ISSN: 2093-5374 / E-ISSN: 2093-5382

Ticket-Based Schemes for Anonymity and Authentication on Wireless Mobile Networks

J. Jayapradha[1], Dr. Mardeni Roslee[2*], T. Senthil Kumar[3], Dr. Chilakala Sudhamani[4], Azmi Ismail[5], Anwar Faizd Osman[6], Dr. Fatimah Zaharah Ali[7], and Idris Olalekan Adeoye[8]

[1]Assistant Professor, SRM Institute of Science and Technology, SRM Nagar, Kattankulathur, Tamil Nadu, India. jayapraj@srmist.edu.in, https://orcid.org/0000-0002-2548-9135

[2*]Professor, Faculty of Engineering, Multimedia University, Cyberjaya, Malaysia. mardeni.roslee@mmu.edu.my, https://orcid.org/0000-0001-8250-4031

[3]Associate Professor, SRM Institute of Science and Technology, SRM Nagar, Kattankulathur, Tamil Nadu, India; Postdoctoral Research Fellow, Faculty of Engineering, Multimedia University, Cyberjaya, Malaysia. senthilt2@srmist.edu.in, https://orcid.org/0000-0002-2200-3339

[4]Postdoctoral Research Fellow, Faculty of Engineering, Multimedia University, Cyberjaya, Malaysia. sudhamanich@gmail.com, https://orcid.org/0000-0002-8823-9053

[5]Centre of Excellence for Intelligent Network, Telekom Malaysia Research & Development Cyberjaya, Malaysia. azmi@tmrnd.com.my, https://orcid.org/0000-0001-5792-9601

[6]Spectre Solution Sdn Bhd, Malaysia. anwarfaizd@spectresolution.com, https://orcid.org/0000-0001-9563-9138

[7]Universiti Teknologi MARA, Faculty of Electrical Engineering, Shah Alam, Selangor, Malaysia. fatimah_zaharah@uitm.edu.my, https://orcid.org/0000-0002-5467-4049

[8]Centre for Wireless Technology, Faculty of AI & Engineering, Multimedia University Cyberjaya, Malaysia. idreezleks@gmail.com, https://orcid.org/0009-0008-3450-7519

Received: March 27, 2025; Revised: May 09, 2025; Accepted: June 10, 2025; Published: June 30, 2025

Abstract

In wireless mobile networks (WMN), user anonymity and authentication are needed to protect the personal information of the user and the integrity of data, respectively. In this work, a ticket-based anonymity and authentication technique using an optimized algorithm called WMN_TAA-QPSO is developed. In this model, a ticket is employed to convey the query request message from the sender to the location server via a set of dummy senders established around the base station. The QPSO algorithm is also applied to locate a central node out of the neighboring base stations of the serving base station. The encrypted query message maintains security. In this respect, the misbehaving nodes were unable to access the private information of the user. As the problem described above, simulation results also demonstrate that this technique will enhance the Authentication Success Ratio (ASR) and reduce both the Authentication Delay (AD) and Communication Overhead (CO).

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 16, number: 2 (June), pp. 611-628. DOI: *10.58346/JOWUA.2025.I2.037*

*Corresponding author: Professor, Faculty of Engineering, Multimedia University, Cyberjaya, Malaysia.

Keywords: Privacy Preservation, Wireless Communication, Authentication, Anonymity, Fitness Function.

1 Introduction

As the age of great invention increases, wireless mobile networks have become an indispensable facility through which people can easily communicate and access information (Reddy & Mohan, 2024). However, with the advancement of mobile devices, a major concern has been raised in the privacy of the users and the security of data transmitted (Khan et al., 2020). Since users are shifting to mobile networks for more transaction sensitivity, the demand for good anonymities and authenticities is great. The anonymity enables the users to be able to communicate without revealing their identity while the authentication provides a check into the legitimacy of the user and also protects against unauthorized users or impostors. Newer research explains the weaknesses in existing methodologies and the need for advanced approaches to tackle these issues which cannot be fixed through existing solutions (Zhang et al., 2021).

The use of new algorithms, including Quantum Particle Swarm Optimization (QPSO), gives a potential direction for the improvement of WMNs' security. It has been seen that QPSO (Thillaigovindan & Subramaniyan, 2019) which is quite efficient in optimization problems can be effectively used for the selection of the central node in the network for optimized routing of the query messages. To this end, the use of QPSO for improving the WMN's user anonymity and data security, this paper presents a new ticket-based anonymity and authentication mechanism. Using a ticket for transmitting the query request to the chain of dummy senders, the proposed model avoids the leakage of information to the malicious nodes. In addition, for secure queries, prompt messages are encrypted from potential threats, protecting users' messages from leaks.

Simulation results indicate that the proposed technique significantly improves the authentication success ratio while reducing both authentication delay and communication overhead. This advancement not only enhances user experience but also fortifies the overall security framework of WMNs, making it a critical contribution to the field of wireless communications (Yeonjin et al., 2023; Kumar et al., 2023).

It is obvious from Figure 1 that, the Wireless Mobile networks are open to various threats like man-in-the-middle attacks, spoofing, eavesdropping, (Ma & Tsudik, 2010) etc. Additionally, the major motives of such threads are focused on the user's personal information or other sensible data that are transmitted between devices or nodes or applications based on IoT. Hence, it is very important to provide security and authentication over the shared data on WMN, which is a crucial task to be achieved efficiently. For attaining security, efficient cryptographic techniques are incorporated in this work eavesdropping.

The main security threat of WMNs lies in the ability of an attacker to easily interpose himself into the wireless communication link (Booch et al., 2025). WMN attacks can be broadly categorized into two types: passive-form attacks and active-form attacks. In most cases, passive attacks carry the aspect of observation. It covers listening to the network communication and understanding its functions without necessarily influencing or modifying its activities (Jain & Chatterjee, 2024).

Common examples of passive attacks in WMNs include eavesdropping on data traffic to gather sensitive information, traffic analysis to deduce patterns or behaviors, and monitoring network activities to identify vulnerabilities.

The primary objective of passive attacks is to gather information or gain insights into the network's operation without raising suspicion or causing disruption. Active attacks, in contrast, involve exploiting vulnerabilities or actively interfering with network operations. They are more aggressive in nature and can have a direct impact on the network's functionality and security. Active attacks in WMNs include a wide range of bad things, like sending unwanted traffic, changing data packets, stopping network services (for example, denial-of-service attacks), and pretending to be legitimate nodes. The primary aim of active attacks is to compromise the integrity, availability, or confidentiality of the network's resources and services.

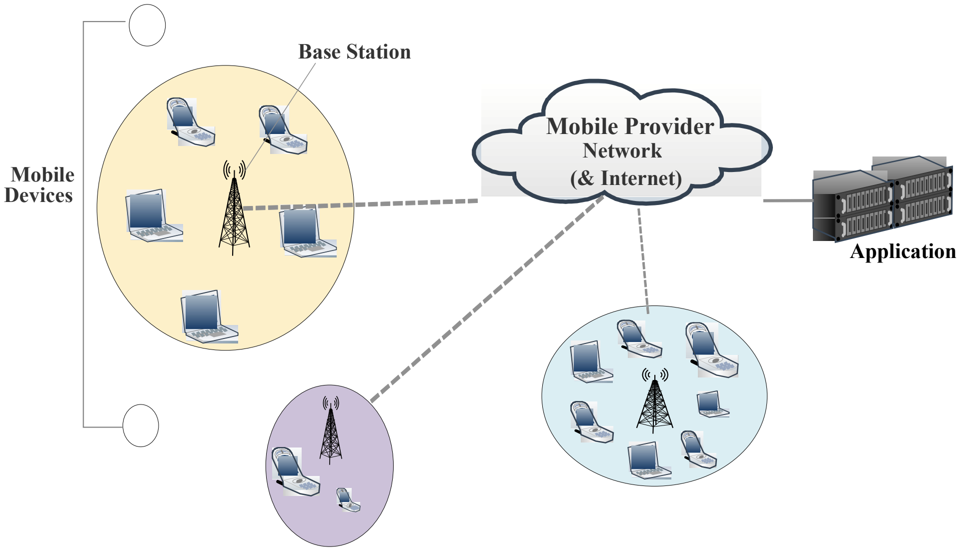

Figure 1: The General Heterogeneous Architecture of WMN

2 Problem Identification

As aforementioned, WMN is vulnerable to several distinctive attacks because of their wireless mode of communication and features (Selvam & Stalin, 2018). Hence, there is a need for a model that works on user anonymity and secure communication for protecting the user's private information by assuring the attackers cannot derive sensible user data. Initially, the End User (EU) uses the IMSI for its authentication.

The main motive of this work is to provide privacy for the sender and communication anonymity. To achieve this, the Ticket-Based Anonymity and Authentication (TAA) technique has been developed. Furthermore, the model combines the efficacy of Quantum-behaved Particle Swarm Optimization (QPSO) for efficient center node selection among the neighbors that are nearer to the Serving Base Station (srBS). TAA makes the communication more confidential; the encrypted query message is sent to the EU.

3 Related Work

The progressive nature of people using Wireless Mobile Networks (WMNs) for communication has made it mandatory to focus on the requirement through the provision of a reliable security protocol for the privacy and protection of user data. Substantial scientific efforts have been targeted at anonymity and authentication schemes specific to WMNs due to the mobility characteristics of the network.

User anonymity is essential for WMNs because it helps protect the user's identity in case of an attack. Different measures have been used in the literature to capture user anonymity. For example, Cha et al. (Cha et al., 2019) proposed a mix-zone-based scheme that involves the use of fake nodes to hide user coordinates and thus increase anonymity. Likewise, Wang et al. (Wang et al., 2020) put forward another hierarchy topology-based anonymous routing protocol with dynamic consideration for the conditions encountered in anonymizing networks to achieve more efficient and reliable communication for the users without compromising their privacy.

Like in the case of the wired networks, the authentication mechanisms are as important in protecting transmitted data in WMNs. More often, conventional approaches to authentication prove inadequate, especially under mobile scenarios, given that most rely on infrastructure with fixed connectivity. In light of this, Liu et al. proposed a lightweight authentication scheme designed to take advantage of the features of mobile devices to reduce the overhead created by the authentication process.

The incorporation of optimization algorithms has been described as a promising approach to improving the effectiveness of anonymity as well as authentication protocols. Due to the fact that Particle Swarm Optimization (PSO) has been proven to solve many optimization problems, this is why Quantum Particle Swarm Optimization (QPSO) has attracted much attention. In WMNs, QPSO has been used to improve routing paths as well as select the central nodes. For instance, Zhang et al. showed that by using QPSO, it was possible to reduce the communication cost whilst ensuring that all the authentication processes gained success rates.

Other published research has also discussed especially the topic of encryption so as to enhance the security of information being disposed of. A study by (Ali et al., 2022) developed an encryption model involving both the symmetric and asymmetric key encryption mechanisms as a suitable security model for protecting query messages in WMNs. This approach does more than secure data privacy; it also prevents the exposure of important data to unauthorized nodes.

In addition, ticket-based systems have been proposed and analyzed to perform safe operations in WMNs. (Kumar et al., 2023) presented yet another model of ticket-based authentication in which temporary tickets are issued to the users in a very critical way in order to minimize the chance of repaying attacks. This model may be said to fit in well with the requirement for security in mobile environments, which will be dynamic in nature.

A literature review has proved the efficiency of each of these proposed techniques through simulation. For example, Chen et al. performed research on anonymity protocol and showed that enhancing the anonymity level of users employing the anonymity protocol proposed by them has a very low impact on communication latency. Similar to the potential benefits of using QPSO pointed out by (Gupta et al., 2022), the research demonstrated the benefits of QPSO optimization in the flow of authentication to enhance the success ratios while at the same time minimizing the delays.

Nevertheless, tasks related to anonymity as well as authentication still pose some problems even at this age. The mobility of WMNs presents challenges that explain why their security features are not static. To emphasize, Sharma et al. noted that the mobility of nodes makes the network vulnerable, which existing protocols may not effectively address. That is why constant research is needed to create effective security strategies that can counter the constantly changing nature of wireless communication. In a comparable manner to works that propose approaches to 5G authentication and enhanced handover for end-to-end connectivity in diverse networks. The goal is to protect user privacy and data integrity. A significant body of research has focused on anonymity and authentication protocols tailored for WMNs, addressing the unique challenges posed by mobile environments.

Security of user identities is of paramount importance, and thus anonymity in WMNs is paramount. Several methods on how user anonymity can be improved have been suggested. For example, Cha et al. (Dhanalakshmi et al., 2015) proposed a mix-zone-based adaptive approach that hides the identity of users by incorporating dummy nodes. Likewise, Wang et al. developed a dynamic anonymous routing scheme that makes routes according to the condition of the network for effective communication without compromising the privacy of the user.

The conceded security threats show that authentication mechanisms are equally important in protecting the integrity of WMN's data transmissions. Historical concepts of authentication are not sufficiently sufficient in mobile environments because of the foundations of these methods. In response to this, (Liu et al., 2021) designed a lightweight authentication that takes advantage of the features of mobile devices to curb the high overhead that goes with most authentications.

The use of optimization algorithms has appeared as one of the most viable approaches to improve anonymity and authentication protocols. It is mainly selected because of its high efficiency in solving complex optimization problems, Quantum Particle Swarm Optimization (QPSO). For WMNs, QPSO has been employed to improve the choice of central nodes and routing paths. For example, (Zhang et al., 2022) provided a use of QPSO, demonstrating how the approach facilitates low communication overhead with a high success rate of the authentications.

Other new research work has also investigated the role of employing encryption capabilities to strengthen the secure communication of transmitted information. A robust and efficient encryption model for securing query messages in WMNs is developed by Ali et al. through the integration of both the symmetric and asymmetric encryption principles. It also proactively improves the security of data by protecting it from fraud and other illegitimate nodes with no right to such data.

Furthermore, the authors have also proposed the alternative of ticket-based systems in order to enable secure communication in WMNs. Kumar et al. proposed a ticket-based authentication model that employs short-lived tickets to enhance security, hence limiting replay attacks continued on page 11. This model fits well in the current and expected deployments of security on mobile platforms since they are or are likely to be ever-changing.

Simulation studies have also supported the identified techniques for the proposed method. For instance, the study done by (Chen et al., 2021) shows how the efficiency of their anonymity protocol enhanced the anonymity level of users and their low latency in communicating. Consistent with the findings made by Gupta et al., the advantages of using QPSO in optimizing the authentication were noted; the time taken to complete the authentication was considerably decreased, and a better success rate was achieved.

Despite the advancements in anonymity and authentication protocols, challenges remain. The dynamic nature of WMNs poses difficulties in maintaining consistent security measures. As highlighted by (Sharma et al., 2023), the mobility of nodes can lead to vulnerabilities that existing protocols may not adequately address. Therefore, ongoing research is essential to develop adaptive security mechanisms that can respond to the evolving landscape of wireless communications.

Similar to works that address 5G authentication and improved handover algorithms for seamless connectivity in heterogeneous networks. It might also include elements of how to use RF energy efficiently and rectify it, as shown in the hybrid energy harvesting research (Roy et al., 2021; (Khan et al., 2021; Sadeque et al., 2019; Dwiputriane & Heng, 2022; Iqbal et al., 2020). These approaches endeavour to call for confident, secure, and reliable communications and authentication in improved wireless networks.

Accordingly, this literature shows an increasing concern about anonymity and authentication issues in WMNs. The use of optimization algorithms in conjunction with encryption techniques coupled with a ticket-based system in the ticket system provides a rich layered approach to security. Further work has to be focused on improving the idea and investigating new strategies to overcome the limitations of mobile platforms, avoiding privacy issues for users.

4 Ticket-Based Anonymity and Authentication Using QPSO (TAA-QPSO)

In this work, a ticket-based anonymity and authentication technique is proposed for WMN. The steps involved in TAA-QPSO are as follows in Figure 2:

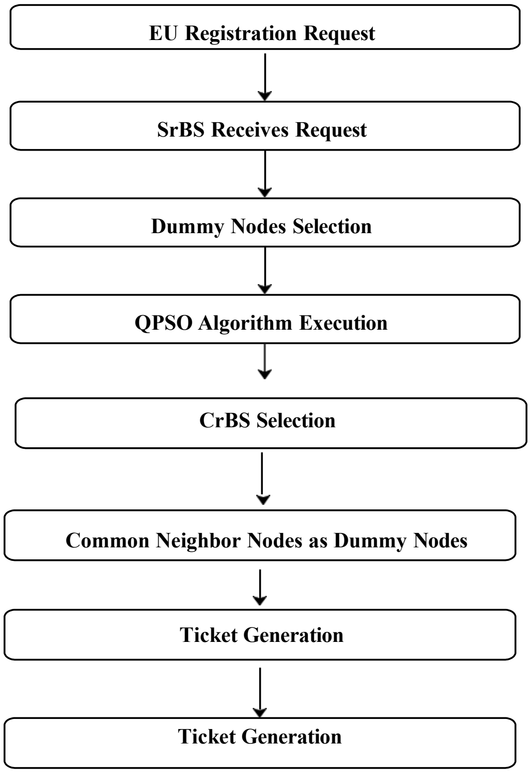

Figure 2: Flow of TAA-QPSO

- The End User (EU) is the party that is responsible for initiating and sending a registration request through a secure tunnel to the Serving Base Station (SrBS).
- Since SrBS supplies a set of fake nodes, it guarantees that the identification of its neighbors is concealed, which makes it impossible to determine the identity of the EU.
- To select the center node (CrBS) from among the neighborhood of the SrBS structure, the process known as Quantum Particle Swarm Optimization (QPSO) is used.
- For constructing the fitness function of the QPSO algorithm, deployed parameters are distance to the node, the degree of the node, and received signal strength (RSS).
- Based on the selection, the output of the QPSO technique is used to choose one of the neighbors of SrBS to act as the CrBS. This selection is based on the selection result.

- A set of neighbors that is assumed that both SrBS and CrBS have in their selection is defined as dummy nodes of the network.
- The production of a ticket that contains CrBS and its dummy neighbors {NeBS}k for the time slot TLk is the responsibility of SrBS. This is true for all k values that range from 1 to n.
- In the eighth step of the registration procedure, the ticket is encrypted before being sent back to the End User (EU) in order to complete the process.

4.1 Role of QPSO In TAA

The technique of particle swarm optimization (PSO) is becoming popular since it can yield better results for optimization problems with limited time complexity and cheaper cost. In order to improve the performance of the PSO algorithm, a number of its variants have been proposed (Khan et al., 2020). Quantum-behaved particle swarm optimization (QPSO) is a probabilistic optimization solution that is modified from PSO and originated from quantum mechanics. Each particle in QPSO swings around and converges to its local attractor. In QPSO, the particle is assumed to possess quantum behavior in a bound state and to be attracted by a centered local attractor. Hence, it has a new stochastic position update equation. A global best position was used in the algorithm to enhance the global search ability of the QPSO algorithm. QPSO shows fast convergence performance and stronger global search capability (Zhang et al., 2020; Ali et al., 2022).

In the QPSO algorithm, since the velocity and position of each particle cannot be determined together, the quantum state of the particle is represented by a wave function.

$$\phi(Y) = \frac{1}{\sqrt{L}} e^{-|Y|/L} \tag{1}$$

Where L is the probability of the particle at the opposite point position, given by

$$\mathrm{L} = \frac{1}{\beta} \tag{2}$$

where β is the shrinkage factor varying with time *t*.

Thus the position of each particle can be represented using the Monte Carlo method as

$$\mathrm{X_i(t+1)} = P_i(t) \pm \frac{L_i(t)}{2} \ln\left(\frac{1}{u}\right) \tag{3}$$

Where,

X_i denotes the position of the i^{th} particle.

u is a random number in the range of [0,1].

P_i is the local attractor of the i^{th} particle given by

$$\mathrm{P_i(t)} = a.pbest + (1-a).gbest \tag{4}$$

Where a is a uniformly distributed random number in the range of [0,1], pbest and gbest represent the personal best position and global optimum position of the particles, respectively.

And $L_i(t)$ can be derived from the following equation.

$$\mathrm{L_i(t)} = 2\alpha \left| mbest_i(t) - X_i(t) \right| \tag{5}$$

Here

$$\text{mbest}_i(t) = \frac{1}{M}\sum_{i=1}^{M} pbest(t) \tag{6}$$

Where α is parameter, t is the number of iterations, and mbest is the average of pbest positions of all particles.

$$X_i(t+1) = P_i(t) \pm \alpha \left| X_i(t) - mbest_i(t) \right| . \ln\left(\frac{1}{u}\right) \tag{7}$$

Where

$$\alpha = \frac{(1-0.5).(t_{\max} - t)}{t_{\max}} + 0.5 \tag{8}$$

The steps involved in the process are summarized in the QPSO algorithm:

1 Initialize the particle's current positions and their pbest positions

2 For each iteration j

3 Evaluate the fitness function F

4 Compute the pbest and gbest positions of the particle

5 Update the position of each particle

6 Terminate when the condition is not met

7 Stop

4.2 Query Request/Response Using Ticket-Based Anonymity

In order to safeguard the privacy of the EU and the receiver, anonymity is maintained using the ticket-based technique. The SrBS selects CrBS from its neighbors using the QPSO algorithm. The EU splits the query message based on the number of dummy neighbors. The encrypted message is thus secure from malicious nodes. The Notations used with meaning are depicted in Table 1 and the steps involved in the process are described in the following Algorithm 1.

Table 1: List of Notations and Meaning

Notations	**Meaning**
EU	End User
$T_{c,t}$	Ticket
D_{SN}	distance between a node and SrBS
N_{degree}	Degree of the Node
Ne	Neighbouring node
RSS	Received Signal Strength
FF	Fitness Function
SrBS	Serving Base station
CrBS	Center Base station
TL	Time interval
NeNB	List of Neighbouring node
RSS	Received Signal Strength
M_{QR}	Query Request Message
$s_{c,l}$	random seed

c	node
l	cluster level
$K_{c,t,l}$	symmetric key
t	time interval
a_1, a_2, and a_3	Numerical constants in the range of {0,1}

Algorithm 1: Ticket-based Anonymity using QPSO

```
1. EU transmits a registration request to SrBS through a secure tunnel.
2. SrBS splits the time interval t into slots $\{TL_1, TL_2,...TL_n\}$
3. For each $TL_t$, k=1,2...n,
4. SrBS looks up its neighborlist list {NeNB}
5. For each neighbor $Ne_j \in$ NeNB
6.         SrBS estimates the distance $D_{SN}$ to $Ne_j$.
7.         SrBS estimates RSS of $Ne_j$
8.         SrBS estimates the node degree $N_{degree}$ of $Ne_j$
9.         SrBS generates the fitness function FF as
                 $FF = \alpha_1 RSS + \alpha_2 N_{degree} + \alpha_3 D_{SN}$          (8)
           Where $\alpha_1$, $\alpha_2$ and $\alpha_3$ are numerical constants in the range of [0,1]
10.        Update the position of each particle using Eq. (6)
11.        Return the position of the particle corresponding to gbest value
12.       Select the neigbor $Ne_j$ as CrBS.
12. End For
13.  SrBS selects the common neighbour to CrBS $\{DNB_1, DNB_2...DNB_k\}$ as dummy set of neighbours.
14. SrBS creates the symmetric key $K_{pri}$ shared with EU
15. SrBS generates the ticket $T_{c,t}$ based on the following equation:
                 $T_{c,t} = \{TL_{k,} Id(CeNB), DNB_j\}$          (9)
16. SrBS encrypts $T_{c,t}$ as
                 $T^1_{c,t(i)} = \{E_{k_{pri}}(T_{c,t})||Val\}$          (10)
17. SrBS send the ecnrypted $T^1_{c,t}$ to EU
18. On receiving $T^1_{c,t}$, EU decrypts it with $K_{pri}$.and fetches the ticket.
19. EU splits the query message $M_{QR}$ into t packets i.e., $\{m_1, m_2,.....m_k\}$.
20. EU encrypts each $m_i$ using $K_{pri}$ as given below
                 $m^1_i = \{E_{k_{pri}}(m_i)||Val\}$
21. EU transmits $m_1^1$ to the server S through SrBS
22. For each $m_j^1$, j=2,3...t
22. EU transmits $m_j^1$ to the server S through $DNB_j$
23. End For
24. S collects all $m_j^1$ and groups all packets corresponding to the same $M_{QR}$.
25. S reconstructs $M_{QR}^1$ and decrypts using its $K_{pri.}$ to retrieve $M_{QR}$ .
```

26. S sent the response to query M_{QR} to EU through SrBS and DNBj
27. EU receives the response from SrBS
28. The same steps are repeated for the next interval

Thus, the CrBS and its dummy neighbors are selected for each query interval. During the next query, another suitable CrBS is selected by the SrBS. Since the anonymity set changes dynamically at each time interval, any attacker is unable to track the location of CrBS.

5 Results and Discussion

5.1 Simulation Parameters

The proposed ticket-based anonymity and authentication technique using QPSO (TAA-QPSO) is simulated in NS2 and the performance is compared with the privacy-preserving nearest neighbor queries (PPNNQ) technique (Mishra & Kumar, 2021). The simulation parameters and simulation topology are as follows and in Figure 3, respectively.

➢ Total Cells	: 18
➢ Number of Users per cell	: 6
➢ Number of SPs	: 6
➢ Topology Size	: 1000 X 1000m
➢ Traffic Model	: Constant Bit Rate (CBR)
➢ Propagation model	: Two Ray Ground
➢ Antenna model	: Omni Antenna

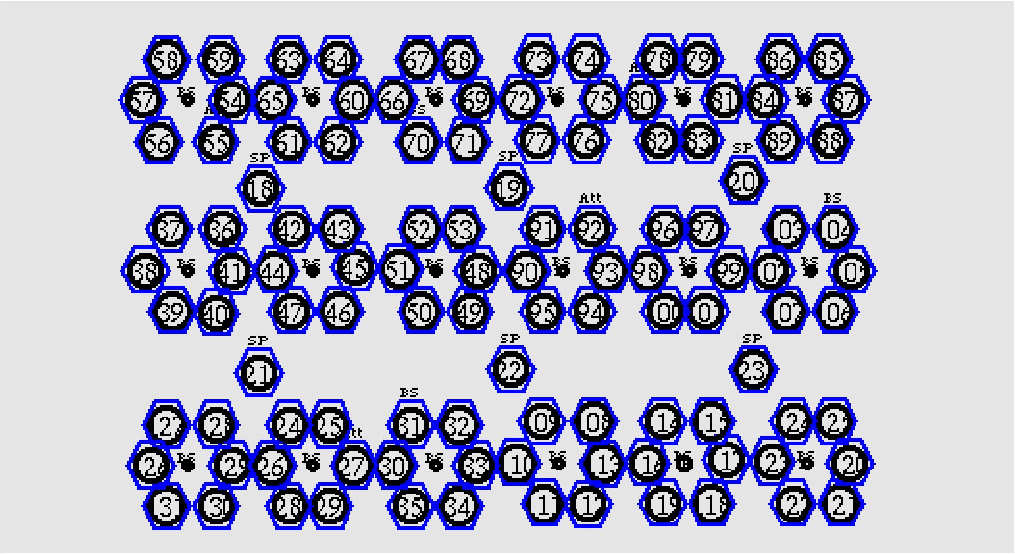

Figure 3: Simulation Topology

5.2 Results & Analysis

5.2.1. Effect of Misbehaving Nodes Across the Cells

Initially, the number of misbehaving nodes per cell varied from 1 to 5.

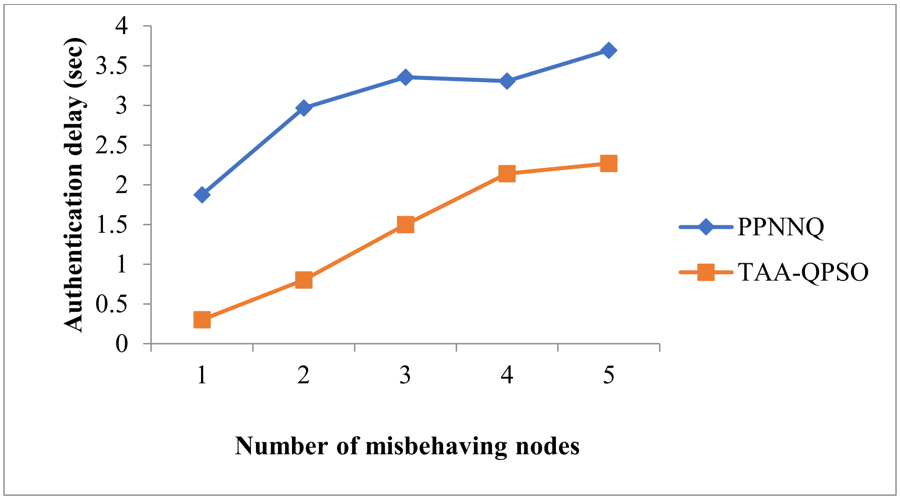

Figure 4: Authentication Delay for Various Misbehaving Nodes

Figure 4 illustrates the authentication delay for TAA-QPSO and PPNNQ when the number of misbehaving nodes is changed. The delay of both systems exhibits a positive correlation with the number of misbehaving nodes. The authentication latency of TAA-QPSO is 55% lower than PPNNQ due to the utilization of a shared symmetric key for ticket creation. As the quantity of malfunctioning nodes per cell rises from 1 to 5, both TAA-QPSO and PPNNQ encounter a rise in authentication delay. Consequently, as additional nodes in the network exhibit malicious or uncooperative behavior, the duration required to validate communication requests likewise escalates. Nevertheless, TAA-QPSO routinely surpasses PPNNQ in terms of authentication delay, and this superiority can be attributed to the utilization of a shared symmetric key for ticket production in TAA-QPSO.

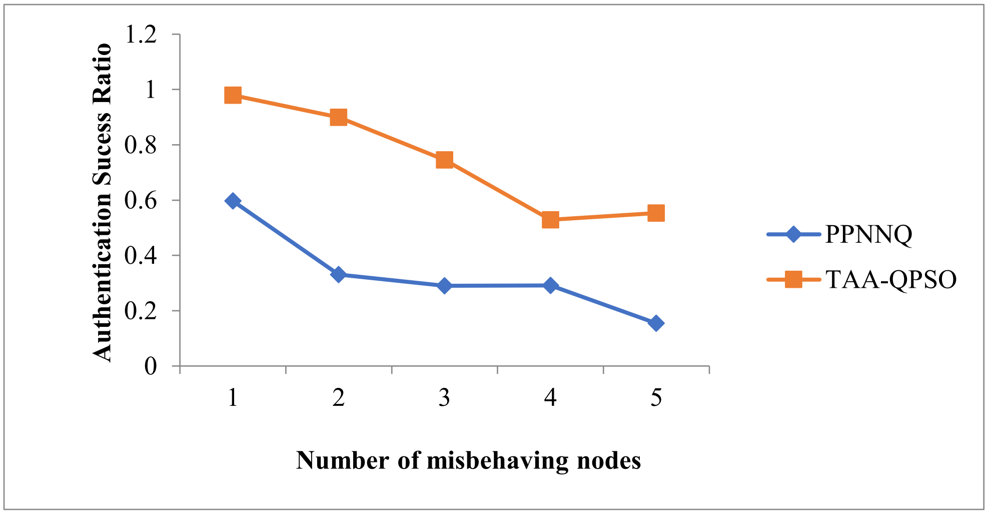

Figure 5: Authentication success ratio for various misbehaving nodes

Figure 5 displays the authentication success ratio of PPNNQ and TAA-QPSO. As the number of malfunctioning nodes increases, the success rate of both systems diminishes. The query message is divided and distributed randomly among the dummy nodes. The authentication success rate of TAA-PSQ is 56% more than that of PPNQ. The vertical axis of Figure 4 most likely indicates the authentication success rate, which is measured as a percentage. This ratio quantifies the effectiveness of the authentication procedure in confirming valid communication requests in the presence of malicious nodes inside the network. As the number of nodes exhibiting improper behavior rises, both PPNNQ and TAA-QPSO encounter a decline in their ratio of successful authentication. These findings indicate that the existence of malfunctioning nodes has a detrimental effect on the successful authentication of communication requests in both systems. The distribution strategy employed in TAA-QPSO is likely a significant factor in its elevated authentication success ratio. It can improve the robustness of the authentication process, making it harder for malicious nodes to interfere with or undermine it.

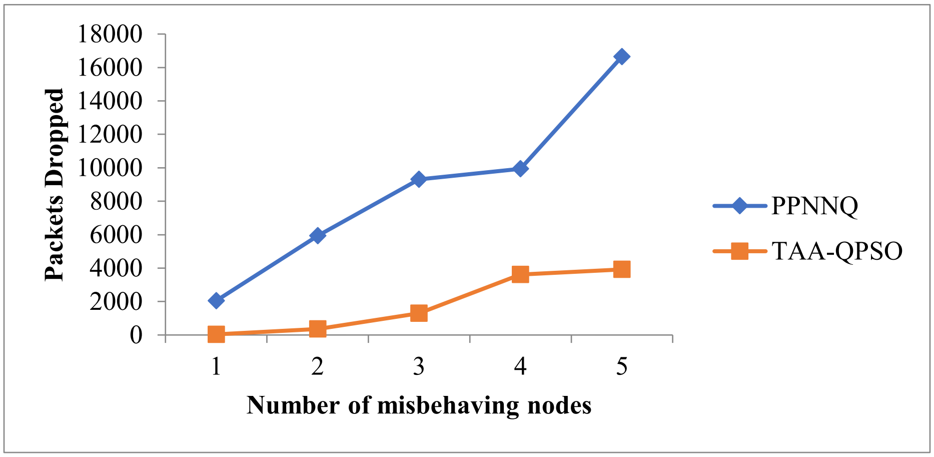

Figure 6: Packets Dropped for various misbehaving nodes

The analysis of packet drop for the PPNNQ and TAA-QPSO systems is depicted in Figure 6. As the number of awkward nodes grows, the packet drop rates in both systems are higher as well. From this, it can be argued that the availability of faulty nodes within a network implies that packets being transmitted within the network have a high chance of being dropped or even disappearing. The results obtained here prove that TAA-QPSO outperforms the others in handling misbehaving nodes, resulting in an 83% reduction in packet drops as compared to that of PPNNQ. Therefore, TAA-QPSO has a significantly lower packet drop rate, especially where there are nodes with improper behaviour, making the use of the protocol as a finite strategy for the delivery of packets more reliable. A lower packet drop rate demonstrated by TAA-QPSO analysis shows that the proposed work has the ability to avoid or reduce the impact of the faulty nodes on the network. All of these goals can be achieved by employing several techniques, some of which are better routing algorithms, better packet handling, or introducing security measures that curb unsavoury behaviour of nodes during the transmission of packets of data.

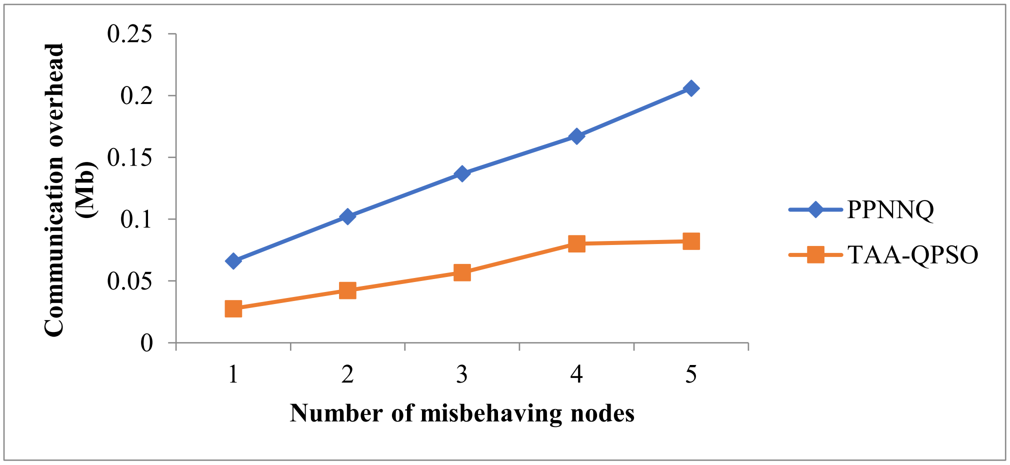

Figure 7: Communication Overhead for Various Misbehaving Nodes

The communication overhead of the PPNNQ and TAA-QPSO methods is shown in Fig. 7. The figure shows the communication overhead that represents additional resources, messages, or data provided to support the delivery of communication content. This refers to the control messages and the routing information as well as the extra data used for supervisory operations in the course of the communication process. The communication overhead of both PPNNQ and TAA-QPSO increases as the number of malfunctioning nodes increases in the network. Based on these findings, it can be concluded that malfunctioning nodes require more communication resources and data for the management and protection of the communication line. To deliver the message packets, TAA-QPSO employs a fewer number of nodes than the proposed multi-hop paths. This may well be another reason for the decrease in the amount of contact between the parties. TAA-QPSO can also reduce the communication overhead where a few numbers of nodes are involved, and TAA-QPSO may use superior methods of routing or data management.

5.2.2. Effect Of the Number of Query Requests Per Cell

Next, the number of query request messages per cell is varied from 1 to 5.

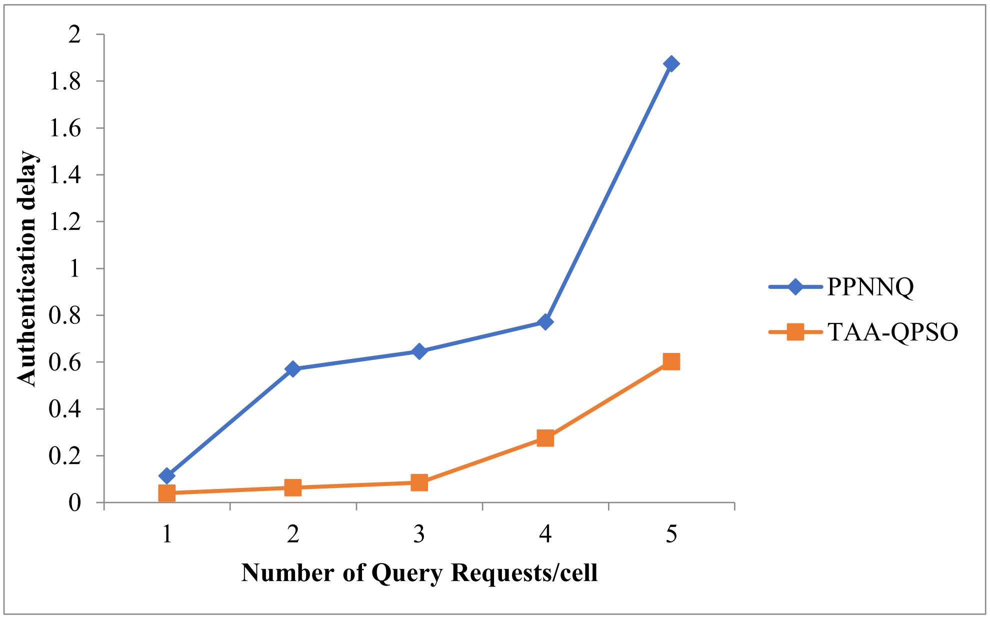

Figure 8: Authentication Delay for varying query requests

A comparison of the authentication latency for the PPNNQ and TAA-QPSO systems is presented in Figure 8. Any increase in the number of requests will result in an increase in the latency for both of the schemes. In comparison to the PPNNQ scheme, the TAA-QPSO scheme's utilization of a shared symmetric key has a considerable impact on the reduction of the amount of time an authentication process takes. When opposed to more complicated approaches such as public-key cryptography, which is frequently utilized in asymmetric key-based systems, a shared symmetric key is typically more efficient when it comes to authentication needs. Due to the fact that a shared symmetric key is utilized in the process of ticket creation, the authentication delay of TAA-QPSO is 82% smaller than that of PPNNQ.

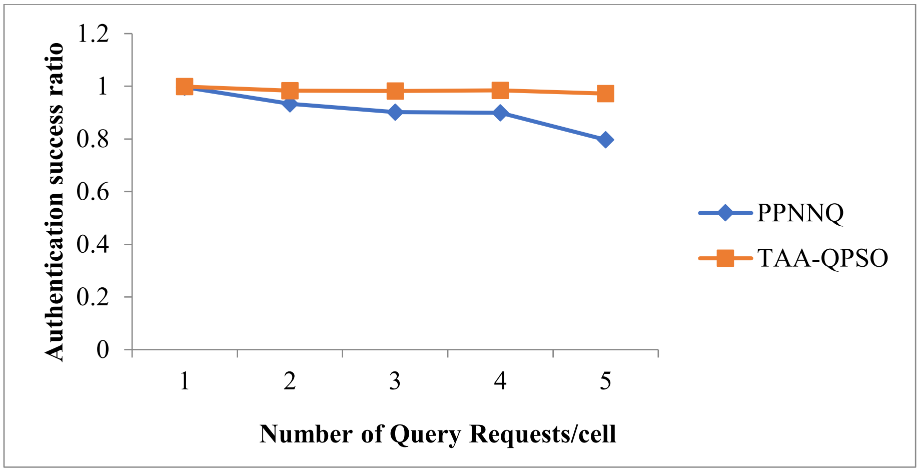

Figure 9: Authentication Success Ratio for varying query requests

Figure 9 illustrates the percentage of successful authentication attempts made by PPNNQ and TAA-QPSO. There is a minor decline in the success ratio of both of the methods when the requests are varied significantly. This improvement can be due to how query messages are split and randomly dispersed across dummy nodes, which is the reason why the success ratio of TAA-QPSO is 18% higher than that of PPNNQ. The fact that this is the case suggests that the design or strategy of TAA-QPSO, which involves splitting and distributing query messages in a certain manner, results in a greater success ratio when compared to the PPNNQ scheme. When it comes to effectively authenticating requests under these circumstances, a higher success ratio indicates that TAA-QPSO is more effective than other procedures. The success ratio of TAA-QPSO is 18% higher than that of PPNNQ. This is because the query message is split across the dummy nodes and then randomly dispersed between them.

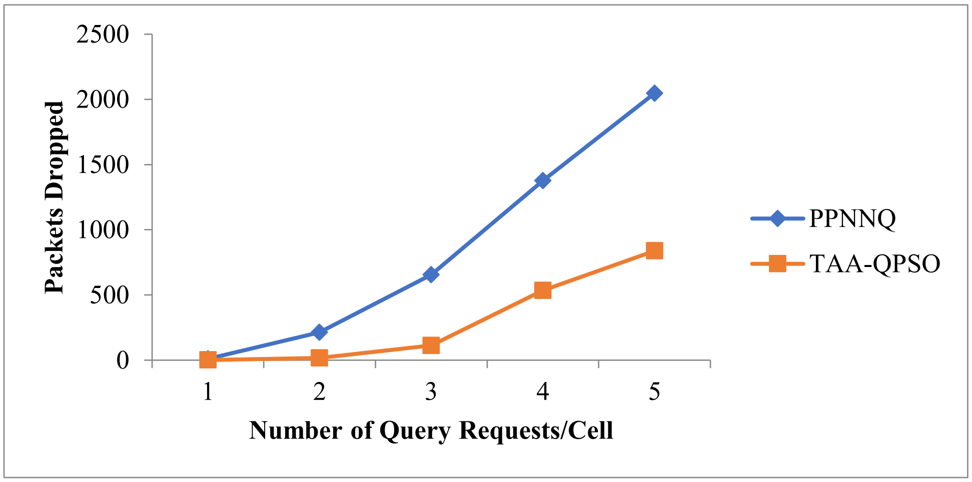

Figure 10: Packets Drop for varying query requests

Figure 10 shows the number of requests varies (presumably increases); both the PPNNQ and TAA-QPSO schemes experience an increase in packet drop rates. This means that as the network becomes more congested or faces higher demand, a greater percentage of packets are not successfully delivered to their intended destinations. The key point highlighted is that TAA-QPSO outperforms PPNNQ in terms of packet drops, with a 77% reduction. This is a significant improvement, indicating that TAA-QPSO is more robust in maintaining packet delivery even under challenging network conditions, potentially due to its ability to handle misbehaving nodes more effectively.

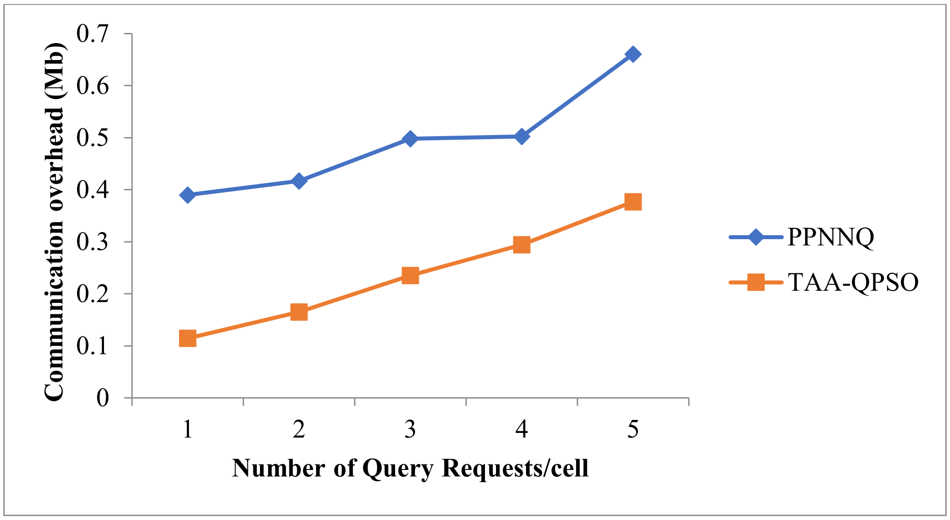

Figure 11: Communication Overhead for varying query requests

The communication overhead of PPNNQ and TAA-QPSO schemes has been depicted in Figure 11. TAA-QPSO has 53% lower communication overhead than PPNNQ because the subset of nodes that forward message packets is smaller. This observation also implies that the overhead cost of communication in TAA-QPSO is less heavy than that of the PPNNQ scheme. We suppose that decreasing the number of nodes involved in forwarding messages in TAA-QPSO decreases the quantity of the network traffic and resources necessary for communication and hence decreases overhead. When the requests are increasing, it can be observed that the overhead of both schemes increases. Nevertheless, the communication overhead of TAA-QPSO is 53% less than that of PPNNQ because only a small set of nodes is responsible for forwarding the message packets.

6 Conclusion

Here in this work, TAA-QPSO for WMN has been realized by implementing T-based anonymity and authentication techniques using QPSO. In this technique, the query request message is sent from the sender to the location server using a ticket through a number of dummy nodes chosen by SrBS. For the selection of the central node among the neighbours of the serving base station, the QPSO algorithm is utilized. Thus, conscious efforts are made to safeguard the identity of the senders and the ability to access the message is limited to a confirmed user. The use of the TAA-QPSO has been simulated in NS2 and the result with the PPNNQ technique has also been shown. From the simulation studies, it is proved that this technique increases the mutual authentication success ratio, and decreases the delay in authentication and the communication overhead.

Acknowledgement

This work was supported and funded by the Telekom Malaysia Research & Development (TMRND), MMUE/220071, Malaysia

References

[1] Ali, S., et al. (2022). Hybrid Encryption Scheme for Securing Query Messages in WMNs. *Journal of Information Security and Applications.*

[2] Ali, S., et al. (2022). Secure and Efficient Authentication Protocol for Wireless Mobile Networks. *Journal of Information Security and Applications, 66,* 103-115.

[3] Booch, K., Wehrmeister, L. H., & Parizi, P. (2025). Ultra-low latency communication in wireless sensor networks: Optimized embedded system design. *SCCTS Journal of Embedded Systems Design and Applications, 2*(1), 36–42.

[4] Cha, H., et al. (2019). A Mix-Zone-Based Approach for User Anonymity in Wireless Networks. *IEEE Transactions on Mobile Computing.*

[5] Chen, L., et al. (2021). Anonymity Protocols for Wireless Networks: A Performance Evaluation. *IEEE Communications Surveys & Tutorials*

[6] Dhanalakshmi, N., Atchaya, S., & Veeramani, R. (2015). A Design of Multiband Antenna using Main Radiator and Additional Sub-Patches for Different Wireless Communication Systems. *International Journal of communication and computer Technologies*, *3*(1), 1-5.

[7] Dwiputriane, D. B., & Heng, S. H. (2022). Authentication for 5G Mobile Wireless Networks. *Journal of Engineering Technology and Applied Physics*, *4*(1), 16-24. https://doi.org/10.33093/jetap.2022.4.1.3

[8] Gupta, A., et al. (2022). Enhancing Authentication Processes in WMNs Using QPSO. *Journal of Network and Computer Applications.*

[9] han, M. A., et al. (2020). A Hybrid Approach of Particle Swarm Optimization and Genetic Algorithm for Feature Selection. *Journal of King Saud University - Computer and Information Sciences.*

[10] Iqbal, A., Jiat Tiang, J., Kin Wong, S., Alibakhshikenari, M., Falcone, F., & Limiti, E. (2020). Multimode HMSIW-based bandpass filter with improved selectivity for fifth-generation (5G) RF front-ends. *Sensors*, *20*(24), 7320. https://doi.org/10.3390/s20247320

[11] Jain, A., & Chatterjee, D. (2024). The Evolution of Anatomical Terminology: A Historical and Functional Analysis. *Global Journal of Medical Terminology Research and Informatics*, *2*(3), 1-4.

[12] Khan, M. A., Abbas, S., Nasir, Q., Almogren, A., & Guizani, M. (2020). A survey on security and privacy issues in wireless mobile networks. *Journal of Network and Computer Applications*, 168, 102739.

[13] Khan, S. A., Shayea, I., Ergen, M., El-Saleh, A. A., & Roslee, M. (2021, December). An improved handover decision algorithm for 5G heterogeneous networks. In *2021 IEEE 15th Malaysia International Conference on Communication (MICC)* (pp. 25-30). IEEE. 10.1109/MICC53484.2021.9642076

[14] Kumar, R., et al. (2023). Quantum Particle Swarm Optimization for Secure Communication in Wireless Networks. *Journal of Information Security and Applications.*

[15] Kumar, R., et al. (2023). Ticket-Based Authentication Model for Wireless Mobile Networks. *Journal of Computer Networks and Communications.*

[16] Liu, Y., et al. (2021). Lightweight Authentication Scheme for Mobile Devices in Wireless Networks. *IEEE Access.*

[17] Ma, D., & Tsudik, G. (2010). Security and privacy in emerging wireless networks. *IEEE Wireless Communications*, *17*(5), 12-21. 10.1109/MWC.2010.5601953

[18] Mishra, A., & Kumar, A. (2021). Privacy-Preserving Techniques for Nearest Neighbor Queries in Mobile Networks. *Journal of Network and Computer Applications, 175,* 102-115.

[19] Reddy, S., & Mohan, P. (2024). Optimizing Energy Efficiency in Wireless Power Transmission Systems for Industrial Applications. *Association Journal of Interdisciplinary Technics in Engineering Mechanics*, *2*(2), 19-23.

[20] Roy, S., Tiang, J. J., Roslee, M. B., Ahmed, M. T., & Mahmud, M. P. (2021). A quad-band stacked hybrid ambient RF-solar energy harvester with higher RF-to-DC rectification efficiency. *IEEE Access*, *9*, 39303-39321. 10.1109/ACCESS.2021.3064348

[21] Sadeque, M. G., Yusoff, Z., Roslee, M., & Hadi, N. S. R. (2019, August). Design of a broadband continuous class-F RF power amplifier for 5G communication system. In *2019 IEEE Regional*

Symposium on Micro and Nanoelectronics (RSM) (pp. 145-148). IEEE. 10.1109/RSM46715.2019.8943508

[22] Selvam, P., & Stalin, N. (2018). Power Transfer Efficiency Analysis of Double Intermediate-Resonator for Wireless Power Transfer. *International Journal of Advances in Engineering and Emerging Technology*, *9*(3), 130-141.

[23] Sharma, P., et al. (2023). Challenges in Maintaining Security in Mobile Wireless Networks. *International Journal of Information Security.*

[24] Thillaigovindan, S. K., & Subramaniyan, P. (2019). EPPAA-enhanced privacy preserving-anonymity authentication model with QPSO for wireless mobile networks. *International Journal of Intelligent Engineering and Systems*, *12*(2), 135-144.

[25] Wang, J., et al. (2020). Dynamic Anonymous Routing Protocol for Wireless Mobile Networks. *Journal of Network and Computer Applications.*

[26] Yeonjin, K., Hee-Seob, K., Hyunjae, L., & Sungho, J. (2023). Venting the potential of wirelessly reconfigurable antennas: Innovations and future directions. *National Journal of Antennas and Propagation*, *5*(2), 1-6. https://doi.org/10.31838/NJAP/05.02.01

[27] Zhang, Y., et al. (2020). A Quantum-Inspired Particle Swarm Optimization Algorithm for Resource Allocation in Wireless Networks. *Wireless Networks, 26*(5), 1-12.

[28] Zhang, Y., et al. (2021). An Overview of Anonymity and Authentication in Wireless Networks. *IEEE Communications Surveys & Tutorials.*

[29] Zhang, Y., et al. (2022). Optimizing Routing Paths in WMNs Using Quantum Particle Swarm Optimization. *International Journal of Wireless Information Networks.*

Authors Biography

J. Jayapradha is an Assistant Professor at department of Computing Technologies, SRMIST. She had completed her Ph.D(CSE) in Privacy Preservation. and has published many research articles on Machine Learning, Data Mining, and Privacy. She has 6 patents published and 2 patents granted in the field of ML and data privacy. Her research interests include Machine Learning, Databases, and Privacy.

Dr. Mardeni Roslee serves as Chairman of Centre of Wireless Technology, Deputy Director of Research Management Centre and was President of MMU Mesra, Multimedia University. At international/local level, he was a Chairman of IEEE Malaysia in Comsoc/VTS for 2019-2020 and currently service as Vice-Chair of Malaysian Radar & Navigations Interest Group (MyRaN ig), Malaysian Society for Engineering & Technology (MY SET). He was also the main founder of Armada Smart Tech MR Sdn Bhd, Spinn Off Company and registered Chartered Engineer with Engineering Council United Kingdom, and Member with The Institution of Engineering and Technology (IET), UK He has published 154 papers for indexed journals, conference proceedings, professional magazine and book chapters with 558 citation, h-index 13 and i10 index 15. At national and international level, he has been involved in industry consultation and collaborations with some companies, private and government sectors.

T. Senthil Kumar graduated with a bachelor's degree in Electronics and Communication Engineering and a master's degree in computer science and engineering in 2004 and 2006, respectively. He completed his Ph.D. in CSE from SRMIST, Chennai, 2019. His areas of expertise include Wireless Communication, Network Security, Machine Learning, the Internet of Things, and Vehicular Networks. He had developed various inhouse projects for SRM Institute of science and technology to automate the process of End semester examinations. He had published more than 40 scopus indexed journals. He is doing Post doctoral fellowship in Multimedia University, Malaysia

Dr. Chilakala Sudhamani received her B.Tech degree in electronics and communication engineering from Jawaharlal Nehru Technological University, Hyderabad, India in 2005, M.Tech degree in Digital Electronics and Communication Science from Jawaharlal Nehru Technological University, Kakinada, India in 2011 and completed her Ph.D. degree in Wireless Communications and Networking from Acharya Nagarjuna University, Andhra Pradesh, India in 2020. She is currently working as a Postdoctoral Research Fellow in the Center for Wireless Technology Lab, Faculty of Engineering, Multimedia University Malaysia. She published more than 30 research papers in reputed journals and conferences. Her areas of research interest are 5G Networks, wireless channel modeling, spectrum sensing in cognitive radio networks, Cooperative Spectrum sensing, Signal Processing.

Azmi Ismail is an experienced engineer (researcher) with a demonstrated history of working in the telecommunications, semiconductor & electronics industry. Programming skills in Javascript (Back-end), Python, Java/Android, C/C++ and hardware skills in mixed-signal circuit design and data converter. Strong research professional with a Bachelor of Engineering (B.Eng) majored in Electrical and Electronics from Universiti Teknologi Malaysia (UTM).

Anwar Faizd Osman was born in Georgetown, Penang. He has a Master of Science degree in Electrical and Electronic engineering from Universiti Sains Malaysia (USM). His master's thesis is on wideband low noise amplifier design. He is currently the Head of 5G Product Development for Telekom Malaysia. In Telekom Malaysia, he leads the End to End roadmap development for Telekom Malaysia (TM) 5G Core as a Service, which include Network Slicing, 5G Standalone capable solutions and related 5G Value Added Services. Prior to Telekom Malaysia, he has worked in Rohde & Schwarz, Agilent Technologies, Motorola Solutions and Intel Malaysia, either in manufacturing or field application positions. He has published multiple technical papers on LNA, RF switches, and RF filter designs. His research interests include wireless testing for mobile operators and interference hunting. Mr. Osman has been a Committee Member of IEEE ED/MTT/SSC Penang Chapter, since 2015, currently serves as the Chapter Author.

Dr. Fatimah Zaharah Ali is a senior lecturer at College of Engineering, Universiti Teknologi MARA (UiTM), Malaysia since 2012. She obtained her Bachelor of Engineering (Honours) in Electrical and Electronics from Universiti Teknologi Petronas (UTP), Perak, Malaysia in 2009; MSc. in Telecommunication and Information Engineering from Universiti Teknologi MARA (UiTM), Selangor, Malaysia in 2012; and PhD in Electrical Engineering, UiTM, Selangor, Malaysia in 2023. She also had worked as an Assistant Manager in Telekom Malaysia (TM) Berhad in 2010 for a year before she pursued her master's degree.

Idris Olalekan Adeoye is a senior lecturer at Centre for Wireless Technology, Faculty of AI & Engineering, Multimedia University Cyberjaya, Malaysia.