any other third parties. On the other side, data integrity of aggregated data is also to be ensured. The following security requirements should be satisfied in the secure data aggregation model,

- The main objective is to ensure data confidentiality and data integrity of shared private data of users in People Centric Sensing Networks.
- Data Confidentiality is achieved by securing the data with Homomorphic Encryption and Homomorphic MAC for the observed or shared data.
- Data Aggregation is processed with the additive operations and Hash Functions are incorporated before sharing the data through the network.
- Finally, Integrity Verification (IV) is performed based on the generated MAC, hash derivations and timestamp values.
- The model evaluations have been carried out based on the security and performance measures. Moreover, the results evidence that the proposed model provides better security for user data.

In the proposed model, the security requirements are derived with respect to prevent the data from attacks such as External Attack, Internal Attack and Collusion Attack.

- External Attack is the attack when an attacker tries to modify the data that are transmitted between the MN and aggregator.
- Internal Attack happens when the aggregator involves in acquiring the private data of all nodes and tries to change the original content.
- Collusion Attack is the attack that happens when the attacker tries to get the data through some collusion activity.
- Message Tampering is the attack that happens when the actual data to be transmitted via the network is corrupted before transmitting to other.
- On-off Attacks are happened when the malicious nodes are being active and inactive instead to be in the trusted framework of the networks.

Moreover, the security factors that are focused in this work for secure data aggregation are, Privacy Preservation, Data Authentication and Data Integrity. For achieving the factors effectively, the Security Data Aggregation and Integrity Verification (SDA-IV) is proposed in this paper. The model considers the data security in PCSN along with the computational efficiency. The remainder of this work is organized as follows: Section II presents the detailed review about the existing works. Section III explains about the construction and work process of Security Data Aggregation and Integrity Verification (SDA-IV) model that utilized cryptographic techniques for ensuring security in various aspects. Security analysis and performance evaluations of the proposed work are presented in Section IV. Finally, Section V concludes the paper narration with some pointers for further enhancements.

II. RELATED WORKS

This section deliberates the works and methodologies that are developed focusing on the secure data aggregation and data sharing in various wireless communication networks, specifically in People Centric Sensing Networks. In [5], Anonysense framework has been developed for detecting the anonymous operations in performing specific tasks and reporting to the concern AP. Further, Privacy preserving model for data aggregation has been derived in [7] and named as Prisense. The model has been developed in supporting additive and non-additive aggregative operations for data aggregation. In [8], secure data aggregation for providing data confidentiality in sensor networks. Further, in [9] Generic Privacy Preservation Solutions has been derived for effective data aggregation in wireless sensor networks. A Resilient aggregation model has been derived for protecting the data aggregation from malicious node attacks in sensor networking models [10]. Hierarchical Aggregation model for sensor networks has been designed in [11]. Further, a robust data aggregation model has been described in [12]. In cases of people centric sensing networks, the devices or nodes are belonging to individual persons but cannot be controlled by single admin. Hence, there are always needs of secure data aggregation process, which cannot be acquired from some other network methodologies such as Wireless Mobile Networks (WMNs), Wireless Sensor Networks (WSNs), Wireless Mesh Networks and so on. Secure aggregation model that serves for providing data confidentiality in public subscribe system in [13].

Furthermore, in [14], location based data aggregation model called PrivStats has been developed. The model designed in terms of false data an injection attack that also supports data integrity. Fault tolerance based aggregation with the security enforcement has been done by the authors of [15]. And, the model has been named as Efficient Privacy Preserving Fault Tolerance Aggregation (EPPFTA) and the results are evaluated based on the performance factors such as packet delivery rate and transmission delay.

In [16], PPsense has been developed for providing privacy preserving network sensing. The model used Attribute based Encryption for securing the data. A location based privacy preserving model for PCSN was given in [17]. The process was complicated to process when several reports are given to the same point. Further, PriSense has been derived for data aggregation for security purpose of data sharing [18]. Location based privacy preserving for sensor networks has been presented in [19], which was not feasible for people network sensing. Security oriented challenges and methodologies have been well analyzed and the available models have been discussed in [20]. Poolview based method has been discussed in [21] for measuring the computing complications without concentrating on the aggregation process and its security. For providing data security for the unauthorized users, PEPSI was developed in [22]. The method was given as Privacy Enhancing Participatory Sensing Infrastructure, which contained no preferences for data aggregations.

III. WORK PROCESS OF SECURITY DATA AGGREGATION AND INTEGRITY VERIFICATION (SDA-IV) MODEL

This section describes the work process of the proposed Security Data Aggregation and Integrity Verification (SDA-IV) model. The work comprises four phases, namely,

1. Setup Phase
2. Data Encryption and Data Division
3. Secure Data Aggregation (SDA)
4. Integrity Verification (IV)

Moreover, the functions involved in the proposed model are given in Fig. 2. The framework comprises three layers called Bottom, middle and top layers that performs the respective operations from the aforementioned phases.

A. *Setup Phase*

This phase is to prepare the network with required security and system factors in prior for the mobile devices and the Aggregation point (AP). When the devices are intend to send the data to its corresponding AP. Before transmitting, the data is to be secure by encryption and the secured data is transmitted for aggregation. Here, the AP is responsible for data aggregation and data verification that are acquired from their corresponding device in PCSN. The verification process is explained in phase 4 and the base station involves in the process of IV and the data that are successful in Integrity Verification process will be decrypted for acquiring the original data.

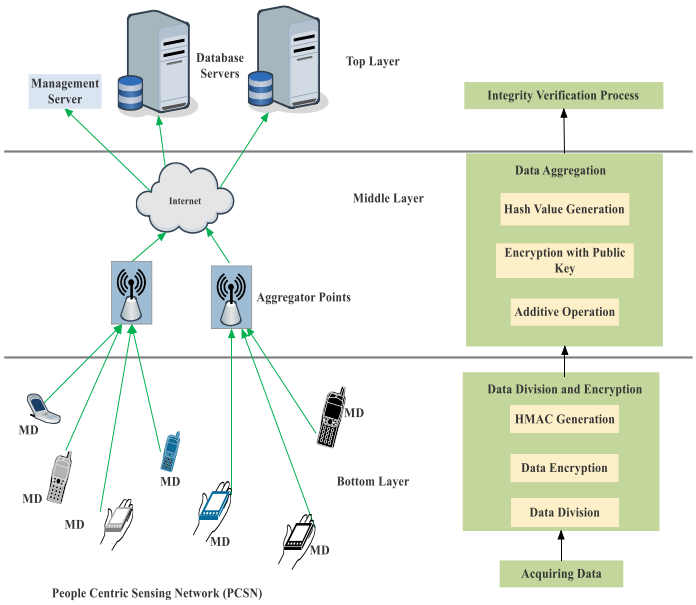

Fig. 2. Framework of Proposed SDA-IV Model in PCSN

The Setup phase comprises the following steps,

1. Each device in the network is assigned with an Identity as Mobile Device $MD_i \in [1, \dots, n]$.

2. Aggregation Points are determined for certain group of devices and ID is assigned.

3. The MS shares a unique key pair for all nodes that are under same access point or aggregation point for producing HMAC for integrity verification.

B. *Data Division and Encryption*

***Data Division Process*:**

For tightening the security process, the data is divided and swapped in pairwise manner. It is considered that there is an aggregator linked with several numbers of devices that are given as, $MD = \{md_1, md_2, .., md_n\}$. For certain time period, the devices acquire data $D = \{d_1, d_2, .., d_n\}$ considerably.

In the first phase, each mobile device, md_i divides the collected data $D_i (i \in 1,2, \dots, n)$ into 'n' portions as, $P_{ij} (i \in 1,2, \dots, n), (j \in 1,2, \dots, n)$ respectively, where, 'n' denotes the number of mobile devices that are presented in the network, which can be stated as,

$$\begin{cases} d_1 = \sum_{j=1}^{n} P_{1j}, \\ d_2 = \sum_{j=2}^{n} P_{2j}, \\ \dots \\ d_n = \sum_{j=n}^{n} P_{nj} \end{cases} \quad (1)$$

In the second phase, the divided portions of data are swapped with each other. The portion P_{11} is secured by MD_1, when others are distributed.

On considering that, a device MD_1 requires sending n-1 portions of data $P_{ij} (j \neq i)$ to others, then, data encryption operations are carried out, as explained below.

The proposed model utilizes homomorphic encryption that computes fast encryption of data and decryption. The algorithm is mainly based on the probabilistic asymmetric process that used secure scalar factor for privacy preserving in shared data. The Key generation process, encryption and decryption steps are explained below.

Key Generation Process:

i. Select two random large numbers that are mutually independent that are x and y, which gives gcd(xy, (x-1)(y-1))=1. It is ensured from the random numbers that both are in equal length.

ii. Derive n=xy and $\gamma = 1$, which is the constant factor, for (x-1, y-1).

iii. Select a random integer R , where $R \in \mathbb{Z}_{n^2}^*$.

iv. It is given that 'n' separates the order of R based on the availability of the modular multiplicative inverse (δ), which is given below,

$$\delta = (F(R^{\gamma} mod^{n^2}))^{-1} \, mod \, n \qquad (2)$$

Where, function F is given as, $F(X) = (x-1)/n$

v. The public key is given as (n, R)

vi. The secret key is given as (γ, δ)

Encryption Process:

Given Data 'D', where, 0≤D≤n, choose a random number 'r', which also lies between 0 and n. And, the cipher text of given data is stated as,

$$CT = R^m . r^n mod n^2 \qquad (3)$$

Decryption Process:

The obtained encrypted data 'CT' can be converted into original data as in (4).

$$D = F(CT^{\gamma} mod n^2). \delta \, mod \, n \qquad (4)$$

Incorporation of HMAC:

In this work, HMAC is generated for the encrypted content, instead of original content that effectively avoids the node compromised attacks and node capture attacks. The keys that are used to generate the HMAC for certain message that are under similar aggregation point uses identical keys. The pseudo code is presented in Table I.

Table -I: Pseudo Code for HMAC Generation

Begin
Setup Initialization
Key Generation:
Select $k_1 and \, k_2 \in \mathbb{Z}_{n^2}^*$, then $K = k_1, k_2$
HMAC Generation,
Do
Compute
$U \leftarrow F(k_1) \in \mathbb{Z}_{n^2}^*$
$P \leftarrow G(k_2(ID, i))) \in \mathbb{Z}_{n^2}^*$
$HMAC_T \leftarrow (U.V) + P) \in \mathbb{Z}_{n^2}^*$
Call Aggregate_Procedure ()
Call Intergity_Verification()
End

C. *Data Aggregation*

All the divided and concealed data are aggregated securely and the process is explained in this section, which is executed when there is a call for Aggregate_Procedure (). Here, additive aggregation function is used for the concealed data, which is given as (AD-Aggregated Data).

$$\begin{cases} d_1{}' = P_{11} + \sum_{j=1}^{n} P_{1j}, \; (i \neq 1) \\ + \\ d_2{}' = P_{22} + \sum_{j=2}^{n} P_{2j}, \; (i \neq 2) \\ + \\ \dots \dots \\ + \\ d_n{}' = P_{nn} + \sum_{j=n}^{n} P_{nj}, (i \neq n) \end{cases} \qquad (5)$$

And, the final Aggregated Data is given as,

$$AD = \{d_1{}' + d_2{}' + \cdots + d_n{}'\} \qquad (6)$$

It is to be denoted that the secret keys are utilized for MD to MD communications are updated often. Hashing technique is enforced for this one time pad, with the consideration that the initial private key as, K_1, and the consequent secret keys up to K_n are given as,

$$\begin{cases} K_2 = HS(T \parallel K_1) \\ K_3 = HS(T \parallel K_2) \\ \dots \\ K_n = HS(T \parallel K_{n-1}) \end{cases} \qquad (7)$$

The resultant data of each MD is presented in Table II. Here, $d_i (i \in (1,2, \dots, n))$ is the original data of mobile devices $MD_i (i \in (1,2, \dots, n))$ and $d_i{}' (i \in (1,2, \dots, n))$ is the concealed data of $MD_i (i \in (1,2, \dots, n))$ after performing the above operations. In this manner, the original data that are observed by all devices have been secured. Meanwhile, the aggregation of device data does alter, as, $\sum_{i=1}^{n} d_i = \sum_{i=1}^{n} d_i{}'$. Hence, the aggregator can acquire the actual and appropriate data and does not reveal the original data of each MD. After the MDs shares the observed data, the original data is concealed. All the secured data $d_i{}' (i \in (1,2, \dots, n))$ will be encrypted with the public key of management server before perform data transmission that can be given as,

$$ED_i = S_{pk}(d_i{}') \, (i \in (1,2, \dots, n)) \qquad (8)$$

Further, hash value will be generated by each MD, with their identity (ID), timestamp ts and the encrypted data ED_i. And, the hash function is denoted as, $HS(ID \parallel ts \parallel ED_i)$ for helping the aggregator point to check that the shared private data of the users are not changed or replayed anywhere in the transmitted period. Finally, the Mobile devices provide the aggregator about the data such as ED_i, timestamp and hash rate. When the aggregator receives the information, the data integrity verification is done as explained in the next section.

Table- II: Resultant Data Obtained by the Above Operations

	MD_1	MD_2	...	MD_i	...	MD_n	Original Data
MD_1	P_{11}	P_{12}	...	P_{1i}	...	P_{1n}	d_1
MD_2	P_{21}	P_{22}	...	P_{2i}	...	P_{2n}	d_2
...	...	...	...	...	...	...	...
MD_i	P_{i1}	P_{i2}	...	P_{ii}	...	P_{in}	d_i
...	...	...	...	...	...	...	...
MD_n	P_{n1}	P_{n2}	...	P_{ni}	...	P_{nn}	d_n
Concealed Data	d_1'	d_2'	...	d_i'	...	d_n'	

D. *Integrity Verification in PCSN*

With the obtained cipher text, timestamp and generated hash value, the integrity verification is performed and the pictorial representation is presented in Fig. 3. This process executes when there is a call for the Integrity_Verification(). The IV process is carried out based on three functions such as timestamp, HAMC and hash function.

Timestamp based Verification:

The BS checks the timestamp validity of the message, whether the data is delivered within certain period of time. If it is valid, then, further verification process for HMAC and Hash value for end to the verification is effectively carried out. Otherwise, the data will be discarded by the base station, with a note that the data is a non-reliable one.

HMAC based Verification:

The base station computes the HMAC and compares that the received content. If both are equal, it can be stated that the received encrypted data are not altered by any kind of adversaries.

End-to-End Verification:

The End-to-End Verification process is performed for checking the data for final integrity verification, for processing the aggregated data. Based on the hash value, the verification process is performed. The data from each aggregator point is checked specifically, after establishing that, the base station initiates the decryption process. When the verification process is not successful, then, the data will be discarded. The final verification process is done at this section for checking the content modification and the possibilities of adversary's presence. If the hash value at base station is similar to the hash value of aggregated data, it is mentioned as success and no attacks are noted during the process of data aggregation. By this process, both the base station and the aggregator point may not have the knowledge about the original data from the mobile devices.

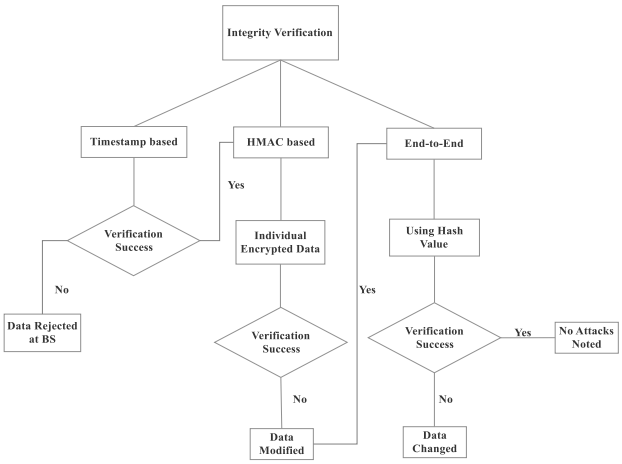

Fig. 3. Workflow of Integrity Verification Process

IV. EXPERIMENTS AND RESULTS

This section comprises the security based performance evaluations and comparative result analysis of the proposed model. Moreover, the results are evaluated based on secure communications, transmission delay and communication overhead. The obtained results are compared with the existing models such as Anonysense [5] and EPPFTA [15]. Further, the model is evaluated using the Network Simulation Tool called NS-2, with the initial simulation settings, mentioned in Table III, since, the real-time evaluations are complicated to process.

Table -III: Initial Simulation Settings

SIMULATION PARAMETERS	VALUES
Simulator	NS-2.34
Sensing area	1000 m^2
Simulation Time	800 s
No. of MDs	Varies from 100-1000
Simulation End Time	50 Seconds
Mobility Model	Random Waypoint
MAC type	IEEE 802.11
Traffic type	CBR
Mobility speed	5 m/s
Avg. Hop Distance between MDs	10 m
Payload Size	512 bytes
Transmission Range of each MD	500

A. *Security based Evaluations*

This section explains about the security based evaluations carried out with the proposed model based on the design goals presented in Section I. For the purpose of analysis, the following conditions are assumed, that,

i. The aggregation point could be compromised by attackers.

ii. The MDs can be malicious.

iii. The data communication in the network can be eavesdropped by the attackers.

iv. The adversary may try to change the content of data.

Based on the assumptions, the analysis is carried out and the results are presented in the following charts. Moreover, here, secure rate of the links for data aggregation is evaluated based on the probability of attacks that are happened to occur in the communications. In Fig. 4, it is assumed when collusion attack is happened in the data aggregation process, the secure rate is computed.

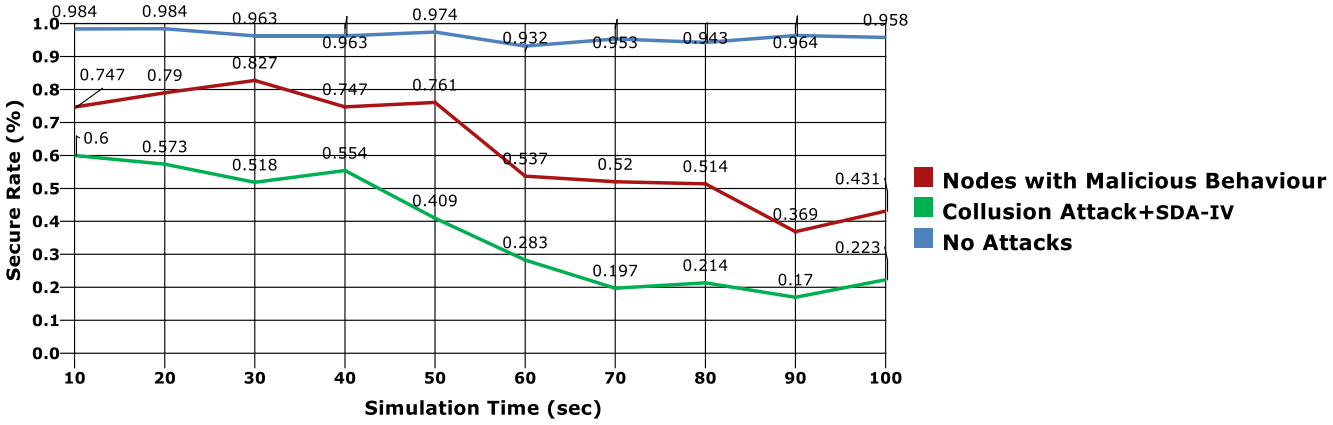

Fig. 4. Analysis with Collusion Attacks

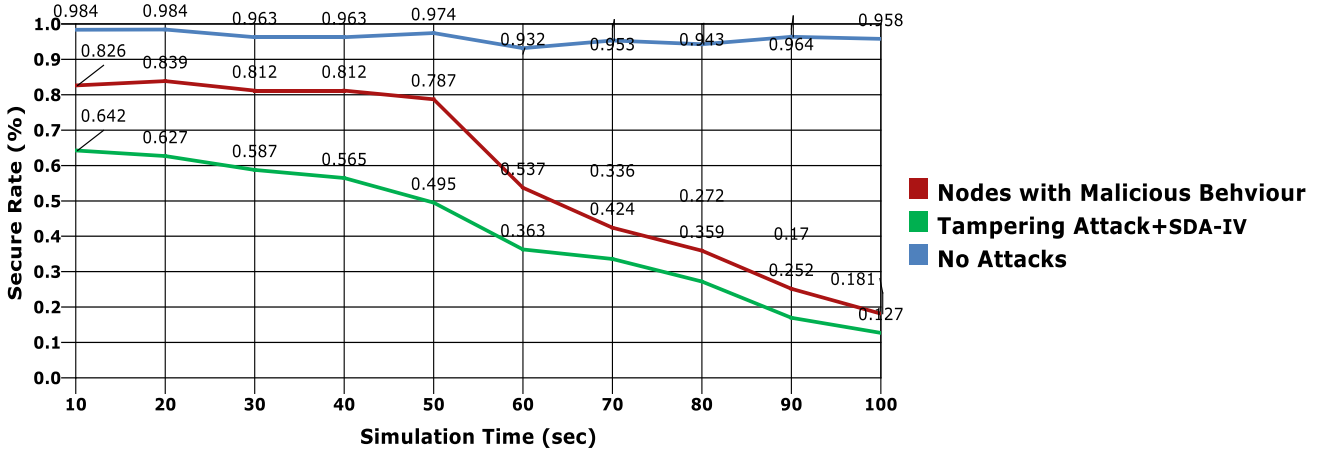

Fig.5. Model Evaluation with Tampering Attacks

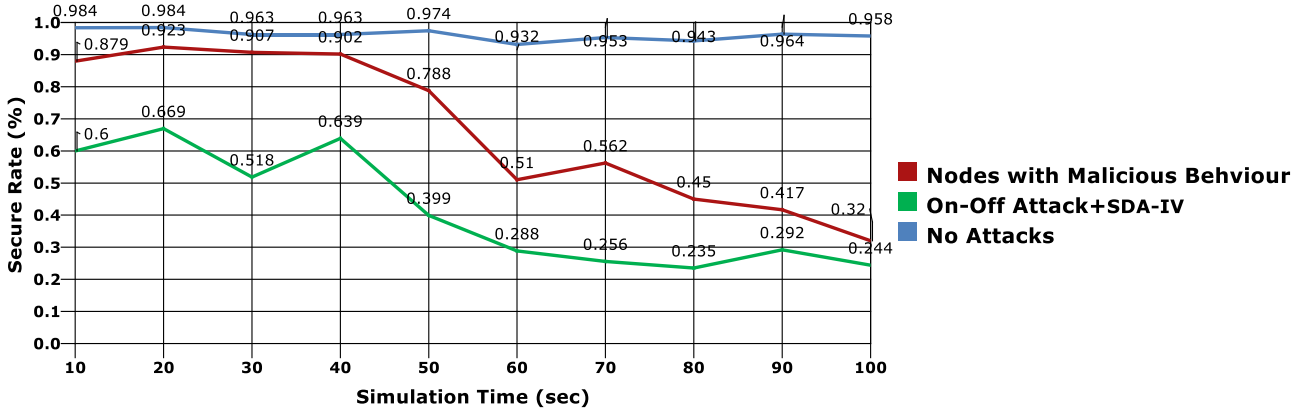

Fig. 6. Security Computation against On-Off Attack

With the proposed model, the secure rate values are minimal based on the impact of attacks. Based on that scenario, the Fig.5. and Fig.6.presents the graph provides the results, when tampering attack and on-off attacks, respectively. It is obvious from the graphs that the secure rates when enforced with the proposed SDA-IV model, the attacks are captured effectively by computing lesser. The communication process with no attacks shows higher secure rate, which is almost equal to 1. When the communication process is happened before the detection of attacks, the secure rates are generated as, 0.673, 0.578 and 0.713 in average, for the evaluations of the presence of malicious node behaviours respectively.

The proposed model uses, homomorphic encryption with data division technique, which makes the aggregation process more secure from various attacks. Moreover, HMAC and hashing techniques are incorporated for Integrity Verification process. Hence, in cases of the incorporation of proposed model, the results show minimal secure rates that results the presence of adversaries that are to be resolved or the malicious node are to be revoked for efficient and secure communication in Public Centric Sensing Network.

B.*Comparative Evaluations*

This section presents the performance based comparative evaluations, includes, communication overhead, packet delivery ratio, transmission delay and packet drop. Those are the significant performance metrics that are to be evaluated for evaluating the goodness of the proposed network model. The primary factor for measuring the performance of the proposed SDA-IV model is the communicational complexity. There are the possibilities of third party attacks in the process of data aggregation. Here, the communication complexity is given as $O(m * n)$, where 'm' denotes the number of mobile devices and 'n' denotes the number third parties to be involved in the process, that are computed to be minimal in any communication model. And, the results are presented in the Fig. 7.

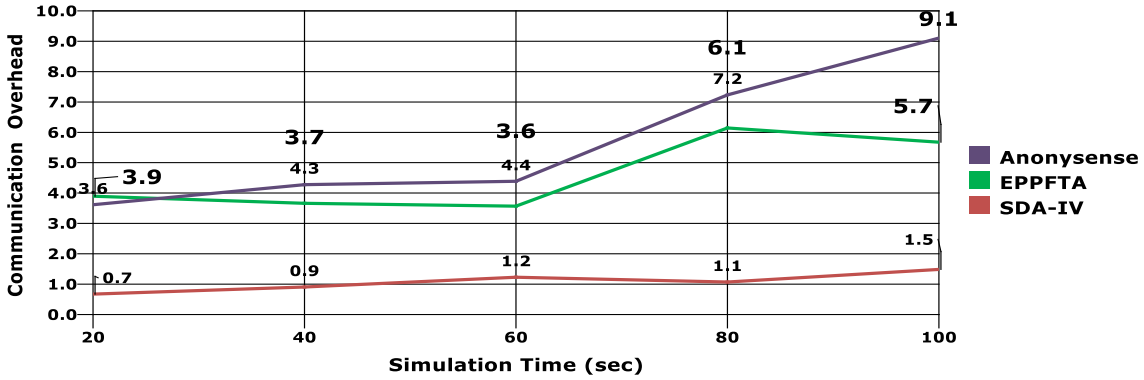

Fig.7. Communication Overhead Comparison

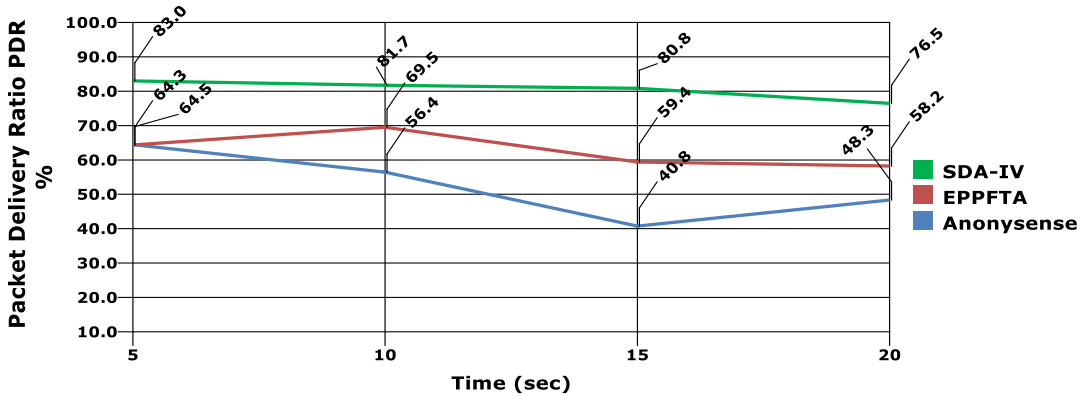

Fig. 8.Packet Delivery Ratio Comparison between Models

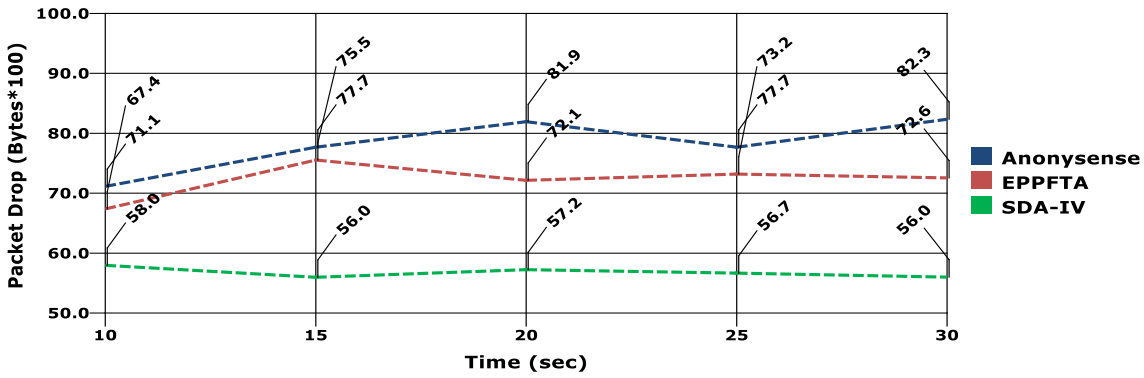

Fig. 9: Simulation Time Vs Packet Drop

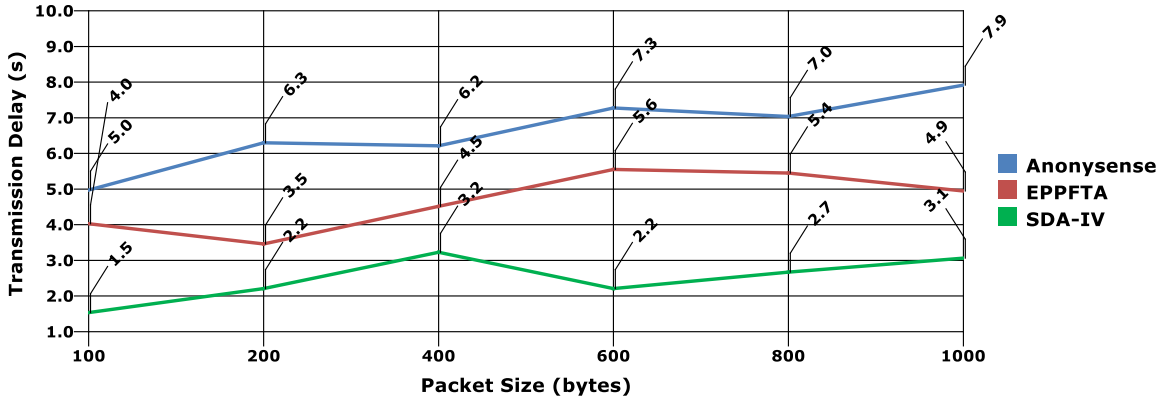

Fig. 10: Analysis on Transmission Delay

The next important factors in performance analysis of a network model are Packet delivery ratio and packet drop. Packet Delivery Ratio (PDR) can be computed with the ratio to the amount of packets delivered to the total amount of data packets sent through the network. The obtained results are provided in the Fig. 8. The graph in Fig. 9 .presents the packet that is dropped from delivery. The results are explicitly showing that packet delivery rate for the proposed model is higher than other compared works with minimal rate of packet drop.

Further, using the proposed model, transmission delay is effectively reduced. In secure data aggregation model, there are less possibilities of attacks and mainly involved in reducing the transmission delay, which is also to be concentrated on developing an aggregation model in communication network. Here, the transmission delay is evaluated based on the packet size of data. The results are portrayed in the Fig. 10. And, from the figure, it can be noted that the average transmission delay achieved is about 2.73 sec, which is the lower value than the delay produced by other compared works.

V. CONCLUSION

In this paper, a novel model called Secure Data Aggregation with Integrity Verification (SDA-IV) for providing efficient and secure communication in People Centric Sensing Network (PCSN). The model incorporates homomorphic encryption, HMAC and hashing technique. Moreover, the model is implemented with four phases and data division before HMAC generation is performed for effective privacy preserving. Integrity Verification is carried out using hashing technique that check for the data modification by any adversaries in case. The simulation results show that the proposed model provides better PDR with minimal transmission delay and packet drop. Furthermore, security based evaluations are also done with the proposed model and the results are provided. Analyzing the results, it can be stated that the proposed SDA-IV model provides privacy preserved data aggregation in PCSN.

In future, the work can be enhanced by utilizing blockchain based technique for tightening the security process by considering newer attacks.

REFERENCES

1. K. R. Jansi and S. V. Kasmir Raja, “A survey on Privacy Preserving Data Aggregation Schemes in People Centric Sensing Systems and Wireless Domains” Indian Journal of Science and Technology, Vol 9, No. 37, pp. 1-7, 2016.
2. E. Paulos and T. Jenkins, “Urban Probes: encountering our emerging urban atmospheres,” in ACM CHI’05, Portland, pp. 341–350, 2005.
3. A. Thiagarajan, L. Ravindranath, K. LaCurts, S. Madden, H. Balakrishnan, S. Toledo, and J. Eriksson, “VTrack: accurate, energy-aware road traffic delay estimation using mobile phones,” in ACM SenSys’08, Berkeley, CA, Nov, pp. 85–98, 2009.
4. J. Froehlich, T. Dillahunt, P. Klasnja, J. Mankoff, S. Consolvo, B. Harrison, and J. Landay, “UbiGreen: investigating a mobile tool for tracking and supporting green transportation habits,” in CHI’09, Boston, MA, pp. 1043–1052, 2009.
5. C. Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin, and N. Triandopoulos, “AnonySense: privacy-aware people-centric sensing,” in Proceedings of the 6th International Conference on Mobile Systems,Applications, and Services (Mobisys ’08), pp. 211– 224, ACM, Breckenridge, Colo, USA, June 2008.
6. B. Hull, V. Bychkovsky, Y. Zhang, K. Chen, M. Goraczko, A. Miu, E. Shih, H. Balakrishnan, and S. Madden, “CarTel: A distributed mobile sensor computing system,” in ACM SENSYS’06, Boulder, CO, pp. 125–138. 2006.
7. J. Shi, R. Zhang, Y. Liu, and Y. Zhang, “PriSense: privacy preserving data aggregation in people-centric urban sensing systems,” in Proceedings of the IEEE International Conference o Computer Communications (INFOCOM ’10), San Diego, Calif, USA, March 2010.
8. T. Feng, C. Wang, W. Zhang, and L. Ruan, “Confidentiality protection for distributed sensor data aggregation,” in Proceedings of the 27th IEEE International Conference on Computer Communications (INFOCOM ’08), pp. 475–483, Phoenix, Ariz, USA, April 2008.
9. W. Zhang, C. Wang, and T. Feng, “GP2S: generic privacy preservation solutions for approximate aggregation of sensor data,” in Proceedings of the 6th IEEE Annual International Conference on Pervasive Computing and Communications (PerCom ’08), pp. 179–184, Hong Kong, March 2008.
10. D. Wagner, “Resilient aggregation in sensor networks,” in Proceedings of the 4th ACMWorkshop on Security of Ad Hoc and Sensor Networks (SASN ’06), pp. 71–82, Alexandria, Va, USA, October 2006.
11. H. Chan, A. Perrig, and D. Song, “Secure hierarchical in network aggregation in sensor networks,” in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS ’06), pp. 278–287, ACM, Alexandria, Va, USA, November 2006.
12. M. Conti, L. Zhang, S. Roy, R. di Pietro, S. Jajodia, and L. V. Mancini, “Privacy-preserving robust data aggregation in wireless sensor networks,” Security and Communication Networks, vol. 2, no. 2, pp. 195–213, 2009.
13. K. Minami, A. J. Lee, M. Winslett, and N. Borisov, “Secure aggregation in a publish-subscribe system,” in WPES’08, Alexandria, Virginia, USA, 2008, pp. 95–104.
14. R. A. Popa, A. J. Blumberg, H. Balakrishnan, and F. H. Li, “Privacy and accountability for location-based aggregate statistics,” in CCS’11, Chicago, Illinois, USA, 2011, pp. 653–666.

15. K. R. Jansi, S. V. Kasmir Raja and G. K. Sandhia, "Efficient privacy-preserving fault tolerance aggregation for people-centric sensing system" Service Oriented Computing and Applications, 2018, Vol. 12, pp. 305–315.
16. Ziling Wei, Baokang Zhao, Yujing Liu, Jinshu Su, "PPSense: A novel Privacy-Preserving system in people-centric sensing networks" 2013 8th International Conference on Communications and Networking in China (CHINACOM), pp. 461-467.
17. Tang, Karen P., "Putting people in their place: an anonymous and privacy-sensitive approach to collecting sensed data in location-based applications." Proceedings of the SIGCHI conference on Human Factors in computing systems. ACM, 2006.
18. Shi, Jing, "Prisense: privacy-preserving data aggregation in people centric urban sensing systems." INFOCOM, 2010 Proceedings IEEE. IEEE, 2010.
19. Li, Shuai,. "Location privacy preservation in collaborative spectrum sensing." INFOCOM, 2012 Proceedings IEEE. IEEE, 2012.
20. A. Kapadia, D. Kotz, and N. Triandopoulos, "Opportunistic sensing: Security challenges for the new paradigm," in Proc. COMSNETS, Jan. 2009.
21. R. K. Ganti, N. Pham, Y.-E. Tsai, and T. F. Abdelzaher, "Poolview: Stream privacy for grassroots participatory sensing," in Proc. ACM SenSys, Nov. 2008, pp. 281–294.
22. E. Cristofaro and C. Soriente, "PEPSI: Privacy enhancing participatory sensing infrastructure," in Proc. ACM WiSec, June 2011.

AUTHORS PROFILE

Mrs.K.R.Jansi currently works as Assistant professor at the Department of Computer science and Engineering, SRM institute of science and technology, Kattankulathur. Her research interest includes data aggregation in wireless sensor networks, security in people centric sensing networks.

Dr.Kasmir Raja S.V currently works as Adjunct Professor /IQAC, SRM institute of science and technology, Kattankulathur. His research interest includes Artificial Intelligence and Computer Communications (Networks).