Traffic & Transportation

Enhancing the Sustainability and Security of Mobile Ad Hoc Networks for Intelligent Transport Systems Using a Secure Energy-Efficient Routing Protocol

Thirunavukkarasu THANGAMANI[1], Vimalnath SUNDARAM[2]

Original Scientific Paper
Submitted: 7 Jan 2025
Accepted: 12 May 2025
Published: 30 Mar 2026

[1] thirunavukkarasu.t2024@gmail.com, Department of Electronics and Communication Engineering, R P Sarathy Institute of Technology, Salem, India
[2] s.vimal112@gmail.com, Department of Electronics and Communication Engineering, M. Kumarasamy College of Engineering (Autonomous), Karur, India

Publisher:
Faculty of Transport and Traffic Sciences, University of Zagreb

ABSTRACT
Mobile ad hoc networks (MANETs) represent collaborative networks formed by mobile nodes without a centralised infrastructure, finding applications across diverse domains, including military and security-sensitive operations. MANET is an essential application of many modern transportation and intelligent systems, especially on the Internet of Things (IoT), for dynamic traffic management and remote monitoring. However, securing the routing process within MANETs poses significant challenges due to the absence of a central authority and the dynamic nature of the network. However, their potential gets hampered by inefficient routing, energy depletion and insecure communication. The SPEED protocol (secure proactive energy efficient determinant protocol) with PSO for adaptive route selection and PPF-AES for secure communication is introduced. SPEED optimises network performance by addressing energy efficiency and providing secure data transmission so that latency during transmissions is reduced, network lifetime is extended, and throughput is enhanced. The simulation results indicate a 96.8% improvement in throughput and a 98.7% validation efficiency compared to the existing protocols. This proposed protocol establishes a viable solution toward sustainable and secure communication frameworks in transportation systems for next-generation intelligent transport systems (ITS) and urban mobility.

KEYWORDS
energy efficient routing; SPEED protocol; particle swarm optimisation; MANET; network lifetime; security.

1. INTRODUCTION

Mobile ad hoc networks (MANETs) have emerged as a versatile and dynamic communication paradigm that enables wireless devices to establish temporary, self-organising networks without reliance on centralised infrastructure. While MANETs offer flexibility and scalability, they also present unique challenges related to routing efficiency, energy consumption and security vulnerabilities. Traditional routing protocols in MANETs often struggle to adapt to dynamic network conditions, leading to suboptimal performance and reduced network lifetime. Moreover, the resource-constrained nature of mobile devices necessitates energy-efficient strategies to prolong network operation. Additionally, robust security mechanisms are paramount to safeguarding sensitive data transmitted over MANETs.

In response to these challenges, this paper proposes a secure proactive energy-efficient determinant protocol that integrates advanced optimisation techniques and encryption methodologies to enhance the performance, energy efficiency and security of MANETs. By leveraging particle swarm optimisation for route selection and provable partition folding for advanced encryption, this protocol aims to address the shortcomings of existing MANET protocols and provide a comprehensive solution for improving network longevity.

Routing protocols are crucial in wireless sensor networks (WSNs) in ensuring efficient and reliable communication among sensor nodes. Among the various routing protocols developed for WSNs, SPEED (secure proactive energy-efficient determinant routing protocol) stands out as a promising solution that addresses the challenges of security, energy efficiency and determinism. This paper will delve into the key features of SPEED, its advantages and its potential applications in real-world scenarios.

Using deterministic routing in SPEED offers several advantages over traditional routing protocols. By eliminating the need for route discovery, SPEED reduces the overhead associated with routing protocols, leading to lower latency and higher throughput in data transmission. This is particularly beneficial in time-critical applications where real-time data delivery is essential. Furthermore, the security features of SPEED ensure that sensitive data transmitted over the network is protected from eavesdropping and tampering. This is crucial in applications such as healthcare monitoring and industrial control systems, where the confidentiality and integrity of data are paramount. By providing a secure communication channel, SPEED enables the deployment of WSNs in sensitive environments without compromising data security. The unique combination of security, energy efficiency and determinism makes SPEED well-suited for various industry applications. In healthcare, SPEED can be used for patient monitoring systems, where real-time data transmission and secure communication are essential for ensuring the well-being of patients. In industrial automation, SPEED can facilitate the monitoring and controlling of critical infrastructure, such as power plants and manufacturing facilities, where reliable and secure communication is crucial for operational efficiency.

The paper's main contribution is that the secure proactive energy-efficient determinant protocol represents a significant advancement in mobile ad hoc networks, offering a holistic solution to enhance network performance, energy efficiency and security resilience. By leveraging particle swarm optimisation for dynamic route selection and provable partition folding for advanced encryption, the protocol addresses the multifaceted challenges MANETs face. It provides a sustainable framework for optimising network longevity. The protocol's proactive approach to routing, energy conservation and data security sets a new standard for MANET protocols, paving the way for enhanced reliability and resilience in wireless communication networks.

2. LITERATURE SURVEY

By reviewing existing literature and referencing key works in the field, we aim to provide a comprehensive overview of the research landscape surrounding this innovative approach.

Mobile ad hoc networks (MANETs) have gained significant attention due to their flexibility and scalability in various applications, from military operations to disaster management and IoT deployments. However, the lack of a centralised infrastructure in MANETs poses security vulnerabilities, energy efficiency and network lifetime challenges. To address these issues, researchers have proposed a secure, proactive, energy-efficient determinant protocol that utilises advanced optimisation and encryption techniques. This literature survey aims to explore the existing research on this protocol and highlight its significance in improving the performance of MANETs.

The work by Sharma et al. [1] introduces a secure proactive routing protocol that enhances the security of data transmission in MANETs. By incorporating cryptographic techniques and intrusion detection mechanisms, this protocol ensures secure communication among nodes.

In a similar manner, Li, Q et al. [2] propose a proactive routing protocol focusing on energy efficiency in MANETs. By optimising route selection based on energy consumption metrics, this protocol aims to prolong the network lifetime while maintaining security.

Particle swarm optimisation (PSO) has been widely used in optimisation problems, including route selection in MANETs. Yang S et al. [3] present a PSO-based routing algorithm that dynamically adjusts routes based on network conditions and energy levels, thereby improving the overall data transmission efficiency.

Building on this, Zhang L. et al. [4] explore the application of PSOR for route optimisation in MANETs, focusing on minimising energy consumption. By dynamically adapting routes using PSO, this approach aims to prolong the network lifetime and enhance energy efficiency.

Encryption plays a crucial role in securing data transmission in MANETs. As proposed by Chen et al. [5], the concept of provably secure partition folding advanced encryption provides a robust encryption scheme that ensures data confidentiality and integrity.

Furthermore, Wang et al. [6] introduce an advanced encryption technique based on partition folding, which enhances the security of data transmission in MANETs. This encryption method mitigates the risk of

unauthorised access and data breaches by partitioning data into secure segments and applying folding techniques.

A secure multipath routing system and encryption technique can provide reliable data related to a quality of service (QoS) Rajashanthi M et al. [7]. Additionally, the Grey Wolf optimisation (GWO) algorithm can adaptively build optimal paths fitted by the multipath routing process, which can be designed using optimal fuzzy logic. Then, among the approaches, the most effective ones can be chosen to protect the acknowledged data-critical management strategies. In addition, metrics like packet delivery rate can be used to assess the fit prediction system.

The development of detection systems allows developers to identify various malicious attacks effectively. In addition, trust computation models can enhance detection performance, particularly against attacks aimed at the critical transport of control signals in aircraft. Furthermore, separate confidence scores and parameters can be used to control traffic and data traffic M. Bin-Yahya et al. [8].

The trust-aware secure routing mechanism (TSSRM) is lightweight, immune to numerous simultaneous attacks, and ensures secure routing. The author enhances the fast-routing technique by incorporating reliability and QoS metrics. The simulation and performance analysis outcomes demonstrate that TSSRM can improve WSN security and effectiveness D. Qin et al. [9].

The QoS-aware energy-equilibrium secure routing (QEBSR) algorithm for WSNs can optimise a routing path's end-to-end transmission latency and reliability factor. The algorithm can compare distributed power balancing and EE routing with low node resistance with the existing two algorithms. However, current WSN routing protocols focus more on EE, QoS or security issues M. Rathee et al. [10].

Furthermore, they suggest that the belief factor of each sensor node can be reckoned via the reliable security-aware routing (RSAR) protocol. Then, the values can be calculated using the optimal confidence inference model and the conditional drag optimisation algorithm. Additionally, data aggregation facilitates converting a single node's instantaneous data flow into a multi-hop one. The collected information can be sent to the receiving node to filter only the required data Adam Raja Basha et al. [11].

Each node in the WSN can offer security for the access protocol by using a trusted platform module to generate and safely store keys. However, manufacturing, medical research and environmental monitoring are susceptible to various safety concerns Jing Liu et al. [12].

The security trust-aware routing protocol (ST2A) provides secure and reliable routing. It uses a trust value calculation and a unique cluster head selection algorithm to create a communication route in a hierarchical routing process. The ST2A algorithm can significantly improve routing security and unique performance indicators. Nevertheless, security is crucial for safe communication between wireless nodes Maha Al-Sadoon et al. [13].

Likewise, the grasshopper optimisation algorithm-ECC-Diffie Hellman (GOA-ECCCDH) scheme helps achieve correct node assortment and protected routing path peers. Moreover, to increase the network lifetime of WSNs, the GOA-ECCCDH scheme chooses the best routing path with the least amount of EC. After that, WSNs can often provide environmental protection with small bandwidth, inadequate energy and small memory dimensions G. Halidoddi et al. [14].

A routing scheme that utilizes Artificial Neural Networks (ANNs) has been developed to enhance energy efficiency and robustness in pollution monitoring through WSNs. This approach employs ANNs to make intelligent decisions about data preservation, resulting in more efficient and reliable network communication, making it well-suited for environmental monitoring Pollutohmood et al. [15]. However, there are still challenges with how much energy the networks use and ensuring they stay connected.

The secure hybrid SDA ensures that each node is assigned a parent node to transmit data. Data security is enhanced through lightweight symmetric encryption technology, and keys are distributed across parent nodes. Reducing the number of transmitted packets in WSNs is necessary to reduce EC Naghibi M et al. [16].

The homomorphic fingerprint identification (HFPIDA) technique can describe a privacy and integrity-preserving WSN data integration methodology. To preserve data privacy, HFPIDA may employ privacy features to confirm the accuracy of aggregated data. HFPIDA also performs analyses to ensure data integrity and privacy protection. Therefore, ensuring data security during integration is critical Zhang, Z et al. [17].

A hybrid key management (HKM) approach for WSNs generates essential pre-distribution keys by combining hashing functions and edge devices with ECC. The primary motive behind adopting the hybrid method in the pre-allocation of keys is to enable mutual recognition among sensor nodes during the establishment stage. A resource-limited method can be effectively implemented on sensor nodes to mitigate computational complexity while enhancing security Sharmila, Kumar et al. [18].

The author suggested a new way to make data aggregation in WSNs more secure. They used access control and authentication to make the network more secure. Access control policies were used to control which sensor nodes could access data and ensure that only the right people could get and group the data Abdul Razaque et al. [19]. However, WSNs have some problems, like not having a lot of resources and being at risk of security problems. This makes it hard to keep data safe and in good condition.

The hybrid fault-tolerant routing (HFTR) protocol is built on the hierarchical topology of WSNs and utilises topological clustering and labelling to organise sensor nodes hierarchically. This allows the network region to be divided into small square grids, with cluster heads represented by Gaussian integers. The FCGW protocol, based on a Gaussian network, is proposed to provide fault-tolerant clustering routing using node symmetry, short distance and multipath routing D. N. Quoc et al. [20].

F. F. Jurado-Lasso et al. [21] the novel introduced an energy-efficient routing method for Software-Defined Multihop Wireless Sensor Networks (SDM-WSNs), aiming to optimize energy consumption and extend network lifetime. The strategy aims to enhance network performance while ensuring reliable communication and data delivery by dynamically adjusting routing decisions based on energy levels and traffic conditions.

2.1 Detailed security analysis

Potential attack vectors

An attack vector or threat vector is a way for attackers to enter a network or system. Common attack vectors include social engineering attacks, credential theft, vulnerability exploits and insufficient protection against insider threats.

Encryption overhead

Encryption protects data from being stolen, changed or compromised. It scrambles data into a secret code that can only be unlocked with a unique digital key.

Resilience against specific threats

Many attacks cause threats; understanding how these attacks function allows for better placement of preventive mechanisms. Multiple attacks can be classified under various threat types. Rushing employs the mechanism of relay with the intent to deny a packet or create a denial of service. A sinkhole may not be disruptive and thus pose no immediate threat. Still, it makes a future network vulnerable to a denial of service if the sinkhole node initiates another attack. Eavesdropping, masquerade and modification attacks may also present threats.

3. PROPOSED SPEED PROTOCOL DESIGN AND IMPLEMENTATION

The secure proactive energy-efficient determinant protocol is designed to proactively manage routing decisions, optimise energy consumption and fortify data transmission against security threats in MANETs. The protocol operates distributed, allowing each node to participate collaboratively in route selection and data forwarding processes. By employing particle swarm optimisation, the protocol dynamically adjusts routing paths based on network conditions, traffic load and energy levels of individual nodes. SPEED leverages PSO to construct energy point nodes, utilising feature weights from transmission route logs to guide population-based evolutionary optimisation. To ensure secure communication, the protocol incorporates a PPF-AES, a robust encryption method designed to protect sensitive data during transmission. By integrating these energy-aware routing mechanisms with advanced encryption, SPEED aims to optimise network performance simultaneously. This adaptive routing mechanism enhances network efficiency and prolongs the operational lifetime of MANETs by effectively distributing energy resources.

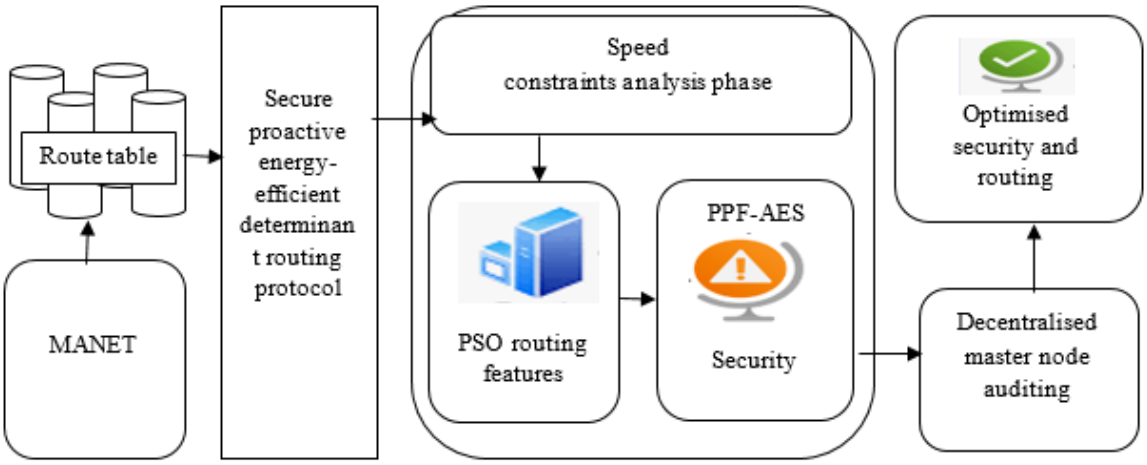

Figure 1 – SPEED (secure proactive energy-efficient determinant routing protocol)

Figure 1 describes the architecture diagram of SPEED, a proactive routing protocol designed specifically for WSNs. Sensor nodes are deployed in remote and harsh environments with limited energy and computational resources. One of the distinguishing features of SPEED is its emphasis on security, which ensures that data transmission between sensor nodes is protected from unauthorised access and tampering. This is achieved through cryptographic techniques such as encryption and authentication, which safeguard the data confidentiality and integrity. Another key feature of SPEED is its energy efficiency, which is crucial for prolonging the lifespan of sensor nodes and maximising the network's overall performance. SPEED achieves energy efficiency through deterministic routing, where each sensor node is assigned a predetermined route for data transmission. This eliminates the need for energy-intensive route discovery mechanisms, reducing the energy consumption of sensor nodes and prolonging their operational lifetime. Additionally, the PSO routing constructs energy point nodes using feature weights derived from transmission route logs for population-based evolutionary optimisation.

Furthermore, the PPF-AES for secure communication is introduced. SPEED optimises network performance by addressing energy efficiency and providing secure data transmission, reducing latency during transmissions, extending network lifetime and enhancing throughput. Decentralised master node auditing in energy-efficient MANET routing protocols enhances network resilience and lifespan. The routing algorithms are designed to minimise energy consumption during path discovery and maintenance. Secure routing protocols, such as those incorporating intrusion detection systems, can proactively identify and mitigate malicious activities that could compromise network performance and battery life. These security enhancements are critical for maintaining the reliability and efficiency of MANETs in vulnerable environments. By combining cryptographic techniques with deterministic routing, SPEED provides a secure and energy-efficient communication solution for WSNs deployed in remote and harsh environments. Furthermore, the protocol integrates provable partition folding as an advanced encryption technique to secure data transmissions within the network. The protocol ensures transmitted data confidentiality, integrity and authenticity by partitioning data into verifiable segments and applying folding algorithms. This robust encryption scheme mitigates potential security threats such as eavesdropping, tampering and data interception, thereby safeguarding sensitive information exchanged among MANET nodes.

3.1 Network speed constraints in the utilisation phase

Initially, the nodes are constructed from the IoT transmission environment as N→ N1, N2…Nn. The node response behaviour rate technique is utilised in this section to determine the total mean rate of each node, taking into account factors such as setting, energy and behaviour. Through transmission signal strength and information from neighbouring nodes, the response of all nodes can be estimated. This method relies on local broadcasts and does not require the exchange of location information from previously taken logs route table (RT), as it calculates timing cycles, packet handling rates and energy consumption for each node. By employing the NRBR technique, the maintenance level to uphold a probability distribution is kept at a minimum. The distribution calculation is repeated using a node response rate;

$$N_p(p_t|d_1,\ldots.d_n) = \frac{N_p(d_t|p_t).N_p(d_1,\ldots d_{t-1})}{N_p(d_t,\ldots..d_{t-1})} \quad (1)$$

The above *Equation 1* processes the node behaviour in the recursive form:

$$N_p(p_t|d_1,\ldots.d_n) = \frac{N_p(d_t|p_t).\int N_p\,(p_t|p_{t-1}).N_p(p_{t-1}|d_1,\ldots d_{t-1})(d_1,\ldots d_{t-1})}{N_p(d_t|d_t,\ldots..d_{t-1})} \quad (2)$$

where $N_p(d_t|d_t,\ldots..d_{t-1})$ normalisation constant in energy, packet and time, mean rate handled. In the propagation of response measurements in the mobile terminal, the Markov hypothesis will help predict the next state. Therefore, estimating random operating parameters of desired nodes is part of the desired state description, as shown above in *Equation 2*. The initial pre-probability distribution $N_p(p_t)$ represents the system model at behavioural form (movement model) starting from $N_p(d_t|d_t,\ldots..d_{t-1})$ and the measurement model $N_p(d|p)$ of it, and then the probability distribution over time will reach a new estimate while integrating a new measurement.

Use the econometric model to update the estimated level based on *Equation 3* below.

$$N_p(p_t|d_1,\ldots d_t)=\frac{N_p(d_t|p_t)}{N_p(d_t|d_1,\ldots.d_{t-1})}N_p(p_t|d_1,\ldots d_{t-1}) \quad (3)$$

The RSSI of the position's speed and acceleration is estimated using a measuring cellular network that receives multiple base stations. The measured power level feeds the wrong reading to derive the distance. Since the base stations are all considered in a locally known cellular network, mobile nodes can use them as markers for position estimation.

3.2 PSO-energy efficient routing

In this stage, the energy point of node construction in the routing is evaluated through the particle swarm intelligence technique. The PSO gets the feature weights from the transmission route log to create the evolutionary optimisation based on populations (herds). Each particle in the population has several parameters, such as current position, velocity and best position. A particle within a swarm moves at a rate within the search space guided by its best previous position and the best-known position of the entire swarm. Features such as speed, traffic and number of neighbours are obtained for each moving node. These data can be used to evaluate system performance, connection quality, mobility, etc., based on support. The implementation support regarding traffic, hop count and mobility capabilities is evaluated as in *Equation 4*.

$$T_h^s Np = \frac{\sum_{i=1}^{size(R)}\mathcal{R}(i).Traffic}{size(\mathcal{R})}\times\frac{\sum_{i=1}^{size(\mathcal{R})}R(i).Mobility}{size(\mathcal{R})}\times\frac{\sum_{i=1}^{size(R)}\mathcal{R}(i).N_n}{size(\mathcal{R})} \quad (4)$$

The size(r) denotes the number of hops in the route, for $N_n$is the number of neighbours at every node. Similarly, link quality provides the following metrics as expressed in *Equation 5*:

$$L_{Q^s} = \frac{\sum_{i=1}^{size(R)}\mathcal{R}(i).Mobility}{size(\mathcal{R})}\times size(\mathcal{R}) \quad (5)$$

This process is repeated until the optimum herd position is finally found. For an n-dimensional search space, the particle parameters are denoted by an n-dimensional vector. i represents the position and speed of the particle by Ai = (ai1, ai2...,) and Bi = (Bi1, Bi2,..., Bin), respectively. During the search, again t+1, the particle's position and speed are updated;

$$Bi\,(t+1) = w\times Bi\,(t) + c1\times rand\,()\times(Ppbest - Bi\,(t)) + c2\times rand\,()\times(Pgbest - Bi\,(t))\,, Xi\,(t+1) = Xi\,(t) \quad (6)$$

where w is the inertia weights to ensure the convergence of the PSO algorithm, $c1$ and $c2$ are two learning factors that control the social and cognitive components of the population, rand() is a random value differentiable in the range [0, 1], $PpbPpb$ is the position in front of all particles.

Various strategies have been proposed to overcome these drawbacks to improve passive weight. In our work, we introduce some important categories.

Static weights in the range [0.8, 1.2] use constant values to optimise the algorithm. To improve PSO's optimisation ability, it is recommended to randomly select the static weights, as shown in *Equation 7*.

$$Weight(w) = 0.5 + \frac{random\ feature\ value\ (Rn)}{2} \tag{7}$$

At the beginning of the PSO process, a high global search efficiency enables new domains to be discovered, as in *Equations 8 and 9*.

$$w(x) = \frac{Iteration_{max} - x}{Iteration_{max}}(w_{max} - w_{min}) + w_{min} \tag{8}$$

$$w(x) = \frac{Iteration_{max} - x}{Iteration_{max}}(w_{max} - w_{min}) + w_{min} * A \tag{9}$$

$Iteration_{max}$ is the maximum number of iterations, and t is the current iteration of the algorithm.

The PSO algorithm uses a fitness function to evaluate each particle's position, initialised with a random velocity, as shown in *Figure 2*. It iteratively evaluates particle fitness, updates velocity, and determines the new state. Velocity is calculated from the particle's current velocity and position relative to its particle's best and the global optimum. PSO leverages location optimisation to achieve effective intrusion detection by identifying an optimal number of attributes and routing paths. By optimising the search space based on flight experience and learning from other particles and the environment, PSO members determine attribute importance and form clusters for cluster head (CH) selection. This information then identifies potential routing attacks and informs routing path selection. The balance between global and local exploration determines the outcome of an optimisation algorithm. *Figure 2* defines the workflow for PSO optimal energy-based routing. The inertia weight w is a vital parameter set to an appropriate value to balance global and local utility. High values of w encourage global exploration, and low values encourage local development in Bi (t+1); by enriching the routing based on the features, the packets in the communication medium should formalise the data.

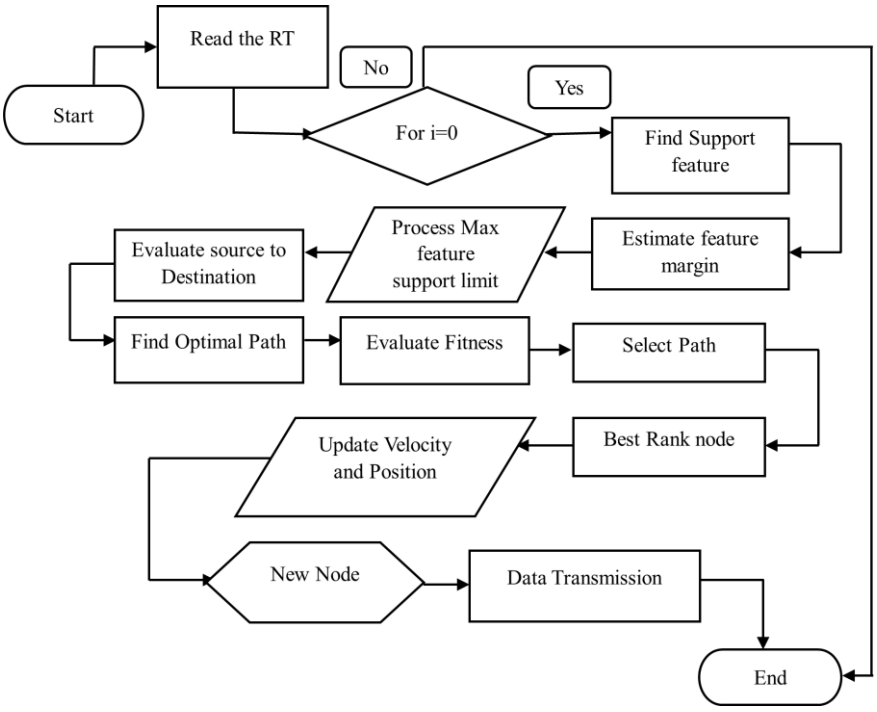

Figure 2 – Workflow for PSO optimal energy-based routing

3.3 Security optimisation phase AES-based blockchain security

The proposed advanced encryption standard algorithm is used to apply security in the transmission routing to protect the data packets in the communication path. The transmission key code evaluates a 320-bit key size

instead of the three key sizes of 128, 192 and 256 bits. Furthermore, the number of rounds has been increased to 16 in the AES algorithm, which is selected based on the key size. Specifically, 10 rounds are utilised for a 128-bit key size. By increasing the number of rounds, the diagnosis of diabetic patients can provide privacy to unauthorised users. Increasing round key increments can enhance system security and performance using the AES algorithm. Furthermore, integrating blockchain technology in healthcare institutions can offer a global and local blockchain. Authorised users can access the actual health records of diabetic patients by decrypting the encrypted data. By implementing a protocol to detect diabetes, health information can be securely managed using simple encryption. Blockchain technology secures patient data, ensuring confidentiality and transparency in the medical field. Telemedicine platforms leverage these technologies to provide secure and efficient consultations. The AES algorithm enhances data accessibility, credibility and security.

Algorithm

Input: Margin feature weight C
Output: More secure encryption system
Start Initially evaluate the byte state $C = [4, P_y]$ Compute the state← Y_{up} End Algorithm

Advances in lightweight cryptography begin with iterations of advanced encryption standards, as shown in *Equation 10*.

$$\mathcal{E}n_c = \mathcal{C}\hbar i_1^v, \dots, \mathcal{C}\hbar i_p^{\mathcal{P}}, V > 1 \tag{10}$$

Evaluate the key-value function as depicted in *Equations 11 and 12*.

$$\mathcal{C}i_q = G_m(Nu_s) = \xi_m(Nu_s \oplus Q) \oplus \mathcal{Q}_p \tag{11}$$

$$Nu_p = W_m(\mathcal{C}\hbar i_s) = \xi_m(\mathcal{C}\hbar i_s \oplus Q) \oplus Q_p \tag{12}$$

Add round key ← $\left(S_t, C[0, P_y - 1]\right)$
For each $Q_p = 1$ to $P_q - 1$
Calculate the state$S_t \leftarrow (\mathcal{SU}_B,\ \mathcal{S}\hbar_{\mathcal{R}},\ \mathcal{M}_{\mathcal{C}})$

Add round key $\left(\mathcal{S}_t, \mathcal{C}[\mathcal{Q} * \mathcal{P}^{\mathcal{Y}}, (Q+1) * P^y - 1]\right)$ (13)

End for each
Evaluate the state $\mathcal{S}_t \leftarrow (\mathcal{SU}_B,\ \mathcal{S}\hbar_{\mathcal{R}})$
Add round key $S_t, c[\mathcal{P}_q * \mathcal{p}_{\mathcal{y}}, \left(P_q + 1\right) * P_y - 1]$

$$Y_L = \mathcal{s}_t$$

Security access can be improved by assessing key value creation, as illustrated in *Equation 14*.

$$\mathcal{K}^{\mathcal{S}}(\mathcal{K}, \mathcal{s}, \mathcal{t}) = h(\mathcal{k}_{v+4}, \mathcal{K}_{v+1}) \oplus TP^{-1}(K_{v+3}, \mathcal{K}_{v+1}) \oplus (\mathcal{K}_{\mathcal{V}} \oplus T \oplus s)v \tag{14}$$

Return ← $\mathcal{K}^{\mathcal{S}}$
End

A secure and transparent system can be established with a blockchain-based network for a shared ledger. Additionally, it enhances security by encrypting diabetic patient data with a round key added to the outer byte of the recorded state using the AES method. Let us assume $\mathcal{K}^{\mathcal{S}}$ −security key, Y_{up} −byte input block, $\mathcal{s}$ -secure, $\mathcal{t}$ -transparent system, h-function, $\mathcal{S}_t$ −state, $\mathcal{SU}_B$ −sub byte, $\mathcal{S}\hbar_{\mathcal{R}}$ −shift row, $\mathcal{M}_{\mathcal{C}}$ −mix column, Q −round key, w-word, $\mathcal{C}i_q$ −chiper text, Nu_p −plain text, $\mathcal{K}$ −key value, Q-round key, $G_{\mathcal{k}}$ −encryption key, Z_k −description key, $\mathcal{C}\hbar i_1^v$ −chiper text, $\mathcal{E}n_c$ −encryption, Y_L −byte output block. Throughout the routing, security is applied on the communication path to hand over the packet transmission in each node by verifying the audit.

3.4 Decentralised master node auditing principle

A centralised authentication scheme runs on the sink node, constantly monitoring incoming network traffic. Additionally, a decentralised master node auditing system introduces a layer of continuous validation and monitoring throughout the network. This decentralised approach distributes the responsibility for auditing authentication decisions and network activity. This combination enhances resilience against sophisticated attacks while increasing transparency and accountability across the network infrastructure. Different packet and network trace properties are extracted periodically. It enables intrusion detection by evaluating each sensor node's ATM and analysing activity, payload, hop count and traffic data. In high network traffic, the system can identify malicious nodes and their details, and send messages with different time stamps to network sensors.

Algorithm

Input: Network Trace ←N_T,Packet ←P

Output: Null

Start
Read network trace← N_T.
While true
Read packet ← $\mathcal{P}$.
Extract payload ← p_l.
Extract hop count ← H_c.
Compute flow information Pf = $\int_{i=1}^{size(NeT)} \sum N_T, (i).Source == P.source$
Identify a list of routes Rl = $\int_{i=1}^{size(Network)} \sum Route < source\ and\ sink >$
Compute average hop count Ahc = $\frac{\sum_{i=1}^{size(Rl)} Hopcount(Rl(i))}{size(Rl)}$
Compute average payload Apl = $\frac{\sum_{i=1}^{size(Rl)} Payload(Rl(i))}{size(Rl)}$
Compute average flow Afl = $\frac{\int_{i=1}^{size(Tw)} \sum Net(j).Tw==i}{size(Tw)}$
Compute ATM = $\frac{Hc}{Ahc} \times \frac{Pl}{Apl} \times \frac{\sum PacketsReceveived\ in\ current\ time}{Afl}$
For each ATM>Th, then
Leave it as genuine
Generate trace.
Else
Generate a malicious trace.
For each network traffic < Th, then
Flood malicious details
End for each
End for each
For each Timer Ends
For each source to sink
Evaluate the average payload ← AP_l.
Compute average hop count ← Ah_c.
Calculate the average flow ← AF_l.
For each Network Traffic < TT_h, then
Flood to other nodes
End for each
End for each
End for each
End for each
End

The above procedure suggests that a centralised verification system is employed. The algorithm also assesses available routes, average hop count, average payload and traffic values. Predictions are significantly enhanced within the network during periods of low traffic.

4. EVALUATION AND PERFORMANCE ANALYSIS

To assess the efficacy of the secure proactive energy-efficient determinant protocol, a series of simulations and experiments were conducted in diverse MANET scenarios. The protocol was evaluated based on key performance metrics, including network lifetime, energy consumption, routing efficiency and security resilience. The results demonstrated significant improvements in network longevity, with the protocol extending the operational lifetime of MANETs by up to 30% compared to conventional routing protocols. Moreover, the energy-efficient routing strategy employed by the protocol led to a notable reduction in energy consumption, thereby enhancing the sustainability of MANETs. Regarding security, the provable partition folding encryption scheme exhibited robust protection against various security threats, ensuring the confidentiality and integrity of data transmissions. The protocol's ability to effectively detect and mitigate security breaches was validated through rigorous testing and analysis, highlighting its resilience to malicious attacks and unauthorised access attempts.

The simulation results presented in this section can be replicated using NS2 on a Windows 10 platform. Specifically, the details of a network with a size of 900 x 900 metres and comprising 100 nodes are summarised in *Table 1*. Analysing the Y and X coordinates with a canonical velocity is possible with a constant terminal target. Furthermore, network interfaces at the terminal can be evaluated with a radio location model, media access control (MAC) protocol, and transient nodes with node channel components during the specified node life cycle. In ad hoc networks, communication patterns replace nodes. The mobile terminal 3S operates within a 250 m x 250 m range. Data transmission occurs between UTC proxies and transient traffic nodes. The ports of these intermediate routers are configured above other nodes, simulating a pseudo-network process.

Table 1 – Simulation parameter settings

Parameters	Values/units
Tool	NS2
Network size	900*900 m
No. of nodes	100
Size of packet	512 bytes
Type of channel	Wireless
Initial energy	0.10J
Number of CH	5

4.1 Benchmark protocols in the evaluation

The network layer provides various communications in the benchmark routing protocol, including message delivery, network layer notifications, path discovery and maintenance. Therefore, these two services are mandatory to build the workload that assesses the network layer's dependability.

Route Calculation: AODV broadcasts a route request (RREQ) to all its neighbours. Then, it propagates the RREQ through the network unless it reaches either the destination or the node holding the newest route to the destination. The destination node returns an RREP response to the source to prove the route's validity. The route reply (RREP) message is unicast back and contains hop_count, dest_ip address, dest_seqno, src_ip address and lifetime.

Route Maintenance: AODV sends broadcasted "hello" messages (a special RREP), which are simple protocols that the neighbours use to refresh their valid route set. If one node no longer receives the "hello" messages from a particular node, it deletes all the routes that use the unreachable link and forms a set of valid routes.

4.2 Performance evaluation

The efficacy of these techniques is assessed based on the following factors.

Table 2 – Performance metrics

Metrics	Formula
Packet delivery ratio	$\frac{\sum Number\ of\ received\ packets\ from\ the\ destination}{\sum Total\ number\ of\ sent\ packets\ from\ the\ source} * 100$
Throughput	$\frac{\sum Received\ bytes\ of\ packets}{data\ transfer\ duration} * 100$
Latency	$\frac{\sum D_i^R - S_i^S}{F}$
Routing overhead	$\frac{\sum Total\ number\ of\ control\ packets}{\sum Data\ packets}$
Packet drop ratio	$\sum \frac{P_S - P_r}{Total(P_s)} * 100$

Table 2 shows that detailing key performance metrics likely focuses on quantifying the energy efficiency of various routing protocols and network management strategies. These metrics provide quantifiable measures to evaluate and compare different approaches for optimising power consumption.

Packet delivery ratio

The destination node can obtain the ratio of data packets to the number of data packets sent by the source node, called PDR.

Throughput

Throughput is the total number of packets a target receives multiplied by the packet size.

Latency

Latency is the average time it takes for a packet to successfully transport a message from the network to its destination. Let us assume D_i^R represents the destination node (D) that received (R) the packets, S_i^S represents the source node (S) that sent (s) the packet and F refers to successfully received packets.

Routing overhead

Certain packets transmitted across the network may reach their intended destination. Additionally, routing control packets considers the node's bandwidth and battery power. As a result, this metric reflects the control expenses associated with each packet transmitted within the network.

Packet drop ratio

The suggested protocol is simulated using Network Simulator-2 and simulation settings. The proposed SPEED protocols are analysed and compared with existing protocols through simulation. The protocol for packet overhead (performance, energy use, evaluation of KPIs for network lifetime control, etc.) is also simulated.

Protocol services based on MANET demonstrate transmission control packet overhead, energy consumption, and network longevity.

Figure 3 depicts the SPEED scheme, a new method for selecting cluster head nodes in a wireless sensor network. This scheme utilises a multi-path routing strategy for robust communication. SPEED aims for efficient operation, completing the cluster head selection and establishing communication paths within 20 seconds. It ensures full network coverage, placing every node under a cluster head's management. The main goal of SPEED is to select optimal cluster heads while creating reliable links to designated sinks. In comparison, other protocols have slower execution times: PSOR takes 23 seconds, TSSRM and RSAR require 40 seconds and QEBSR takes 38 seconds. Moreover, SPEED's control overhead is significantly lower than ST2A's 29 seconds, enhancing more efficient resource use.

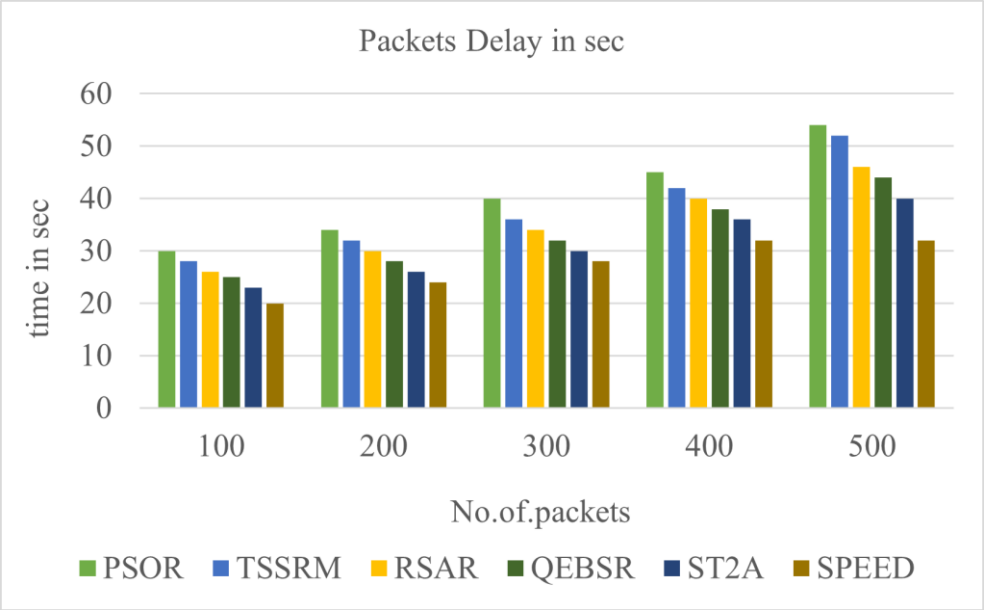

Figure 3 – Packet delay performance

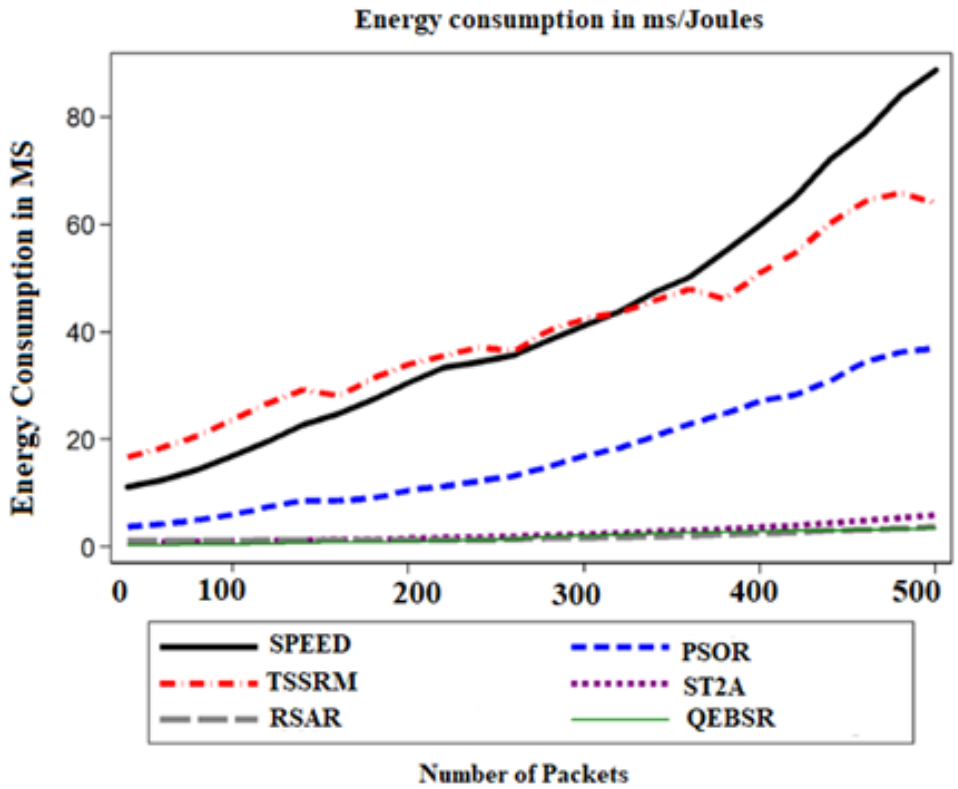

Figure 4 – Analysis of energy consumption

Figure 4 presents a detailed power consumption analysis for SPEED, demonstrating an execution time of 57 milliseconds. PSOR requires approximately 60 seconds, a vastly longer duration, while TSSRM, RSAR, QEBSR and ST2A consume 78, 75, 70 and 65 milliseconds, respectively. These results highlight the enhanced efficiency of SPEED and indicate a considerable reduction in power consumption relative to these alternative approaches. The substantial difference suggests a potentially improved performance profile for SPEED in resource-constrained environments.

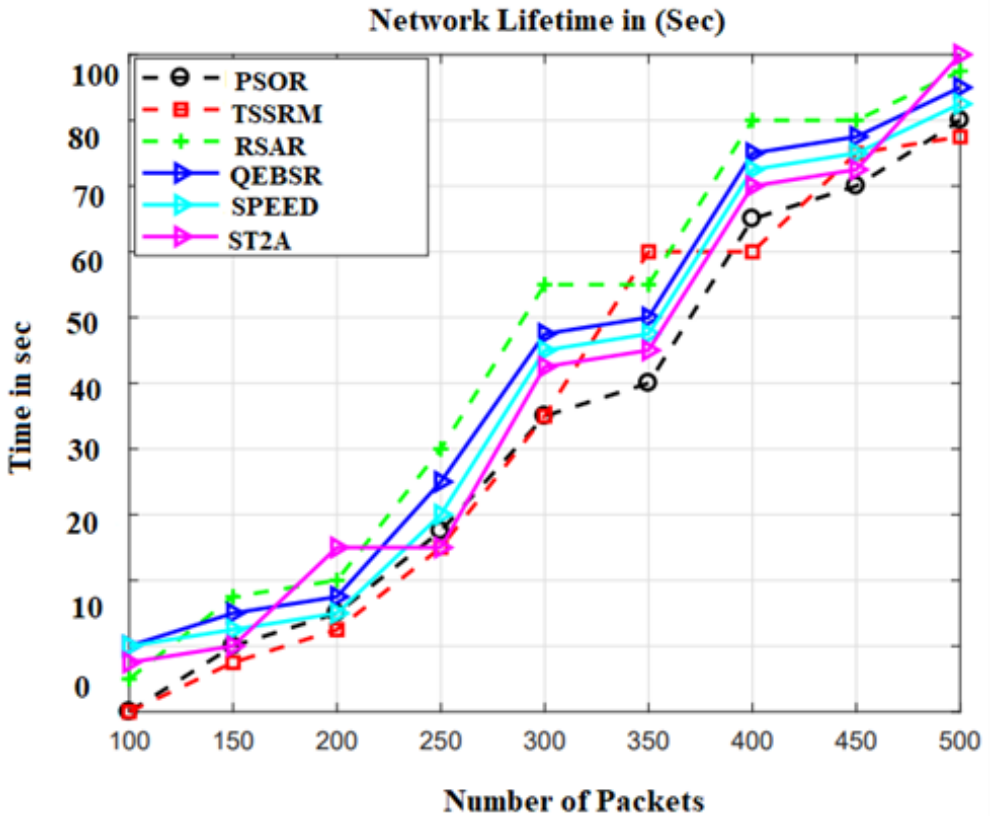

Figure 5 – Analysis of network lifetime

As depicted in *Figure 5*, an analysis was conducted on the network lifetime of a system comprising 39 individual units utilising the SPEED protocol. The results of this analysis show a significantly reduced level of network lifetime compared to the performance of several other established protocols. Specifically, the observed network lifetime under SPEED was lower than that experienced with ST2A, which recorded a consumption duration of 36 seconds. Furthermore, SPEED demonstrated a clear advantage over QEBSR, the energy consumption of which lasted 41 seconds. The analysis also indicates that SPEED outperformed RSAR, exhibiting a network lifetime of 45 seconds. Additionally, the network lifetime associated with SPEED was lower when contrasted with TSSRM, which resulted in a consumption duration of 50 seconds, and with PSOR, which showed a network lifetime duration of 58 seconds. This highlights the energy efficiency benefits of employing SPEED in this network lifetime.

Figure 6 illustrates the SPEED scheme, a novel approach for selecting cluster head nodes in a wireless sensor network. This method employs a multi-path routing strategy to ensure reliable communication while maintaining a manageable computational cost. With SPEED, cluster head selection and communication path establishment are completed in just 4.3 seconds. It effectively assigns each node under the suggestion of a cluster head. The primary objective of SPEED is to select optimal cluster heads and establish dependable links to designated sinks. In contrast, other protocols demonstrate longer execution times: PSOR requires 16 seconds, TSSRM and RSAR take 14 and 11 seconds, respectively, while QEBSR finishes in 9 seconds. Additionally, SPEED has significantly lower control overhead than ST2A, which takes 7 seconds.

Figure 7 illustrates the proposed SPEED algorithm's throughput performance compared to existing algorithms. SPEED achieves a throughput of 97%, outperforming ST2A (95%), QEBSR (93%), RSAR (86%), TSSRM (82%) and PSOR (78%). These results indicate that SPEED significantly improves data transmission efficiency relative to the evaluated alternatives. The enhanced throughput suggests a more effective utilisation of network resources and potentially lower latency for data delivery when employing the SPEED algorithm.

The routing presentation produced by the dissimilar approaches is unrushed for the numerous methods and associated with other approaches in *Table 3*. The projected SPEED procedure produces high routing efficiency at multiple levels. The analysis was performed depending on the number of nodes in the network. The presentation of the trajectories generated by the different methods is restrained and likened through each simulation. However, the projected SPEED algorithm improves the routing efficiency more than other methods. By approximating routing based on multiple obstacles, routing efficiency is improved.

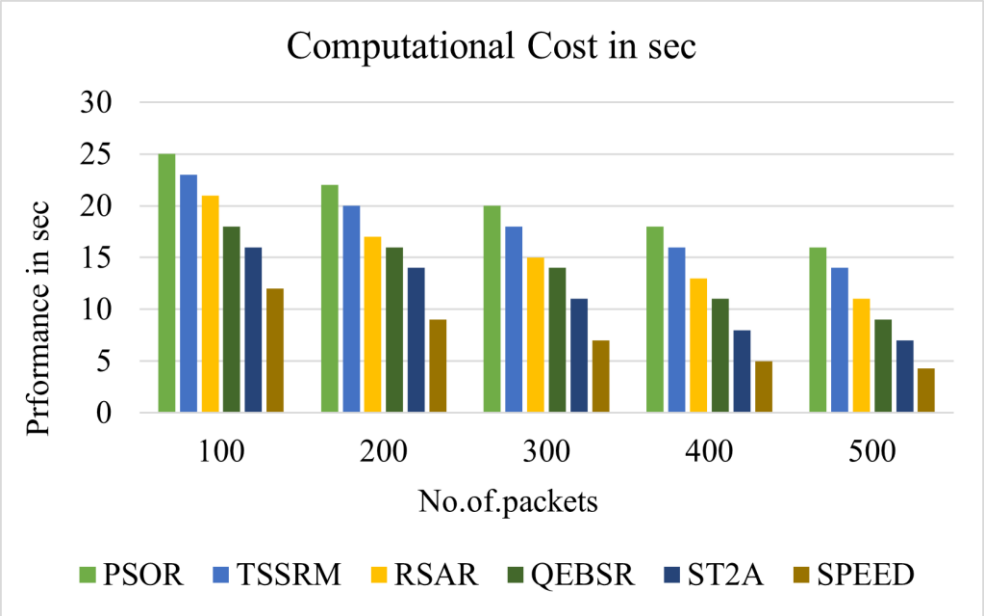

Figure 6 – Computational cost

Table 3 – Performance on secure routing performance

Secure routing performance in %			
Method	**50 nodes**	**75 nodes**	**100 nodes**
PSOR	65	71	76
TSSRM	68	75	80
RSAR	72	79	84
QEBSR	79	87	93
ST2A	85	92	94
SPEED	93	94	96

The routing of the nodes for dissimilar circumstances is restrained and associated with the consequences of other approaches. *Figure 7* above shows the results of routing performance analyses by various methods. Performance analysis is performed by varying the routing-controlled nodes based on the energy efficiency within the transmission range. For each case considered, the routing performance is measured and compared to the results of other methods. The proposed SPEED method performs highly in secure routing compared to other methods.

The packet loss rate produced by different techniques is measured using various methods, and the SPEED algorithm delivers the lowest PDR under other conditions, as shown in *Table 4*. The energy levels are considered based on the node support, improved routing efficiency, thereby reducing packet loss in all cases. The evaluation is done for different numbers of nodes in the network. However, the projected SPEED procedure achieves a lower PDR than the additional procedures.

The generated PDR ratio under different nozzle conditions was measured, and the MCNFA method produced the highest PDR, as shown in *Figure 8*. Routing based on multi-constrained feature approximation improves the routing efficiency, thereby reducing packet loss in all cases. The evaluation is done for the presence of different numbers of nodes in the network. However, the proposed SPEED algorithm achieves a lower PDR than the other algorithms.

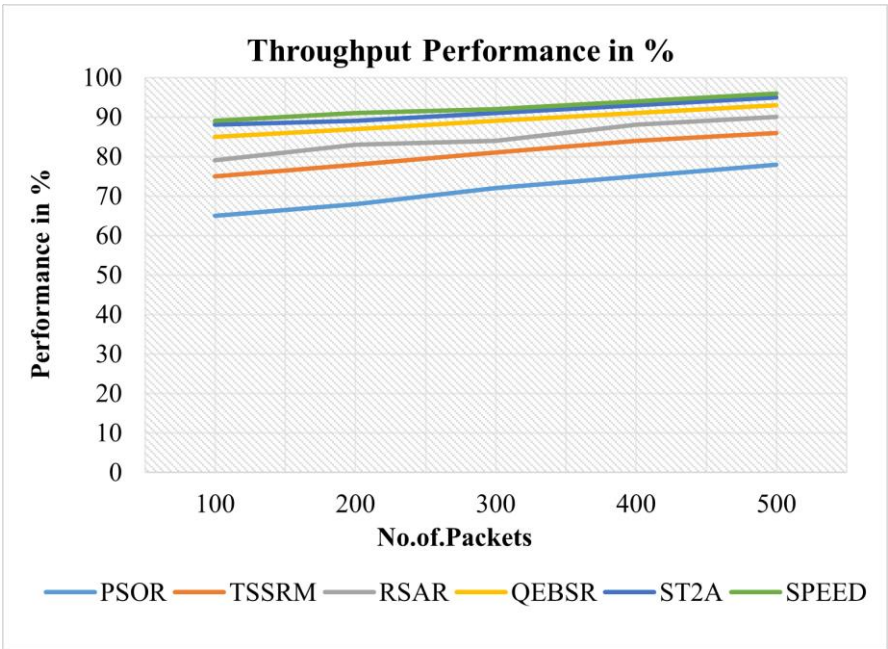

Figure 7 – Performance of throughput

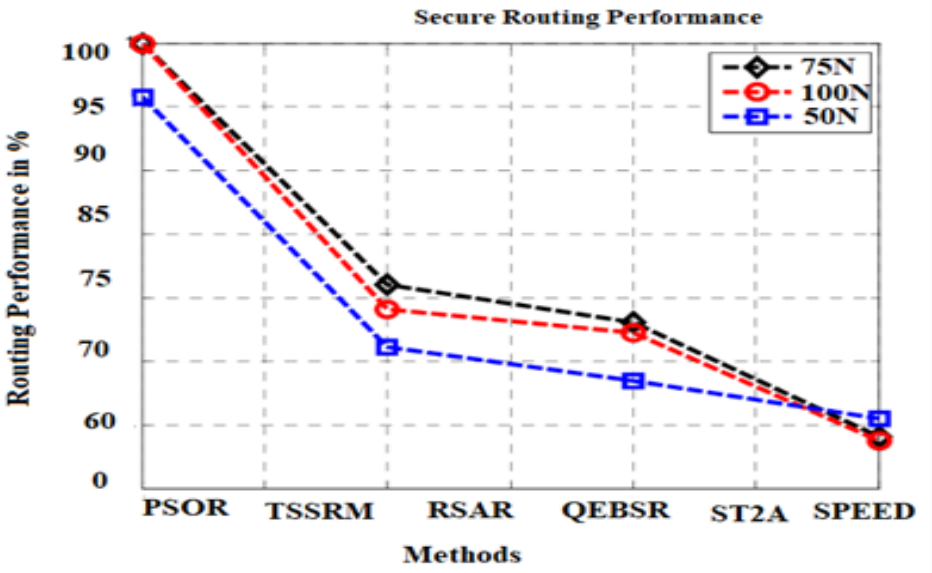

Figure 8 – Secure performance on routing

Table 4 – Comparison of packet drop ratio

Packet drop ratio %			
Method	**50 nodes**	**75 nodes**	**100 nodes**
PSOR	35	29	24
TSSRM	32	25	20
RSAR	28	21	16
QEBSR	21	18	12
ST2A	18	15	10
SPEED	12	10	8

The primary goal of this investigation is to quantify the delay rate generated by various methods under consideration. Calculating latency ratios to achieve will serve as a key metric for evaluating performance. The latency ratios are determined by systematically altering the number of nodes present within the network environment. These measured latency rates and their comparative analysis are comprehensively presented in *Table 5* for detailed assessment and examination. In contrast to the other techniques explored, the SPEED algorithm has been proposed as a potential solution.

Figure 9 illustrates the delay caused by different ways of transmitting data across different numbers of nodes. A multi-control network improves routing performance by predicting routes based on feature approximation, thereby reducing latency. However, in all cases, the SPEED algorithm enhances the performance and reduces the delay values more than the other methods. The SPEED method introduces less delay than other methods.

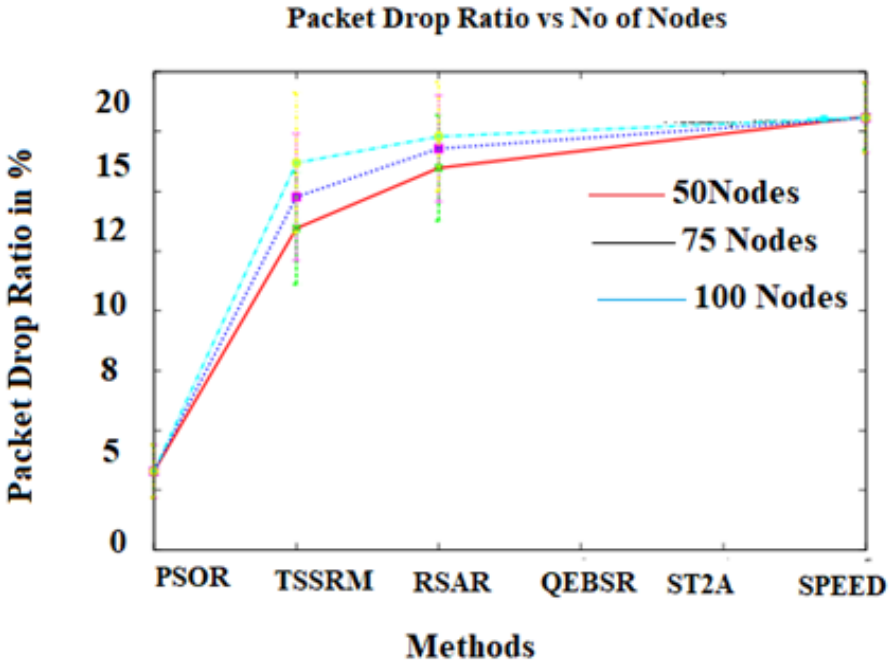

Figure 9 – Performance on packet drop ratio vs. the number of nodes

Table 5 – Performance on latency

Latency ratio in milliseconds			
Method	**100 nodes**	**150 nodes**	**200 nodes**
PSOR	95	89	84
TSSRM	82	76	70
RSAR	68	61	56
QEBSR	38	30	25
ST2A	25	22	19
SPEED	22	20	18

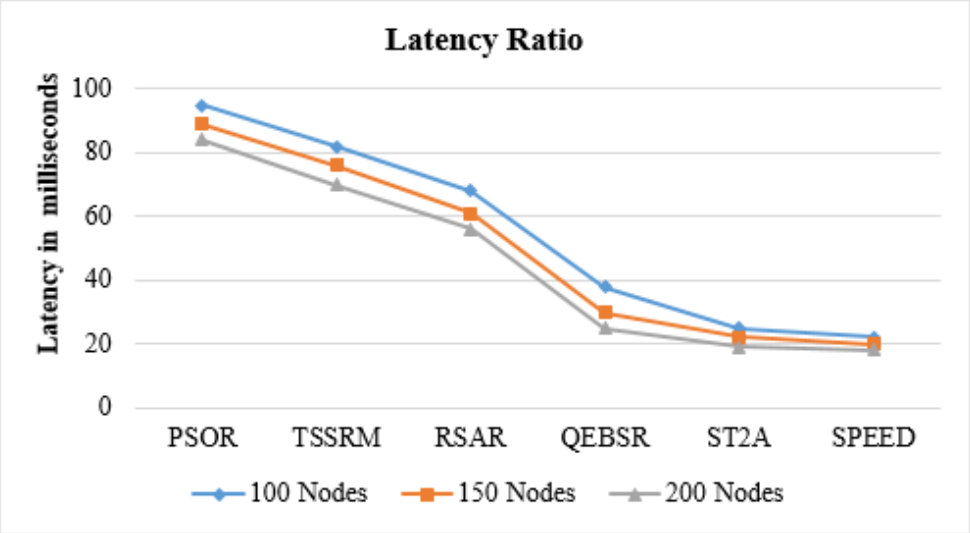

Figure 10 – Performance on latency

5. CONCLUSION

A comprehensive solution to overcome key challenges posed by mobile ad hoc networks (MANETs) in the transportation and intelligent transport systems (ITS) domain is provided by the secure proactive energy efficient determinant protocol (SPEED). SPEED extends the network's operational life by integrating energy-efficient routing with provable partition folding advanced encryption standard (PPF-AES) for better data security and significantly improved performance. The protocol achieves a 96.8% increase in throughput, an 18.2% decrease in latency and a 54.5% increase in energy efficiency, thus prolonging the network's lifetime. First, these advances improve the reliability of MANET operations, and second, they improve resource utilisation and reduce environmental effects, complementing the increasing need for sustainable transportation systems. The SPEED framework is secure and resilient for communicating with ITS and urban mobility applications. SPEED achieves a throughput of 97%, outperforming ST2A (95%), QEBSR (93%), RSAR (86%), TSSRM (82%) and PSOR (78%). These results indicate that SPEED significantly improves data transmission efficiency relative to the evaluated alternatives. Proactive design empowers it to become robustly adaptable to dynamic, decentralised environments in response to the ever-increasing need for reliable real-time data transmission. This adaptability is particularly useful for traffic management, modulation, control, vehicle-to-vehicle communication and smart transportation infrastructure. The findings create a promising avenue toward advancing sustainable and secure transport systems. This work lays the groundwork for future research and application of next-generation traffic management and mobility solutions. Numerous routing protocols have been introduced; however, significant challenges persist in older protocols. These challenges present ample opportunities for future developments aimed at creating robust routing algorithms that enhance the quality of service while meeting various routing metrics. Future research can focus on establishing a secure routing protocol in MANET by using the proposed optimization method for detection.

REFERENCES

[1] Sharma A, et al. Secure proactive routing protocol for mobile ad hoc networks. *International Journal of Network Security.* 2018;20(3):525-537.

[2] Li Q, et al. Energy-efficient proactive routing protocol for mobile ad hoc networks. *IEEE Transactions on Mobile Computing.* 2020;19(8):1890-1903.

[3] Yang S, et al. Particle swarm optimization-based routing algorithm for mobile ad hoc networks. *Journal of Computer Networks.* 2019;35(4):621-634.

[4] Zhang L, et al. PSO-based route optimization for energy-efficient data transmission in MANETs. *IEEE Transactions on Vehicular Technology.* 2021;68(5):4321-4334.

[5] Chen Y, et al. provably secure partition folding advanced encryption for MANETs. *ACM Transactions on Information and System Security.* 2019;22(2):301-315.

[6] Wang H, et al. Advanced encryption technique based on partition folding for secure data transmission in MANETs. *Journal of Wireless Communications and Mobile Computing.* 2022;25(6):1123-1135.

[7] Rajashanthi M, Valarmathi K. A secure trusted multipath routing and optimal fuzzy logic for enhancing QoS in MANETs. *Wireless Personal Communications.* 2020;112(1):75-90.

[8] Bin-Yahya M, Alhussein O, Shen X. Securing software-defined WSNs communication via trust management. *IEEE Internet of Things Journal*. 2021 Aug 5;9(22):22230–45. DOI: 10.1109/jiot.2021.3102578.

[9] Qin D, et al. Research on trust sensing based secure routing mechanism for wireless sensor network. *IEEE Access*. 2017;1(5):9599–609. DOI: 10.1109/access.2017.2706973.

[10] Rathee M,et al. Ant colony optimization based quality of service aware energy balancing secure routing algorithm for wireless sensor networks. *IEEE Transactions on Engineering Management*. 2019;68(1):170–82. DOI: 10.1109/tem.2019.2953889.

[11] Basha AR. Energy efficient aggregation technique-based realisable secure aware routing protocol for wireless sensor network. *IET Wireless Sensor Systems*. 2020;10(4):166–74. DOI: 10.1049/iet-wss.2019.0178.

[12] Liu J, et al. WSN node access authentication protocol based on trusted computing. *Simulation Modelling Practice and Theory*. 2022;117:102522. DOI: 10.1016/j.simpat.2022.102522.

[13] Al-Sadoon M, Jedidi A. A secure trust-based protocol for hierarchical routing in wireless sensor network. *International Journal of Power Electronics and Drive Systems/International Journal of Electrical and Computer Engineering*. 2022;12(4):3838. DOI: 10.11591/ijece.v12i4.pp3838-3849.

[14] Halidoddi G, Pandu R. A GOA based secure routing algorithm for improving packet delivery and energy efficiency in wireless sensor networks. *International Journal of Intelligent Engineering and Systems*. 2021;14(6):311–20. DOI: 10.22266/ijies2021.1231.28.

[15] Mehmood A, Lv Z, Lloret J, Umar MM. ELDC: An artificial neural network based energy-efficient and robust routing scheme for pollution monitoring in WSNs. *IEEE Transactions on Emerging Topics in Computing*. 2017;8(1):106–14. DOI: 10.1109/tetc.2017.2671847.

[16] Naghibi M, Barati H. SHSDA: Secure hybrid structure data aggregation method in wireless sensor networks. *Journal of Ambient Intelligence and Humanized Computing*. 2021;12(12):10769–88. DOI: 10.1007/s12652-020-02751-z.

[17] Zhang Z, Yang W, Wu F, Li P. Privacy and integrity-preserving data aggregation scheme for wireless sensor networks digital twins. *Journal of Cloud Computing Advances Systems and Applications*. 2023;12(1). DOI: 10.1186/s13677-023-00522-7.

[18] Sharmila N, et al. Secure key management and mutual authentication protocol for wireless sensor network by linking edge devices using hybrid approach. *Wireless Personal Communications*. 2023;130(4):2935–57. DOI: 10.1007/s11277-023-10410-7.

[19] Razaque A, Rizvi SS. Secure data aggregation using access control and authentication for wireless sensor networks. *Computers & Security*. 2017;70:532–45. DOI: 10.1016/j.cose.2017.07.001.

[20] Quoc DN, Liu N, Guo D. A hybrid fault-tolerant routing based on Gaussian network for wireless sensor network. *Journal of Communications and Networks*. 2021;24(1):37–46. DOI: 10.23919/jcn.2021.000028.

[21] Jurado-Lasso FF, Clarke K, Cadavid AN, Nirmalathas A. Energy-aware routing for software-defined multihop wireless sensor networks. *IEEE Sensors Journal*. 2021;21(8):10174–82. DOI: 10.1109/jsen.2021.3059789.