Received: November 24, 2018

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

EPPAA- Enhanced Privacy Preserving - Anonymity Authentication Model with QPSO for Wireless Mobile Networks

Senthil Kumar Thillaigovindan[1]* **Prabakaran Subramaniyan[1]**

[1]*Department of Computer Science and Engineering,*
SRM Institute of Science and Technology, Chennai, India
* Corresponding author's Email: senthilkumar.t@ktr.srmuniv.ac.in

Abstract: In Wireless Mobile Networks (WMN), the proliferation of mobile devices and smart phones stimulates an array of personalized information services that exploits the user's personal data for processing. So, it is very significant to preserve the data privacy and protect the integrity of data of mobile users. However, as the WMN devices are heterogeneous and highly independent, it is challenging to achieve privacy protection and efficient authentication in better levels. With those concerns, this paper illustrates a new model called Enhanced Privacy Preserving- Anonymity Authentication (EPPAA) for protecting the user's personal information. Further, the model incorporates the effectiveness of Quantum- behaved Particle Swarm Optimization (QPSO) for selecting the node at middle of neighbours that are closer to the Serving Base Station (seBS). The ticket based anonymity authentication has been employed and the algorithm has been designed and implemented predominantly. For providing confidentiality over the communication, the query message is encrypted, by that way; the anonymous users could not claim the private data of the mobile users. Moreover, the proposed model is implemented and evaluated using the NS2 simulator. The experimentation has been analyzed with the parameters such communication overhead, authentication delay, success ratio, packet delay and compared with some existing privacy preserving models such as Kerberos based Authentication for Inter-domain Roaming (KAIR), Privacy Preserving Nearest Neighbor Queries(PPNNQ) and Efficient Mobile Authentication Scheme (EMAS). The results of the proposed EPPAA show that the model outperforms the traditional methodologies and provides better authentication and security to the user information on WMN.

Keywords: Wireless mobile networks (WMN), Enhanced privacy preserving – anonymity authentication (EPPAA), Quantum particle swarm optimization (QPSO), Authentication, Data privacy.

1. Introduction

In present decade, due to the increasing needs of wireless technologies and developments, there is a dramatic growth in mobile services for providing an expedient life to the people [1]. Due to this express technological growth of mobile usage; wireless network communication has been playing significant parts in many promising applications that includes social mobile networks, Internet of Things (IoT), etc. For an instance, IoT applications converse to collaboratively perceive the active world and provide appropriate responses. Moreover, social mobile networks stimulate the requirement of mobile devices like smart phones to communicate openly in an ad-hoc model to distribute distinctive information like text messages, images and video clips. The following Fig. 1 portrays the general framework of Wireless Mobile Network (WMN) and its components. The distributed mobile devices shares or communicates with others by connecting with the network infrastructure through the Base Station (BS).

In wireless mobile communications, the major issue is the vulnerability of distinctive attacks like eaves dropping, man-in-the-middle, identity spoofing, etc. The main target of such attacks are concerned to be the personal data or some other

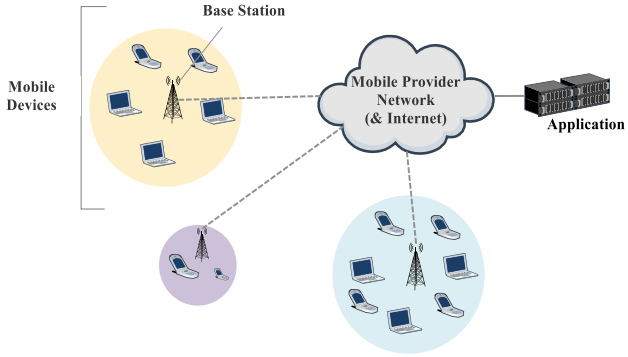

Figure. 1 General framework of WMN

sensitive information of end users like personal health information that are shared between mobile devices or the services of Internet of Things. Therefore, providing authentication and security over the networking is a critical part to be attained efficiently. In an untrusted wireless medium, it is required for the participated nodes to share the symmetric secret key for securing the data from unauthenticated users. This enables a secure communication between the devices. Hence, authentication is very much needed when discussing about developing a secure channel over the network.

Furthermore, whenever mobile services are concerned, securing and authenticating the usage and data is an important criterion to be followed. The features of security include the four major aspects called, Authentication, Integrity, Confidentiality and Availability [2].

Typically, authentication [3] is the process of providing authorized usage over the mobile networks that also paves a way for anonymity aware protection. It also defines the capability of the model to discriminate the authorized or unauthorized customer of certain networks. Integrity is a vital feature to be considered for avoiding the modification of transmitted data on throughout communication [4]. It is responsible for maintaining data accuracy and reliability throughout the communication over the network. Availability ensures that the network with its data is capable to access from everywhere without time limit, when it is accessed by the authenticated people [5]. Another significant feature of WMN in security is confidentiality, which is stated as the secrecy preserving process on shared data between devices. It prevents the network from unwanted disclosure of data to a user.

In particular, there are several anonymity authentication methodologies have been developed to attain secure authentication in WMN. Based on [6], anonymity authentication can be achieved on the basis of two categories:

1. Weak User based Anonymity Authentication
2. Strong User based Anonymity Authentication

The first class involves in hiding user identity only from the unknown third parties (for example: details of neighbour mobile phones). The next category involves in hiding user identity from third parties as well as the foreign servers (i.e. from the network service providers that present in foreign domains).

Generally, in a wireless medium of communication, the information or data of the user is shared between the authenticated customers or end users. But, in some cases, because of the broadcasting criteria of WMN, the shared information is open to some malicious attacks and threats. In order to protect the user data, there is a wide requirement of security protocols or models based on the aforementioned security features. With that node, this paper work aims to develop a model for privacy preserving anonymity authentication to protect the user data and provides reliability over communication.

Moreover, the model adopted an efficient algorithm called Quantum-behaved Particle Swarm Optimization (QPSO). The main reason to incorporate QPSO in this model is to determine the weighted nodes of previous and the global best particles of the network for finding the efficient central node amongst the neighbours [7]. In that, the quantum model is used to illustrate the particle state. Moreover, in QPSO model, the individual nodes are pointed in the quantum space as particles, which are constantly iterated based on the characteristics of the network such as robustness, self-organization, etc. Because of these advancements in QPSO, it is employed here for achieving security over WMN.

Moreover, in the proposed model, ticket based authentication is employed for preserving the privacy of users. Here, ticket is considered as a piece of information that represents the users is permitted with certain protocols. It comprises all the required user data for the mobile service provider to resolve whether it should provide the access or not. It is the most appealing process of mobility based communication networks, wherein the users are continuously roaming and need to contact with foreign server domains. Using ticket based authentication, the communication overhead of the overall process is considerably reduced and the verification of known attacks is fasten to process. Hence, by comparing the conventional network environments, the security design and framing efficient authentication model in WMN is a great challenge. On focussing that, the paper effectively

involves in developing an Enhanced Privacy Preserving – Anonymity Authentication Model (EPPAA) that includes the traditional QPSO for secure communication over WMN.

The remainder of this paper is organized as follows: Section 2 depicts the problem statement in short. Section 3 deliberates the related works based on Security related issues and authentication techniques in WMN. Section 4 presents the operations involved in the proposed EPPAA model. The simulation results and discussions with performance comparison are given in the section 5 and finally, section 6 concludes the work with some key points for future enhancement.

2. Problem statement

The problem is defined specifically designing a model for protecting the privacy of end users in WMN by conserving the user data from unauthenticated third parties. Whenever, the user entity made a registration through the IMSI to authorize them to the network, there is a change of occurrence of man in the middle or some tracking attacks. So, it is significant to maintain confidentiality of the data that is shared between the sender device and the receiver. The data privacy should be ensured throughout the communication over WMN.

Additionally, the process combines the QPSO process for selecting the efficient centre node for securing and the ticket based authentication for providing authorized access on the privacy data of users. The model is named as Enhanced Privacy Preserving – Anonymity Authentication model (EPPAA) and evaluated based on various factor for evidencing its efficacy on providing trusted communicating over the untrusted wireless channel.

3. Related works

The significance of privacy preserving in User Entity (UE) in WMN attracts the scholars working towards the solution of its problem [8]. The strategies of anonymity authentication and privacy models are categorised into three major classes: IMSI (International Mobile Subscriber Entity) Encryption, Utilizing dynamic identity and Pseudonymes based security. For IMSI encryption, the authors of [9] pointed out the IMSI capturing as a security issue on telecommunication authentication protocol. Hence, SPAKA protocol has been framed for encrypting the IMSI during the communication process on the basis of public key cryptography. Nevertheless, there exist a privacy issue on the connect ability between the identity of transmitted entities.

Another work based on location privacy and anonymity of mobile node for heterogeneous networks has proposed in [10]. Further, the authors have considered the conservation of location privacy of a roaming device as a problem included the flawless roaming through the distributed networks. Hence, anonymity based home building update model for wireless mobile and IPv6 networking has been introduced. By this, mutual authentication between nodes has been achieved and a symmetric key has been shared between the anonymous user and the mobile entities over the networks.

Moreover, in [11] an IP based framework for handling several issues like multi homing, roaming and location privacy for 4G networks has been designed. So that, a proxy protocol has been employed as a variation of the conventional mobile IPv6 networking protocol. Those protocols permit home entity to entrust an opportunity to other for authorization instead of the home entity. The virtual identity has been used for attaining the location privacy of mobile devices. It created some issues on impersonating attacks to handle the authorization of delegates. In [12], the authors have suggested a model that embeds the identity user data of the device into the features of signals transmitted for carrying the paging process. But, the model needs some alteration of signal identification at the physical layer, which is not actually required by the whole network.

Furthermore, the authors deigned a Kerberos protocol and afford inter- domain authentication, which is specified as Kerberos based Authentication for Inter-domain Roaming (KAIR) [13]. Kerberos based authenticity has been developed based on tickets for accurate mutual authentication with the employment of session key management. It also aims on providing tickets in such a way that the mobile station can be reachable for the roaming partners of the home network as well as the former visited networks. The authors concluded the work with the portrayal that the process does not entail in the enforcement of authorization for access control and integrity for data protection. Due to the untrusted entities over Internet, W-AKA model has been proposed in [14] for Wi-Fi based Authentication and Key Agreement (AKA). It provided a dynamic identity model for providing privacy on UEs based on some conventional IMSI process. Conversely, in this model, the Home Subscriber Server (HSS) ports are needed to contact the authentication periodically, which leads to a huge network overhead. And, the model failed to

achieve the backward secrecy. Hence, additionally, identity based cryptography is used for developing a model for privacy enforced mutual authentication [15]. In order to avoid the used entity from tracing attacks, the authors have used public key encryption to produce the encrypted IMSI that makes the identity non-traceable. But, the scheme considerably increases the messages needed for authentication performance, thereby, bandwidth consumption also gets increased on the network.

In [16] another model has been developed based on Privacy Preserving Nearest Neighbour Queries (PPNNQ). On focussing the characteristics of cellular networks, the location of the user is hided on the cloaking BS that is responsible for the network connectivity. And, a central node is determined from a group of temporary location neighbours. But, the paper have not discussed about the privacy preserving of user data and integrity.

Further, in [17], the authors have analyzed about the specifications for attaining better location privacy for handling the issues such as communication complexity, cost effectiveness, revocation and effective communication. So that, an identity based sign encryption has been developed for privacy preserving and computational complexities have been managed with bilinear pairings. Efficient Mobile Authentication Scheme (EMAS) is provided in [18] that uses Elliptic Key Cryptography (ECC) based authentication.

HSK-AKA [19] is another model proposed for achieving privacy based on IMSI. The model utilizes the network bandwidth since the authentication scheme reaches the home subscriber server. But, the UE is not capable to check the accuracy of the pseudonyms, hence, malicious attacks are still being an issue. Another Pseudonym based authentication protocol has been designed in [20], since the permanent identity causes the device traceable. For reducing the bandwidth consumption, the protocol defines a set of functions, but those are not liable for the LTE network architecture. Another pseudonym based LTE authentication model is given in [21] for securing the used data. Still there is a chance of attackers to be linked between two eternal pseudonym and the entities are traceable. As a result of this analysis, this paper involved in developing a novel privacy preserving model with ticket based authentication.

4. Proposed model

In the proposed Enhanced Privacy Preserving-Anonymity Authentication (EPPAA) model, the mobile services are provided to the user by the network operators that are autonomous from the location oriented applications needed the location data of UE at the application layer. It is apparent to state that the privacy and the location information of the client can be revealed in some cases such as the collusion made between the telecommunication operator and the location SP (Service Provider). On the other side, the SP usually involves in managing the accounts of users in the application layer. According to that, two different IDs are considered for each user: NID (Network ID) and SID (Service ID). The NID is implemented by the network operator and it is responsible for the user activities. Hence, the user requirements of any provision in application layer, it is serviced by the SP based on the information provided by the SID. The service ID has no connection with the client location or the NID.

4.1 Overall work process of EPPAA

Moreover, in WMN, each mobile user can be accessed with several base stations (enBS). The positions of the base stations are static and there are sufficient number of enBS in the surrounding area of a user can be taken as landmarks. The main purpose of enBS in the proposed model is as follows:

- The enBS are omnipresent in WMN and distributed based on the population density and network traffic.
- Though enBS are static and easily detectable by nature, it can be properly selected in such a way that reducing the detection chance by an opponent or adversary.

Further, in order to provide location privacy, the exact location of the user has never been used. Instead, the location of serving BS called seBS is used and involved in choosing appropriate enBS among the anonymous user group of UE environment. And, for preventing the user data from leakage, Ticket based Anonymity Authentication Algorithm. The algorithm involves in selecting the appropriate nodes from anonymity group. The Fig. 2 illustrated the overall low of the proposed EPPAA model.

Through a secure channel, the UE forwards a registration request to the seBS for authorization. Following that, a set of tentative nodes are provided from the neighbours for hiding the exact identity information of user. The best centre node cBS is selected among the best neighbours using the enforcement of QPSO (Quantum-behaved Particle

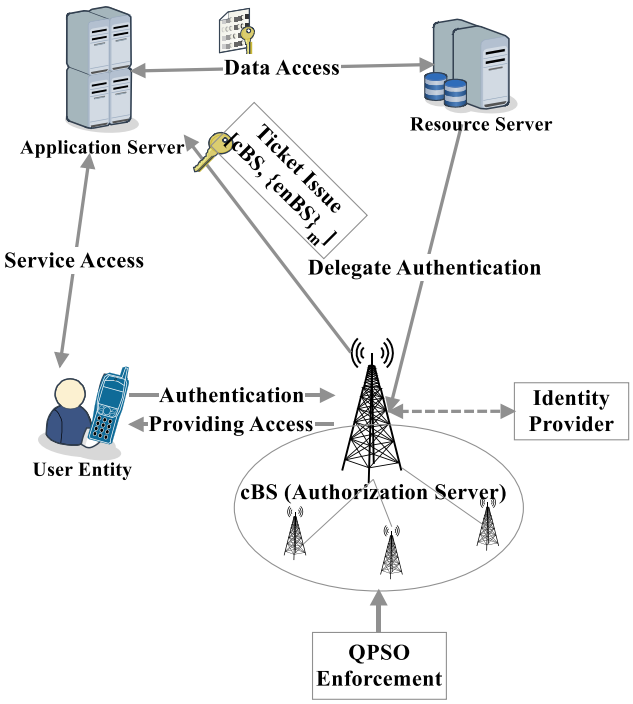

Figure. 2 Overall flow of EPPAA

Swarm Optimization). The fitness function of QPSO is evaluated based on factors such as node degree, distance between nodes and Received Signal Strength (RSS) of the mobile network. With the output of QPSO enforcement, one of the best neighbours of serving BS is chosen as the cBS. Then, the neighbour nodes that are common to seBS and cBS are considered to be the tentative neighbour. And, the seBSs are responsible for tickets issue which contains the cBS and tentative neighbour set $\{enBS\}_m$ for all m=1, 2, ..., n. For enhanced security, the generated ticket is encrypted using a public key.

4.2 QPSO enforcement in EPPAA model

In general, QPSO is derived from typical Particle Swarm Optimization for providing probabilistic optimization solutions. In QPSO, each particle moves around and converges to its local attractor. Moreover, the particles are assumed to acquire quantum behaviour in a state of bound and being attracted by its centre attractor. Hence, a novel stochastic equation for position update is framed. The global best position gBest is enabled for provoking the global searching ability o QPSO algorithm. It is given that the QPSO provides faster convergence performance and greater search capabilities [22, 23].

In QPSO, the particle's quantum state is illustrated by a wave function, since the position and mobility of each particle (here considered as enBSs) cannot be established simultaneously. The wave function of each enBS is given as follows:

$$\phi(w) = \frac{1}{\sqrt{PA}} e^{-|w|/PA} \quad (1)$$

Where 'PA' denotes the probability of particle appearance at the converse point position, stated as, $PA = \frac{1}{\eta}$, where η is the factor of declination with respect to time 't'. Hence, the position o every enBS has been represented using the following demonstration.

$$X_k(t+1) = P_k(t) \pm \frac{PA_k(t)}{2} ln\left(\frac{1}{r}\right) \quad (2)$$

Where, X_k points the position of the k^{th}enBS, 'r' represents the random number between [0, 1], P_k is the local attractor of k^{th}enBS, which is given as,

$$P_k(t) = u.pBest + (1-u).gBest \quad (3)$$

Where 'u' denotes the uniformly distributed random number lies in [0, 1], pBest and gBest point the best position of the particle and the global optimum position of enBS, in that order.
The expression $PA_k(t)$ is derived as follows,

$$PA_k(t) = 2\alpha|mBest_k(t) - X_k(t)| \quad (4)$$

Further, mBest is represented as the mean of $pBest$ values of allenBS, k={1,2,3,.., M}, denotes the number of mBest values. And, the computation is given as,

$$mBest_k(t) = \frac{1}{M}\sum_{k=1}^{M} pBest_k(t) \quad (5)$$

M represents the total number of enBS (particles) and the value of α is evaluated as follows in Eq. (6),

$$\alpha = \frac{(1-0.5).(t_{maxi}-t)}{t_{maxi}} + \frac{1}{2} \quad (6)$$

Where 'α' is an equalizing parameter, t is denotes the total number of iterations. Finally, the position of particles (enBS) can be updated on the basis of the following Eq. (7). The following Fig. 3 illustrates the series of operations and computations involved in QPSO with the proposed EPPAA model.

$$X_k(t+1) = P_k(t) \pm \alpha|X_k(t) - mBest_k(t)|. ln\left(\frac{1}{r}\right) \quad (7)$$

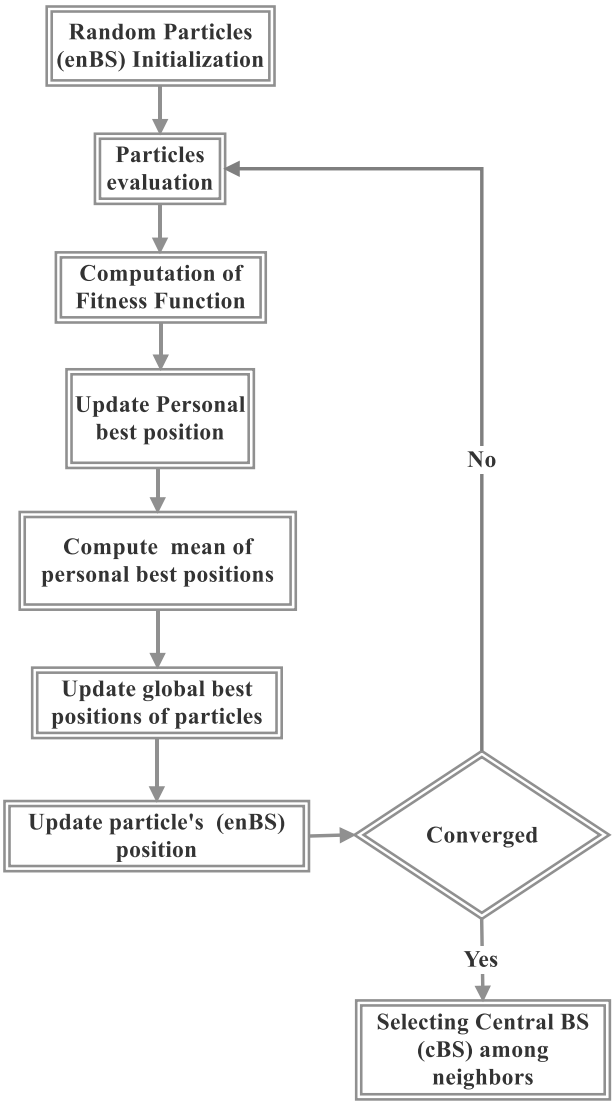

Figure. 3 Operations of QPSO in EPPAA

From the aforementioned computations and the flow, the enforcement of QPSO has been done with EPPAA. Further, based on the final equation given in (7), the position of best neighbours of all enBS has been determined and an effective cBS (center base station) is being selected for user data and location privacy preserving.

4.2.1. Location selection

In the proposed model, it is significant to select proper tentative location to reduce the user data outflow to the service provider. With that concern, the enBSs are classified based on the perception of BS that serves the mobile user, seBS into two classes: 1. Neighbour and 2. Neighbour of neighbour. The Fig. 4 portrays an example scenario, and user is provided with service by enBS-2 (as seBS) and enBS: 3, 4, 5, 6, 7 and 9 are the

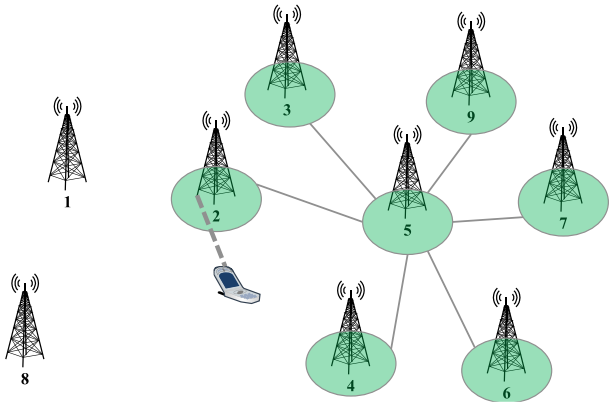

Figure. 4 Selection of seBS by UE and cBS using QPSO with the formation of tentative neighbours and location

neighbours of 1and the remaining are considered under the neighbour of neighbours class. It is also explicit from the figure that the mobile user based on RSS, distance between nodes and node degree. And. cBS is selected among the tentative neighbours and location based on enforcement of QPSO algorithm. Hence, selecting neighbour node from a tentative location that includes seBS is always better. Then, cBS is selection by the procedure explained in (section 4.2).

4.2.2. Selection of cBS

In the perception of service provider, all the neighbours of cBS have equal probability to be as seBS. Moreover, the selected nodes that comprise enBSs from both neighbour and neighbour of neighbour classes. The precision of the model is based on seBS and its belonging neighbours, since the user equipment is surrounded with these. The experimentation shows that the best selection of cBS can be the neighbour of seBS, which contains more common neighbours with seBS or contains greatest signal strength for the user. It further increases the precision rate and affords best environment to the UE.

4.3 Ticket based anonymity authentication algorithm

For achieving the main objective of the work, to conserve the privacy of user data, ticket based anonymity authentication algorithm is employed. After selecting the seBS and cBS using QPSO algorithm, the query message is divided according to the number of tentative neighbours. The message is encrypted with a public key to secure from attackers and malicious nodes. The Ticket based Anonymity Authentication Algorithm employed in EPPAA model is given as follows:

Table 1. Ticket based anonymity authentication algorithm

1. **UE** transmits **REGREQ** to **seBS** through secure channel of communication
2. **seBS** splits the time interval '**t**' as time slots '**TS**' **{TS_1, TS_2,..., TS_n}**
3. **For each**TS_k , k=1,2,..., n
4. **seBS** check its neighbour list **{NenBS}$_k$**
5. **For each** neighbour **NenBS$_j$**∈ {**NenBS**}**k**
6. ***seBS*** evaluates the distance $Dist_{sn}$ ***for all*** **NenBSj**
7. **seBS** evaluates **RSS** for all $NenBS_j$
8. **seBS** estimates node degree **enBS$_{deg}$**
9. **Fitness Function** computation based on **QPSO** as,
$$Fitness = \beta_1 . Dist_{sn} + \beta_2 . RSS + \beta_3 . \text{enBS}_{\text{deg}} \quad (8)$$
Where β_1 , β_2 and β_3 are the normalization parameters that ranges between 1 and 0
10. **Update** particle position based on Eq. (7)
11. **Return** the corresponding **gBest** value
12. **Select** the exact **cBS**
13. **End For**
14. **seBS** selects common neighbour to **cBS**
15. **seBS** generates symmetric key (**Ekey$_{pri}$**) to be shared with user
16. **Ticket Tkt$_m$**is generated by **seBS** as,
$$Tkt_m = \{TS_k, ID\ (cBS, \{enBS\}_m)\} \quad (9)$$
17. **Encrypt**Tkt_m using private key as,
$$Tkt'_m = \{EKey_{pri}(Tkt_m) \parallel val\} \quad (10)$$
18. **seBS** forwards the secured $\boldsymbol{Tkt_m}$ to user
19. **UE** decrypts with shared key and fetches the ticket
20. **UE** splits Query Message (**QM**) into 'k' packets **QM={qm$_1$, qm$_2$, ..., qm$_k$}**
21. **UE** encrypts the **QM$_i$** and forwards to **seBS**
22. **For each** qm
23. **UE** forwards **qm**to**SP** through common neighbours
24. **End For**
25. **SP** collects **qm**, decrypts and forms **QM**
26. **Forward** to **seBS**
27. **UE** gets the **RECRESP** from **seBS**
28. **End for**
29. **Goto**Step 2

Hence, the cBS and the tentative neighbours are selected for each query interval. For next query, another appropriate cBS is selected by seBS through QPSO. Therefore, the attackers are not able to acquire the privacy of the mobile user, since the anonymity settings are dynamically changed at specific time intervals.

5. Simulation results and performance comparison

For providing evidence to the efficiency of the proposed model, the results of EPPAA are compared with the previous models such as KAIR, PPNNQ and EMAS. The comparative analysis has been made with the parameters such as packet drop, authentication delay, authentication success ratio and communication overhead. Further, the performance of the adduced work is evaluated using Network Simulator tool (NS2) with the initial parameter settings as in Table 2.

Table 2. Initial parameter settings

PARAMETERS	INITIAL VALUES
Simulator	NS-2.34
Simulation Time	800 s
No. of cells	18
Simulation End Time	50.0
Mobility Model	Random Waypoint
Topology Size	1000 x1000m
Traffic Model	CBR (Constant Bit Rate)
Propagation Model	Two Ray Ground
Pause Time	0 s
Payload Size	512 bytes
Transmission Range	250 m
Antenna Type	Omni Antenna
Frequency	9 Mhz

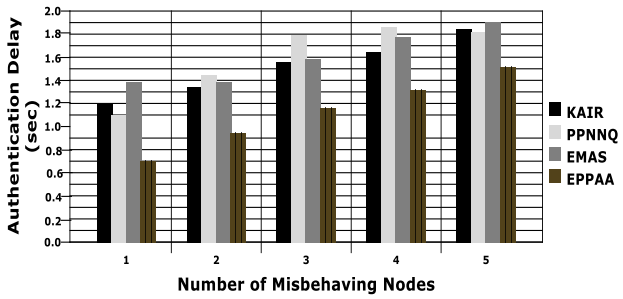

Figure. 5 Number of misbehaving nodes vs. authentication delay

The following graph given in Fig. 5 illustrates the comparison of models evaluated for Authentication Delay achieved for number of misbehaving nodes. It is apparent from the graph that the proposed EPPAA model achieves minimum authentication delay than the compared models. It is also shown in the figure is the authentication delay is directly proportional to the number of misbehaving nodes found in the defined WMN.

As is well known, the significant parameter for analyzing the efficiency of an authentication model is the evaluation of Authentication success ratio. The results of the evaluation are given in the Fig. 6. From the figure, it is obvious that the proposed model achieves better results than KAIR, PPNNQ and EMAS. The EPPAA model obtained 98% (0.98) authentication success ratio, when there occur one misbehaving node, but, it considerably reduced

when there is an increase in misbehaving nodes. Further, the Fig. 7 portrays the comparison chart for packet drop against number of misbehaving nodes. When compared, the proposed model achieves lesser packet drop than others. Typically, the packet drops increase when there is a rise in the findings of misbehaving nodes. The proposed EPPAA model produces maximum 8% of packet drop in the overall analysis. The results given in the figure based on the comparative analysis have shown that the compared models KAIR, PPNNQ and EMAS produces more packet drop than the proposed.

Communication overhead is another important factor to examine the efficiency of the proposed work. For a good authentication mode, the communication overhead should be lower and it is proved from the graph given in the Fig. 8. The computational complexity in the proposed model is low; thereby the communication overhead is low at the initial stage and started increasing when there is a rise in number of misbehaving nodes. But, it is apparent from the graph that the communication overhead evaluated is comparably lower than other models of authentication in WMN, since the ticket is encrypted using shared symmetric key. Hence, it provides a point to state the proposed EPPAA model is more efficient than the compared models.

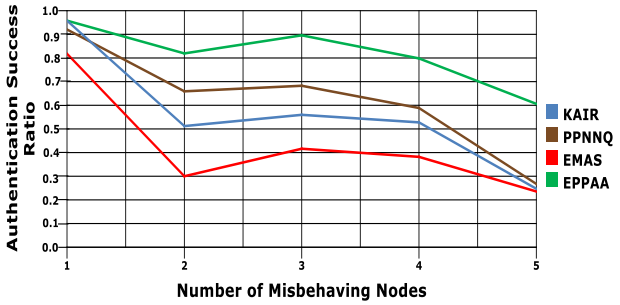

Figure. 6 Comparison for authentication success ratio

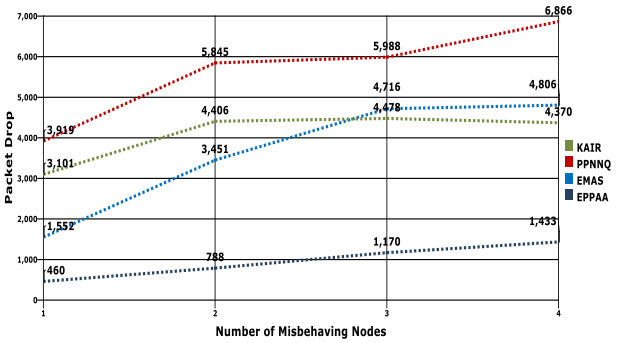

Figure. 7 Comparison of packet drop for varying misbehaving nodes

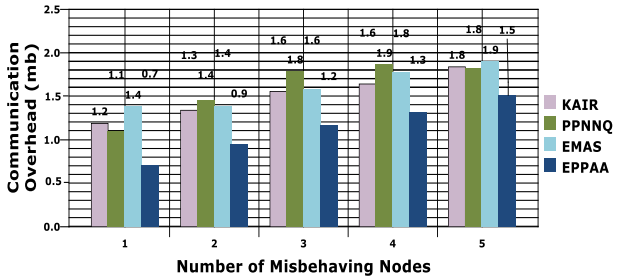

Figure. 8 Communication overhead comparison between models

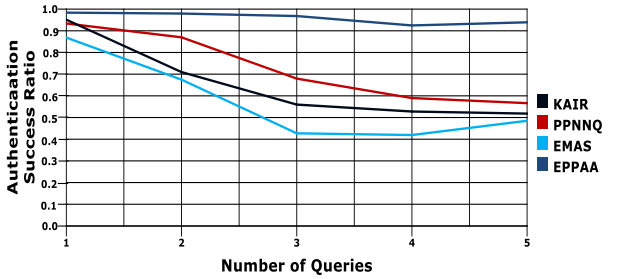

Figure. 9 Authentication success ratio based on queries

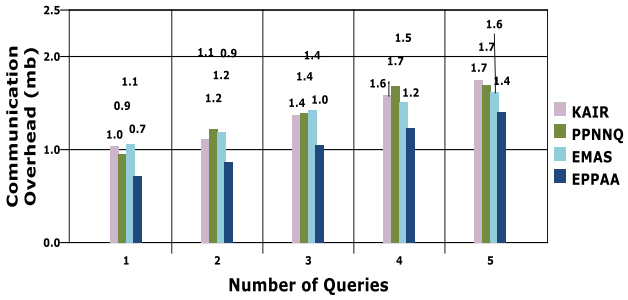

Figure. 10 Communication overhead with respect to queries

The authentication success ratio is also to be evaluated on the basis of input user queries given. Here, the number of cells is varied from 1 to 5. The authentication success ratio of the proposed model is almost at the peak among all compared. And, the evident graph is shown in Fig. 9. From the comparison chart, it is to be stated that the proposed EPPAA model generates authentication success ratio, 24% greater (in average) than the other compared models with respect to queries. Further, in Fig. 10, communication overhead based on queries is depicted. The values show that the communication overhead is completely dependent on number of queries acquired. It increases when there is an increase in input queries. It is also explicit from the figure that the proposed EPPAA model outperforms the results of other models and provides better security for the user data on WMN.

6. Conclusion and future work

In this paper, an Enhanced Privacy Preserving – Anonymity Authentication model has been proposed for protecting the user private data, while communication over WMN. The QPSO model is enforced here for selecting the cBS among the neighbours of seBS. Moreover, the ticket based anonymity authentication algorithm is framed to implement the model effectively. The computations incorporated in the algorithm are used for proving authentication to the UE and to forward the query message in a secure way through the tentative nodes. By this way, the privacy of the UE is preserved and authentication mechanism is employed for WMN. The model is evaluated in NS2 and the obtained results are compared with the existing models such as KAIR, PPNNQ and EMAS. The evaluation has been made with the parameters such as Authentication Success Rate, packet drop and communication overhead with respect to misbehaving nodes and acquired queries. From the analysis, the proposed EPPAA model outperforms others and provided better authentication success ratio and communication overhead with reduced delay and packet drop.

In further developments, the proposed work can be expanded to produce a framework for managing user location privacy in cases of emergencies. Moreover, the work can also be extended by incorporating some other cryptographic functionality for securing.

References

[1] O. Aliu, A. Imran, M. Imran, and B. Evans, "A survey of self organisation in future cellular networks", *IEEE Commun. Surv. Tut.*, Vol. 15, No. 1, pp. 336–361, 2013.

[2] A. Jacques B, D. Jacques, A. Kassem, C. Hakima, and P. Guy, "EPS mutual authentication and crypt-analyzing (SPAKA)", In: *Proc. of 2013 International Conference on Computing, Management and Telecommunications*, pp. 303–308, 2013.

[3] Y. Jiang, C. Lin, X. Shen, and M. Shi, "Mutual authentication and key exchange protocols for roaming services in wireless mobile networks", *IEEE Trans. Wireless Commun.*, Vol. 5, No. 9, pp. 2569–2577, 2006.

[4] X. Lin, "CAT: Building couples to early detect node compromise attack in wireless sensor networks", In: *Proc. of IEEE Global Telecommun. Conf.*, pp. 1–6, 2009.

[5] W. Stalling, "Cryptography and Network Security: Principles and Practices", *3rd ed. Englewood Cliffs*, NJ, USA: Prentice-Hall, Jan. 2010.

[6] G. Yang, Q. Huang, D.S. Wong, and X. Deng, "Universal authentication protocol for anonymous wireless communications", *IEEE Trans. Wireless Commun.*, Vol. 9, No. 1, pp. 168-174, 2010.

[7] J. Sun, B. Feng, and W. B. Xu, "Particle swarm optimization with particles having quantum behavior", In: *Proc. of the IEEE Congress on Evolutionary Computation*, pp. 325–331, 2004.

[8] K. Rechert, K. Meier, B. Greschbach, D. Wehrle, and D. Suchodoletz, "Assessing location privacy in mobile communication networks," In: *Proc. of the 14th International Conference on Information Security*, pp. 309–324, 2011.

[9] A. J. Bou, D. Jacques, A. Kassem, C. Hakima, and P. Guy, "EPS mutual authentication and crypt-analyzing (SPAKA)", In: *Proc. of 2013 International Conference on Computing, Management and Telecommunications*, pp. 303–308, 2013.

[10] T. Sanaa and S. Xuemin, "Anonymous home binding update scheme for mobile IPv6 wireless networking", In: *Proc. of IEEE global Telecommunications Conference*, pp. 1–5, 2011.

[11] S. Chakchai, J. Raj, P. Subharthi, and P. Jianli, "Virtual ID: a technique for mobility, multi-homing, and location privacy in next generation wireless networks", In: *Proc. of the 7th IEEE Consumer Communications and Networking Conference*, pp. 1–5, 2010.

[12] T. Ta and J. S. Baras, "Enhancing privacy in LTE paging system using physical layer identification", *Data Privacy Management and Autonomous Spontaneous Security*, pp. 15–28, 2013.

[13] A. P. Shrestha, D. Choi, G. Kwon, and S. Han, "Kerberos based authentication for inter-domain roaming in wireless heterogeneous network", *Computers and Mathematics with Applications*, Vol. 60, No. 2, pp. 245-255, 2010.

[14] K. Hamandi, I. Sarji, I. H. Elhajj, A. Chehab, and A. Kayssi, "W-AKA: privacy-enhanced LTE-AKA using secured channel over Wi-Fi", In: *Proc. of IEEE International Conference on Wireless Telecommunications Symposium*, pp. 1–6, 2013.

[15] K. Geir, "Privacy enhanced mutual authentication in LTE", In: *Proc. of IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications*, pp. 614–621, 2013.

[16] M. D. Firoozjaei, J. Yu, H. Choi, and H. Kim, "Privacy-preserving nearest neighbor queries using geographical features of cellular networks", *Computer Communications*, Vol. 98, pp.11–19, 2017.

[17] H. J. Jo, J. H. Paik, and D. H. Lee, "Efficient Privacy-Preserving Authentication in Wireless Mobile Networks", *IEEE Transactions on Mobile Computing*, Vol.13, No.7, pp. 1469–1481, 2014.

[18] C. Tang and D. O. Wu, "An Efficient Mobile Authentication Scheme for Wireless Networks", *IEEE Trans. Wirel. Commun.*, Vol. 7, No. 4, pp. 1408–1416, 2008.

[19] K. Hamandi, I. Sarji, A. Chehab, I. H. Elhajj, and A. Kayssi, "Privacy enhanced and computationally efficient HSK-AKA LTE scheme", In: *Proc. of 27th International Conference on Advanced Information Networking and Applications Workshops*, pp. 929–934, 2013.

[20] C. Hiten, R. Basav, and S. Dilip, "Enhancing user identity privacy in LTE", In: *Proc. of the 11th International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 949–57, 2012.

[21] P. Masoumeh and S. Ahmad, "Enhanced authentication and key agreement procedure of next generation evolved mobile networks", In: *Proc. of the 3rd International Conference on Communication Software and Networks*, pp. 557–563, 2011.

[22] W. Wu, X. Wen, H. Xu, L. Yuan, and Q. Meng, "Accurate Range-free Localization Based on Quantum Particle Swarm Optimization in Heterogeneous Wireless Sensor Networks", *KSII Transactions on Internet and Information Systems*, Vol. 12, No. 3, 2018.

[23] J. Sun, W. Fang, X. W. V. Palade, and W. Xu, "Quantum-Behaved Particle Swarm Optimization: Analysis of Individual Particle Behavior and Parameter Selection", *Evolutionary Computation*, Vol. 20, No. 3, pp. 349–393, 2012.