SEMARAK ILMU
PUBLISHING
202103268166(003316878-P)

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

SEMARAK ILMU PUBLISHING
Journal of ADVANCED RESEARCH IN APPLIED SCIENCES AND ENGINEERING TECHNOLOGY
ISSN 2462-1943

Energy Efficient Trust Based Data Communication using AODV Protocol in MANET

Tavanam Venkata Rao[1,*], V. Kumara Swamy[1], K. A. Karthigeyan[2], S. Gopalakrishnan[3], T. Kalaichelvi[4], S. Koteswari[5]

[1] Department of Electronics and Communication Engineering, Sreenidhi Institute of Science and Technology, Hyderabad-501301, Telangana, India
[2] Department of Electronics and Communication Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai-600062, India
[3] Department of Information Technology, Hindustan Institute of Technology and Science, Kelambakkam, Tamil Nadu 603103, India
[4] Department of Artificial Intelligence and Data Science, Panimalar Engineering College, Chennai, 600 123 India
[5] Department of Electronics and Communication Engineering, Pragati Engineering College, Surampalem, East Godavari District, Andhra Pradesh, India

ARTICLE INFO

Article history:
Received 7 May 2023
Received in revised form 13 August 2023
Accepted 19 August 2023
Available online 4 September 2023

Keywords:
Redundant Array Shifting Encryption (RASE); Wireless Sensor Networks (WSNs); Ad Hoc On-Demand Distance Vector (AODV); secure communication; Node Trust (NT); Direct Trust (DT); Path Trust (PT)

ABSTRACT

MANET is a collection of mobile devices and small-scale infrastructure networks built without centralized control. Each node in these networks collaborates with the other nodes to serve as a host or router. Because the detection medium contains information about distributed communication transmitted through Internet resources, security is an essential aspect of the wireless sensor network. Due to security flaws in network routing attacks, most existing principles control power resources and topology structure responsibility in fewer security dependencies, resulting in various intrusion factors due to data breaches. This paper presents a secure routing mechanism for wireless sensor networks based on trust aware routing protocol. Most constraints the routing protocol is resilient in the presence of malicious nodes activities monitoring on the routing levels based on response portability and energy constraints. By concerning energy level-based security, we propose a Trust Aware Energy Efficient Routing Protocol (TAE2RP) using secure routing data transmission for improving lifetime maximization in WSN. Initially the Resistance Support Factor (RSF) was estimated based on the packet drop ratio by handling the data resemblance of route containing information. Then the routing levels behaviors are analyzed through Secure Surf-Channel Multicast Routing Protocol (SSCMRP). To evaluate the trust factor on packet transmission rate using TAE2RP. In addition, Redundant Array Shifting Encryption (RASE) was applied to secure the data packets. The authentication policy was enhanced through Master Node Digital signing authentication. This optimized the cost of security routing by handling energy balancing mechanisms to improve the higher security by concerning authentication to attain higher security**.**

[*] *Corresponding author.*
E-mail address: vrtavanam@gmail.com

https://doi.org/10.37934/araset.32.1.390405

1. Introduction

Data interaction cloud be achieved by passing data packets between mobile nodes that cannot communicate directly. This is because the nodes only have a limited radio range. In contrast to other networks, MANET has a self-organizing dynamic network topology and unidirectional wireless connectivity and operates without structure [1]. MANETs are most commonly used in military operations, emergency and mobile communications, wireless access, and collaboration with sensor networks. For effective communication, it is necessary to establish appropriate routes between MANET nodes because each node is both an end system and a router. Finding a solution to this issue of routing, energy consumption, low-cost packet delivery, and network lifetime improvement is essential. A brand-new procedure known as a trust-aware routing protocol can boost the effectiveness of route optimization [2]. As a result, the packet transmission rate, network lifespan and energy consumption of nodes are enhanced. At first, the drag support factor was calculated using the packet loss ratio and the data similarity of the information-carrying routes. Security is improved by the Redundant Array Shift Encryption (RASE) procedure. Through these routing techniques, it is a process that uses a digital signature to authenticate itself. The longevity of the network is also increased. These reduce the cost of secure routing, improve security by focusing on authentication, and address energy-balancing mechanisms to achieve this. Because traditional routing protocols are established on the presumption of cooperation and a trustworthy environment between nodes, a MANET node can execute and cooperate without incident. In a physically hostile environment, attackers can quickly launch attacks by destroying some influential internal nodes. Network layer attacks are one of the main ideas, and secure routing is one way to avoid data transfer routing failures.

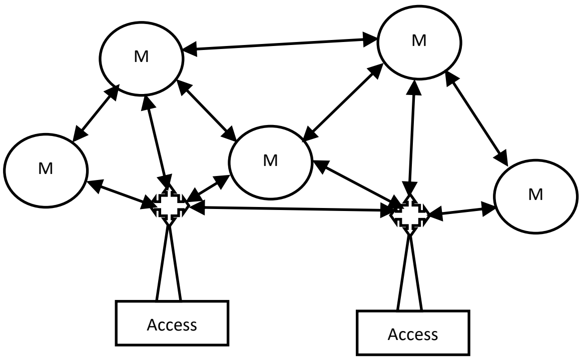


Fig. 1. General Architecture of MANET

Figure 1 define A MANET as a network of as many mobile devices as necessary to form a network. Support is not provided for any existing internet infrastructure or fixed stations. An access point (AP) has always provided communication support to each MANET node. The MANET access point connects the two nodes.

The figure shows that MS2 is now connected to MS4 instead of MS3, so other network nodes need to use this new route to send packets to MS2. Assume that every node in the graph is within the radio range of each other to resolve if all the nodes are switched off and within the radio range of each other. This contrasts the well-known single-hop cellular network model, which uses a fixed base station and a wired backbone to support wireless communication requirements between two mobile nodes. Another issue is the distinct operating modes of different nodes. While some other nodes are primarily static, others are more mobile. Much research has been done to evaluate the performance of nodes using different simulators because it is difficult.

The power level of each node is different. It slows down a little when sending and receiving packets, but a node will drop a package if it doesn't have enough energy to broadcast it. Due to the use of wireless media and a lack of infrastructure, communications can be easily disrupted or eavesdropped on, malicious agents can compromise nodes, and each node must carry out the measures required to detect intrusions in a distributed manner.

1.1 Contribution of This Work

i. Analyze and investigate AODV protocol to find vulnerabilities for active and passive attacks.
ii. Design and build efficient and secure routing protocols.
iii. Verified and validate the proposed routing protocols.
iv. Improving the security and trust values used for data transmission.

1.2 Motivation of This Work

Its efficient use in Mobile Ad Hoc Networks (MANETs) is still an open research problem, mainly due to the specific dynamics of the relevant environment and the need to exploit local considerations for efficient solutions.

2. Related Works

A network comprises a collection of nodes distributed in an environment so that each node can support user needs by reconfiguring itself. Reducing network traffic and extending the lifetime of a network are our new ideas for doing so. Using Hash Distance Calculation (HDC), propose a task in the network to copy packets at the node level. The results of these simulations, which support these analyses, demonstrate that the solutions to these two intermediate problems in a WSN environment are comparable. In addition, the advantages of the proposed charging policy in extending the network's lifespan are demonstrated in comparison to established procedures that use global knowledge.

Propose a framework for minimizing network management costs to boost each WBAN's network throughput and quality of service (quality of service). That will help address the issues of data propagation delay and rising network management costs. Opportunistic WBANs' dynamic connectivity, interference management, and data propagation costs are all aimed at being reduced by the proposed framework. Theoretically, have looked at how the proposed framework provides dependable data exchange over opportunistic WPANs. Compared to existing solutions, the simulation results demonstrate a significant improvement in network performance [3].

WSNs must take the shortest and smoothest routes to circumvent the timing and movement constraints they face. Bezier curves align the flyable path, and the Travel Sales Problem (TSP) is used to plan the shortest route. The proposed algorithm uses less energy, transmits packets at a higher rate, and collects data faster than the other options [4].

The workings of a reconfigurable innovative surface (RIS) provide specifics on various implementation options that use encounter surfaces and reflective arrays. Both implementations' channel models are discussed, and the possibility of getting accurate channel estimates is examined. Discuss how RIS optimization differs from the traditional MIMO array preceding, pointing out new problems and opportunities with this new technology. Lastly, it presents numerical proof that RIS can alter important MIMO channel properties [5].

The proposed anomaly detection method provides the best PI for brilliant meter readings of electricity consumers. Additionally, it employs the compositional idea of PI to address the instability caused by neural networks. To adjust the parameters of the neural network to the high complexity and variability of power user data, a brand-new and improved co-occurrence search-based optimization algorithm is developed. The proposed model's accuracy and performance are evaluated based on data from residential microgrids [6].

A new algorithm that combines the advantages of clustering strategies and compressed sensing (CS-based) schemes is proposed in this paper. The relationship between any two adjacent layers. To alleviate the "hot spot problem" and reduce energy consumption caused by CH role rotation, a third standby CH role (BCH) and the corresponding CH and BCH role rotation mechanism are also proposed [7].

After each global super round, global clustering is performed. As a result, the objective of HCSP is to develop a cluster task schedule that is more adaptable, energy-efficient, and scalable than GRBP. The most significant drawback of the clustering approach is its overhead, which is mitigated by this strategy [8].

Each sensor's availability on a WSN depends on the energy available to extend its lifespan. The issue is the price of producing electricity, as it is always a necessity. Because of this, it will be necessary to intelligently detect malicious or duplicate data while it is being transmitted through wireless sensor networks [9].

The nodes are carried by the cache, according to this algorithm. Find trustworthy trust relay nodes by utilizing node trust. Based on the trust level of the nodes, build a trusted network. For effective zone recovery, group modules of nearby trust zones together. The trusted community includes trusted nodes following the concept of edge nodes. By sharing and transferring data, edge caching reduces backbone network congestion [10].

Table 1
Literature Survey of MANET Protocols

Author	Title	Method used	Drawbacks
Haqiqatnejad *et al.,*	Energy-Efficient Hybrid Symbol-Level Precoding for Large-Scale mmWave Multiuser MIMO Systems	Energy-Efficient Hybrid Symbol-Level	Design issues for code-level precoding in downlink multi-user millimeter-wave (mmWave) multiple-input multiple-output (MIMO) wireless systems
Jia Wu *et al.,*	An efficient data packet iteration and transmission algorithm in opportunistic social networks	Efficient data packet iteration and transmission (EDPIT)	Increasing the data packet transmission between nodes can cause node death
Lin *et al.,*	Dynamic Control of Fraud Information Spreading in Mobile Social Networks		Fraudulent information control problem is an optimal control problem
Yaguang Lin *et al.,*	Incentive Mechanisms for Crowdblocking Rumors in Mobile Social Networks	Incentive mechanism based on the Stackelberg game for homogeneous control tasks.	It is difficult to find that most of the current control measures are centrally implemented by managers.

Certificate management is eliminated from our plan, and trusted resellers are not required to distribute keys for each node. When forming a group, a group of wireless nodes can negotiate keys simultaneously. Furthermore, our strategy is receiver-agnostic, allowing any sender to select any favourable group node as a receiver. Our method meets forward and backward security requirements, known security, authentication, and message confidentiality. Our plan's efficacy is demonstrated by performance evaluation [16].

The proposed algorithm has a much lower communication and computation overhead than published works. It also makes critical renewal possible while resolving key escrow issues. It is contrasted with several recently proposed key management algorithms. The proposed algorithm outperforms other algorithms, according to analysis. For more in-depth simulations, the NS2 simulator is also utilized. Perform large-scale network simulations to validate the analysis results and evaluate the proposed algorithm's performance [17].

Ineffective key management of protocol certificate keys, distinguished by node flexibility, is proposed for WSN communication security in this work. When new nodes join the cluster, CL-EKM makes efficient rekeying easier and ensures the confidentiality of the keys. By removing infected nodes, the protocol reduces the broad impact of a node compromise on the security of active communication links. The method is effective against various multi-hop wireless network security analyses [18].

2.1 Problem Statement

i. Link errors generate many control packets, consume network bandwidth, and decrease network density.
ii. Ineffective key management of protocol certificate keys, distinguished by node flexibility
iii. Lower communication and computation overhead than published works.

3. Proposed Methodology

This section expresses the proposed methodology for secure communication in MANET. Due to their dynamic nature, which causes nodes to move and become unstable, mobile ad hoc networks make it difficult to provide efficient and reliable routing. Despite this, nodes communicate with one another and exchange data with other nodes in their network's range. However, MANET nodes still participate in routing but fail to forward packets, affecting the protocol's performance. Additionally, the nodes must have sufficient power for the transmission to be successful. An AODV based on trust and power is implemented to route trusted nodes. The proposed system directs MANET to increase the network's lifetime, then optimizes network power consumption, analyzes network packet delay performance, optimizes MANET routing optimization, and enhances MANET data transmission security.

The proposed model work programs are discussed in greater detail in Figure 2. MANET's proposed model is depicted in the following diagram. Using trusted protocols, version optimization defines path optimization, packet delivery rate, power consumption, and network lifetime.

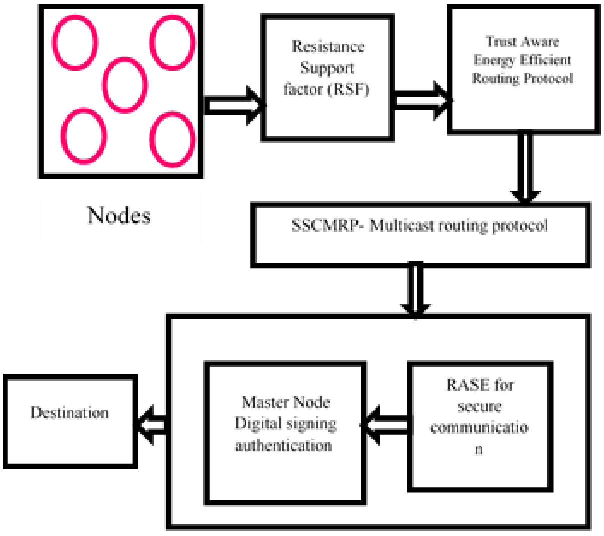

Nodes
Resistance Support factor (RSF)
Trust Aware Energy Efficient Routing Protocol
SSCMRP- Multicast routing protocol
RASE for secure communicatio n
Master Node Digital signing authentication
Destination

Fig. 2. proposed system Architecture

3.1 Network Topology

To extend the network's lifespan, energy metering considers how much each node uses in terms of services. Metrics for the network's topology enable load balancing to be improved and node locations to be better understood. The channel health metric safeguards the network from congestion attacks and builds tolerance for regular outages caused by poor channel conditions. A trust metric evaluates overall compliance and guards against coordinated attacks, while a reputation metric quantifies each specific contribution to network performance.

3.2 Resistance Support factor (RSF)

It uses the communication behaviour of the nodes to determine the node's trust value. A confidence value between 0 and 1 is given to each node. The confidence value for each node is initially set to 0.1. If a node is involved in many continuous transmissions of good packets, its trust value can rise rapidly or fall rapidly. The "2" trust value categories are used to examine each node's trust value in this context. A hybrid confidence valuation is a name given to this confidence assessment. In the Equation, the hybrid trust is represented by Eq. (1)

$$H_T = \sum(D_T + I_T) \tag{1}$$

Here, $\boldsymbol{H_{T\,is}}$ the hybrid network trust evaluation; $\boldsymbol{D_T}$ signifies direct trust; $\boldsymbol{I_T}$ symbolizes indirect trust. A hybrid trust is computed by combining direct and indirect components. Here, trust computation of trustor, j- trustee, $S_{(i,j)}$- hybrid mechanism, $S_{ij}{}^{D}$-direct trust made, $S_{ij}{}^{ID}$-indirect trust made, ζ- trust component Eq. (2). The direct belief calculation is done by direct observation.

$$S_{(i,j)} = (1-\zeta)S_{ij}{}^{D} + \zeta S_{ij}{}^{ID} \tag{2}$$

Here, s-time, δ-Delta, s_1-trust decay with changing time Eq. (3). The indirect trust evaluates the content within the correct confidence length.

$$S_{i,j}{}^{D} = \{_{\delta S_{ij}{}^{D_{s-s_1}}}^{S_{ij}{}^{D}} \tag{3}$$

Here, r-one-hop neighbor, m-node, i and j- Indirect trust evaluate value. Eq. (4).

$${S_{ij}}^{ID} = \{\begin{matrix} S_{r,m} \\ \delta {S_{ij}}^{D_{s-s_1}} \end{matrix} \qquad (4)$$

The p values for this algorithm's optimization of the packet drop rate are evaluated for routing optimization.

Packet drop ratio$p = \frac{1}{n}\int_{m-1}^{N}[p \in f(t,i,j,)]$ (5)

Eq. (6) p is the packet drop ratio, and n is the number of nodes. It calculates the packet delivery ratio$(i,j,)$. Another node should optimize the power consumption of one node. The proposed optimistic routing algorithm is contrasted with the existing system. The energy consumption of E decreased as a result of this method's evaluation of the values of E.

Energy consumption

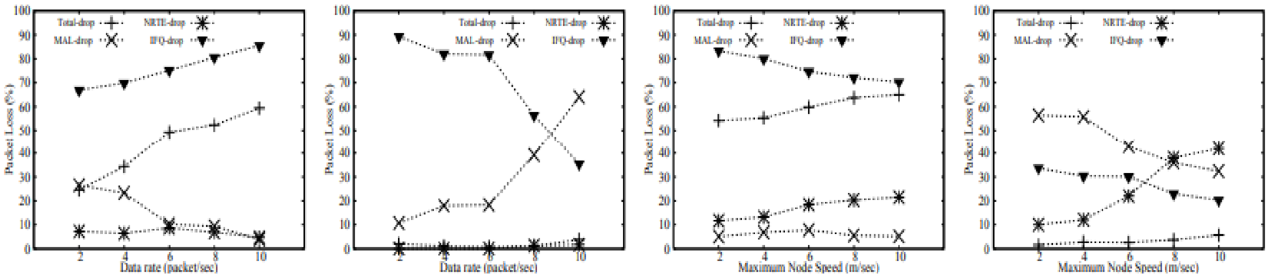
$$E = \frac{1}{N}\int_{m-1}^{N}\sqrt[2]{[p \in f(t,i,j,)]} \qquad (6)$$

Here, Energy consumption $E, \sqrt[2]{[p \in f(t,i,j,)]})$ is the computed energy consumption of the MANET. Overall Energy Consumption

The actual value of EC and the total power consumption of each node transmit, receive, forward, and discard operations can be obtained by summing up the power consumed in all operating modes within the simulated time. Here, m-no of node, a- total no of mobile node.

$$O_E = \sum_{a=0}^{m-1}(Energy\_Consumed\ \_by\_Node(a)) \qquad (7)$$

Figure 3 Shows that the packet loss due to increases with the data rate. DSR Protocol Effect of Increasing Data Rate on PDR. In contrast, OLSR has no such property or information about broken links at the source node. So, there will be more packet loss due to the absence of routing errors.



(a) Impact of data rate on Packet Loss rate (PLR)in OLSR (b) Impact of data rate on PLR in DSR (c) Impact of node speed on PLR in OLSR (d) Impact of node speed on PLR in DSR

Fig. 3. Impact of data rate and node speed on PDR

As shown in Figure 4 in this section, there are two modes of communication between A and B. Send data directly from A to B or relay it to node B. However, these methods result in two different energy consumption levels, so one must be higher. Sending a packet of data from A to B consumes less power than sending the same packet from C to B.

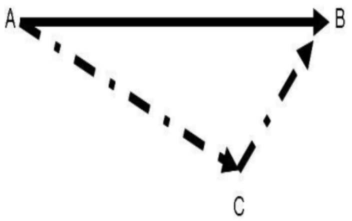


Fig. 4. Simple Energy Consumption in Multi hop Network

3.3 Trust Aware Energy Efficient Routing Protocol (TAE2RP)

This proposed method calculates the node trust centered on its communication range. It is useful and straightforward information about direct communication between nodes. There are direct trust types like path trust and node trust, which can be summed up as follows:

Based on its communication range, the mobile agent determines the confidence of the node. The node's trust is monitored and analyzed here to determine whether a node is forwarding or dropping packets. A measurement to ensure that the DPs (data packets) transferred by the Ni node are transmitted by the N j node. The node N_i's node trust in node N_j at time step t is signified as t $NT_{(i, j)}$ that enumerated as in Eq. (8)

Node Trust

$$(\mathrm{NT}^{\mathrm{i}}{}_{(\mathrm{i,j})}) = (\mathrm{W}_1 * \mathrm{R}_{\mathrm{cf}}) + (\mathrm{W}_1 * \mathrm{R}_{\mathrm{df}}) \tag{8}$$

The trust value of a node is evaluated by combining the opinions of its neighbors. Compute the node trust value (NTV) for the node. Here, i- node, n-no of neighbor.

$$NTV = [NNT(1) + NNT(2) + NNT(3) + \cdots . + NNT(N)]/n \tag{9}$$

Herein, $\mathrm{R}_{\mathrm{cf}}$and R_{df}signifies the control packet forwarding ratio and DP's forwarding ratio at step t; W_1 *and* W_2simply the assigned weight values of t $\mathrm{R}_{\mathrm{cf}}$and R_{df} , respectively correspondingly.

The path reliability of the DBs that is being sent is determined by using the path confidence value calculation. A weighted average of the trust values of the nodes along the path is used to define this value. The Equation is used to calculate the path confidence Eq. (10),

Path Trust

$$(PT_{(i.j)}) = \prod \mathrm{NT}^{\mathrm{i}}{}_{(\mathrm{i,j})} N_i, N_j \in N_i \ \rightarrow N_j \tag{10}$$

Here, $\boldsymbol{N_i} \rightarrow \boldsymbol{N_j}$ signifies that N_j is N_i's next hop. Lastly, the trust is articulated as in Eq. (11)

Direct Trust

$$D_{T(i.j)} = \sum(\mathrm{NT}^{\mathrm{i}}{}_{(\mathrm{i,j})} + \mathrm{PT}^{\mathrm{i}}{}_{(\mathrm{i,j})} \tag{11}$$

It is second hand information about the nodes that comes from a third party as a suggestion of trust. Finding the indirect confidence of node Nk from the common neighbour nodes between nodes Ni and Nj is necessary to improve the accuracy of the confidence value. The Equation depicts the indirect trust value of Nk, a neighbouring node in NJ Eq. (12),

Indirect Trust

$$I^{k}_{T(i,j)} = D_{T(i.k)} * \; D_{T(k,,j)} \tag{12}$$

The implicit confidence values of the nodes N_i and N_j about Nk are denoted by $\mathrm{I}^{\mathrm{k}}_{\mathrm{T(i,j)}}$ in this case; The direct trust of Ni in the node DT indicates Nk (i, k); The immediate trust that N j has in the node Nk is shown by DT$_{(k,\ j).}$ The trust information of all nodes provided between the SN and the DN is included in the direct and indirect trust values. Based on this fiduciary value, which is displayed in Table 2, the position of each node was determined.

Table 2
Node status based on trust values

Trust Value	Node Status
$D_T<0.5, I_T <0.5$	Malicious Node
$D_T= 0.5, I_T = 0.5$	Suspect Node
$D_T< = 0.5, I_T < =0.75$	Less Trustworthy Node
$D_T> = 0.5, I_T > =0.75$	Trustworthy Node

3.4 Secure Surf-Channel Multicast Routing Protocol (SSCMRP)

This stage the proposed SSCMRP algorithm is used to find the multipath for data transmission. Potential obstacles exist in these areas: open channels, the environment around them, and a lack of resources. A MANET is hindered in some way by each of these factors. For packets to reach their destination, the network's nodes can drop any box and alter the network's operations. There is a severe issue with packages being removed. Data loss and delays in the authentication and routing processes are possible outcomes. This proposed examines the variation in packet-dropping nodes, with varying numbers of nodes, while maintaining a constant working area and by altering the working room while maintaining an endless number of nodes. The analysis's output helps determine a region's optimal number of nodes. The network will function more effectively as a result of the effect of the current work. When one node is compared to another, the packet drops rate decreases. The trust routing algorithm that is being proposed is compared to the existing system.

$$\text{Maximization of network lifetime } L = \frac{1}{N}\int_{m+1}^{N}\left(\sqrt[3]{p \in f(t,i)}\right) \tag{13}$$

Here, Maximization of network lifetime L. This Equation is $\int_{m+1}^{N}\left(\sqrt[3]{p \in f(t,)}\right)$ i calculates the Maximization of the network lifetime of the MANET.

The route maintenance procedure uses time intervals to predict the node's response time, power level, and communication quality to determine its dependability. When an intermediate node transfers a DP to the subsequent node, the first node must determine whether its next-hop link has been broken. The reliability of each node is evaluated by focusing on its response time, power level, and communication quality. The thresholds for response time, power, and communication quality are assigned manually for verification. Any node that falls below the point in terms of power, communication quality, or response time sends a routing error message to the SN, as the Equation above demonstrates Eq. (14)

$$if\sum(E_{res},T_{res}C_q)_{node} < \sum E_{res},T_{res}C_q)_{Threshold} \tag{14}$$

$$Former\ node \rightarrow \text{Source node} \tag{15}$$

where $\sum(E_{res},T_{res}C_q)_{\,node}$ represents the node's current residual energy, response time and communication quality. $\sum E_{res},T_{res}C_q)_{Thershold}$Represents the assigned threshold energy, packet drop ratio and routing performance and improve security level. The route maintenance procedure boosts the Performance of MANET's routing procedure.

Algorithm steps for SSCMRP

```
Begin
    Initialize the candidate solution $\psi_j$ randomly
Determine the initial position using,
$\psi_{j=\psi_{min}} + (\psi_{max} - \psi_{min})$
Evaluate fitness for each solution using
$$F_{opt} = \left[\!\!\left[\begin{array}{c} max\sum_{n=1}^{d} PT(N_n, N_{n+1}) \quad \text{path trust} \\ max\frac{1}{N}\sum E_{res}\,\text{residual energy of each node} \\ min\sum_{n=1}^{d} PT(N_n, N_{n+1})\ \text{path disance between source and destination} \end{array}\right]\!\!\right]$$
$While\ I = 0\ to\ I_{max}\ do$

Sort the solutions in ascending order based on $F_{opt}$ and form group Determine step size for each shepherd using,

    $S_j = W * L_0^y(\psi_d - \psi_j) + W * L_0^y(\psi_k - \psi_j)$
    Generate new elements using
$\Psi_j^n = \Psi_j^0 + S_{s_j}$
$if(F_{opt}(\Psi_j^n) \geq (F_{opt(}\Psi_j^n)$
Sheep position =$\Psi_j^n$
Else
Sheep position =$\Psi_j^0$
End if
To estimate the best route for data transmission
    $f(t,i,j,) = \frac{1}{N}\int_{m-1}^{N} \sigma^{t-m}\, D_{T(i.j)}$
Replace entry in the routing table
End while
Return best routing path
End
```

Routers can automatically incorporate data from connected routers into their routing table with the assistance of the SSCMRP routing protocol. These protocols notify routers of any changes to the network's topology.

3.5 Redundant Array Shifting Encryption (RASE)

Before transmitting the packets from source node (SN) to destination node (DN), the proposed RASE method encrypt the information. The primary purpose of converting DPs into encrypted data is to prevent unauthorized access. The RASE key encryption algorithm is used in the proposed system. MANETS uses the RASE key encryption algorithm to make it possible to have multiple levels of security.

MANETS employs the RKE encryption procedure to implement a multi-level security. To begin, the RSA key is generated randomly by selecting the prime numbers. Please consider the prime numbers a and b, and determine their product Q using the formula Eq. (16)

$$Q = a * b \tag{16}$$

Then, choose '1' as an integer k that must be greater than '1' and less than (a-1) and (b-1). Then, a fixed pair of integers Q and k make up the force RK, denoted ask. Then, the secret key $\boldsymbol{K_S'}$ is calculated as the integers a, b, and$\boldsymbol{K_S'}$in Eq. (17)

$$K_S' = K^{R-1}(a-1)(b-1) \tag{17}$$

The RKE process begins once the key has been generated. Let's refer to DP's input as Pd. Using the uniform random assignment in Equation, a distributed transform encoder (DTE) is used in the encoding process to generate the seed Eq. (18).

$$\delta \rightarrow \alpha\mathrm{DTE}(P_D) \tag{18}$$

In this case, it denotes uniform randomization. Following the seed acquisition, which is centred on the RKE key and a random string, a conventional encryption method is used to encrypt the seed to generate the corresponding cypher text DP Pd using the RKE key and secret key, as shown in Eq. (19).

$$\delta = \mathrm{RKE}\ (p, k') \tag{19}$$

The δ⍰signifies the encrypted seed is denoted by suggests a random string; RKE represents the cryptographic hash function. Finally, as shown in Eq. (21), the ciphertext is obtained using seed and encrypted seed.

$$C(p_d)\text{=}(\delta + \delta)k_s' \tag{20}$$

The ciphertext $\boldsymbol{C(p_d)}$ is denoted by C Pd here. During encryption, the receiving side (authenticated users) receives the random string, encrypted seed, RKE key, and secret key. The original DP can be recovered using this random string, the encrypted source, the RKE key, and the secret key. Unauthorized users cannot access this ciphertext. Master Node Digital Sign Authentication ($MNDSA$)

$$\mathrm{MNDSA} = \sum \mathrm{C}(\mathrm{p_d}) \tag{21}$$

Herein, MNDSA digitally authenticates the user key encryption technology, thus all improve the security performance of RASE Key Encryption methods.

4. Result and Discussion

The result and discussion of the MANETs and node communication are based on a central system. Existing WSNs have route optimization problems and security balancing problems. It also affects network attacks significantly. The network lifespan and energy consumption of nodes, not to mention the packet transmission rate, both rises. Initially, the Resistance support factor was estimated based on the packet drop ratio by handling the data resemblance of a route containing information. The Redundant Array Shifting Encryption (RASE) process enhances the security levels. The overall function of the proposed system has been improved. The proposed approach of the Trust-Aware Routing Protocol has better. Table 3 displays that the simulation parameters outperform one of the measured analogue conditions, in which the proposed method's various parameters evaluate their performance.

Table 3
Simulation parameters of the proposed method

Parameters	Value
Network Area	100x100
BS Position	Indoor
Tool	NS2
Number of nodes	50
Simulation time	10mis
Network topology	Hybrid network
Bandwidth (Kbps)	200

The Network lifetime of MANETs in comparison to that of various routing protocols and algorithms is shown in Figure 5. The EECCTS protocol takes up to 85.5% of the lifetime, and the MIMO protocol takes up to 87.2% of the lifetime, the EDPIT protocol takes up to 93.2% of the lifetime, the TWR protocol takes up to 96.2% of the lifetime.

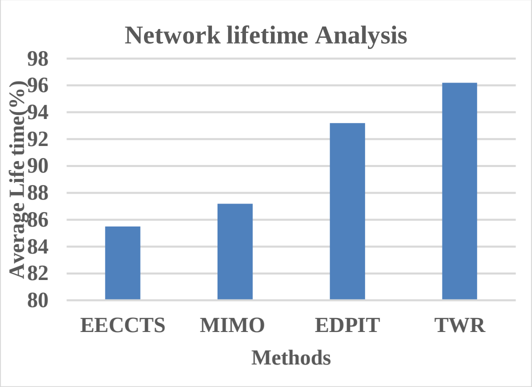


Fig. 5. Network Lifetime Improve

The power consumption of MANETs in comparison to that of various routing protocols and algorithms is shown in Figure 6. The EECCTS protocol takes up to 140 milliseconds for 200kbps, and the MIMO protocol takes up to 120 milliseconds for 200kbps, the EDPIT protocol takes up to 104 milliseconds for 200kbps. The TWR protocol takes up to 102 milliseconds for 200kbps.

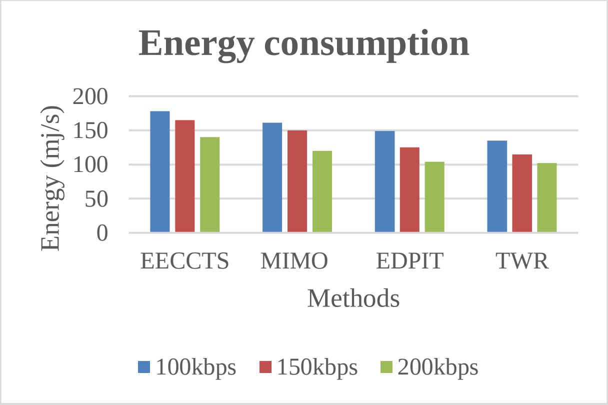


Fig. 6. Energy consumption rate analysis

The packet drop ratio of the MANETs is compared to that of various routing protocols and algorithms in Figure 7. The drop ratio for the EECCTS - protocol is 95.2%; The MIMO protocol has a drop ratio of 92.1 %, the EDPIT protocol has a drop ratio of 89.2 %, and the TWR protocol has a drop ratio of 87.4%.

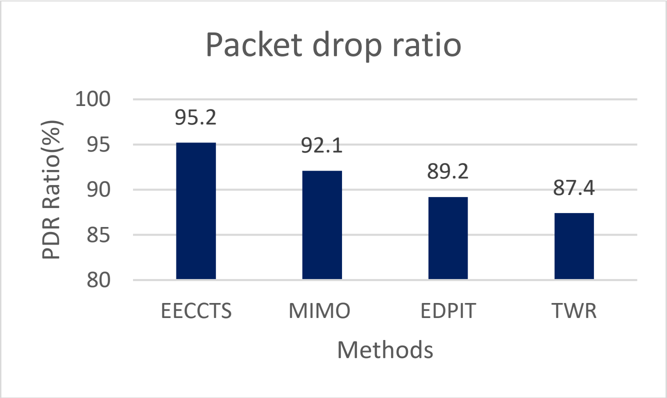


Fig. 7. Packet drop ratio

The latency bring about in information transmission at various number of nodes by different methodologies are plotted in Figure 8. The dormancy assessment is estimated when there are 15nodes, 25 nodes and 10 nodes in the reenactment. At each condition, the worth of idleness is estimated and introduced in Figure 8. The proposed **TWR** calculation has created less idleness in each experiment than different strategies.

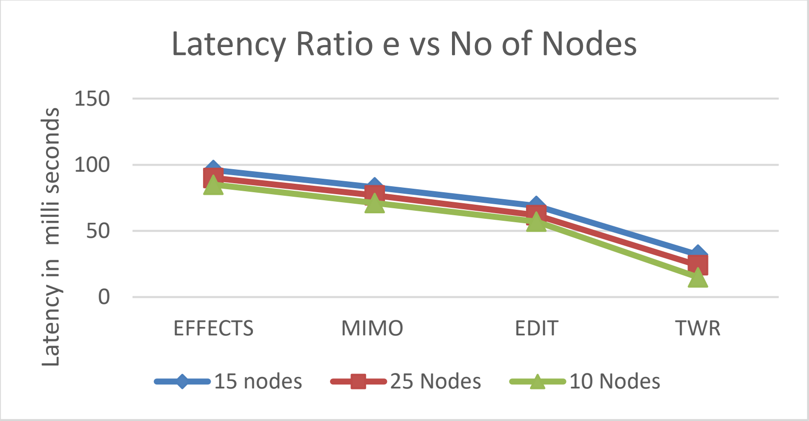


Fig. 8. Latency ratio

The proposed TWR algorithm's routing performance has been compared to other methods like EECCTS, MIMO, and the EDPIT -based protocol, as shown in Table 4 and Figure 6.

Table 4
Routing Performance Analysis

Time in	Routing Performance in (%)			
Sec	EFFECTS	MIMO	EDIT	TWR
120	19	23	26	32
140	26	29	32	42
160	48	52	58	69
180	78	82	88	93
200	92	95	96	97.5

Figure 9 defines Manet's routing performance compared to various routing protocols and algorithms. The EECS -based protocol has a routing performance of up to 200kbps of 93%; the MIMO protocol has a routing performance of up to 200kbps of 95%, the EDPIT protocol has a routing performance of up to 200kbps of 96%, and the TWR protocol has a routing performance of up to 200kbps of 97.5%

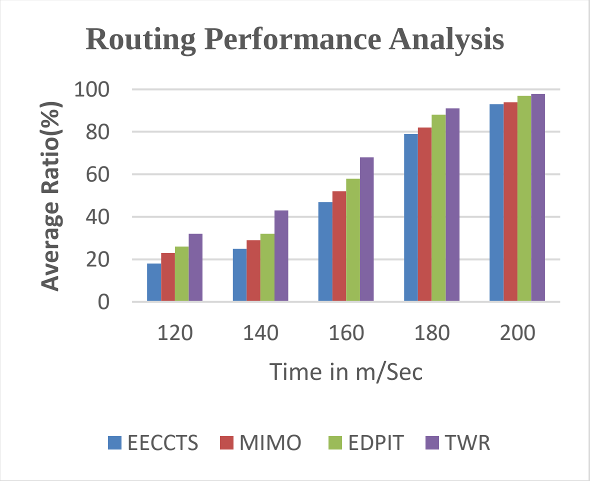


Fig. 9. Analysis of routing performance

Figure 10 discuss the security level performance of the MANET. The efficient Key Management (EKM) method performance is 85%, the ECC method essential performance is 89%, and the Secure and Receiver-Unrestricted Group Key Management (SRUGKM) actual performance is 92%. The proposed method of RASE key is 93% of the average calculated.

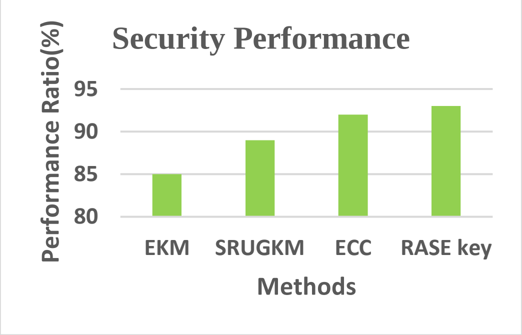


Fig. 10. Security fundamental performance analysis

5. Conclusion

This paper concentrated on a secure routing protocol to improve lifetime maximization for WSNs. Therefore, the proposed Resistance Support Factor (RSF) technique evaluates the packet loss ratio performance during data transmission. Furtherly identifies the node behaviour using Surf-Channel Multicast Routing Protocol (SSCMRP) method. Finally, the proposed Redundant Array Shifting Encryption (RASE) algorithm encrypts the packet during transmission for secure communication based on the trust factor rate. Finally, the proposed method got a simulation result of is packet drop ratio of 87.4%. Routing performance of up to 200kbps of 97.5%. The TWR protocol takes up to 102 milliseconds for 200kbps. Future research may address the issue of using a trust handshake-based approach to detect different attacks and improving security. Therefore, issues related to the implementation of detection methods to detect other types of attacks can be addressed, and future work is focused on reducing the overhead of maintaining trust metrics over time.

Acknowledgement
This research was not funded by any grant.

References

[1] Ramasamy, Karthick, Mohammad Hossein Anisi, and Anish Jindal. "E2DA: Energy efficient data aggregation and end-to-end security in 3D reconfigurable WSN." *IEEE Transactions on Green Communications and Networking* 6, no. 2 (2021): 787-798. https://doi.org/10.1109/TGCN.2021.3126786

[2] Tsoumanis, Georgios, Konstantinos Oikonomou, Sonia Aïssa, and Ioannis Stavrakakis. "Energy and distance optimization in rechargeable wireless sensor networks." *IEEE Transactions on Green Communications and Networking* 5, no. 1 (2020): 378-391. https://doi.org/10.1109/TGCN.2020.3039338

[3] Samanta, Amit, and Sudip Misra. "Energy-efficient and distributed network management cost minimization in opportunistic wireless body area networks." *IEEE Transactions on Mobile Computing* 17, no. 2 (2017): 376-389. https://doi.org/10.1109/TMC.2017.2708713

[4] Goudarzi, Shidrokh, Nazri Kama, Mohammad Hossein Anisi, Sherali Zeadally, and Shahid Mumtaz. "Data collection using unmanned aerial vehicles for Internet of Things platforms." *Computers & Electrical Engineering* 75 (2019): 1-15. https://doi.org/10.1016/j.compeleceng.2019.01.028

[5] ElMossallamy, Mohamed A., Hongliang Zhang, Lingyang Song, Karim G. Seddik, Zhu Han, and Geoffrey Ye Li. "Reconfigurable intelligent surfaces for wireless communications: Principles, challenges, and opportunities." *IEEE*

Transactions on Cognitive Communications and Networking 6, no. 3 (2020): 990-1002. https://doi.org/10.1109/TCCN.2020.2992604

[6] Kavousi-Fard, Abdollah, Wencong Su, and Tao Jin. "A machine-learning-based cyber attack detection model for wireless sensor networks in microgrids." *IEEE Transactions on Industrial Informatics* 17, no. 1 (2020): 650-658. https://doi.org/10.1109/TII.2020.2964704

[7] Wang, Quan, Deyu Lin, Pengfei Yang, and Zhiqiang Zhang. "An energy-efficient compressive sensing-based clustering routing protocol for WSNs." *IEEE Sensors Journal* 19, no. 10 (2019): 3950-3960. https://doi.org/10.1109/JSEN.2019.2893912

[8] Neamatollahi, Peyman, Saeid Abrishami, Mahmoud Naghibzadeh, Mohammad Hossein Yaghmaee Moghaddam, and Ossama Younis. "Hierarchical clustering-task scheduling policy in cluster-based wireless sensor networks." *IEEE Transactions on Industrial Informatics* 14, no. 5 (2017): 1876-1886. https://doi.org/10.1109/TII.2017.2757606

[9] Yuvaraj, D., M. Sivaram, and S. Navaneetha Krishnan. "Intelligent detection of untrusted data transmission to optimize energy in sensor networks." *Journal of Information and Optimization Sciences* 41, no. 3 (2020): 799-811. https://doi.org/10.1080/02522667.2019.1616910

[10] Wu, Xiaomin, Liu Chang, Jingwen Luo, and Jia Wu. "Efficient edge cache collaboration transmission strategy of opportunistic social network in trusted community." *IEEE Access* 9 (2021): 51772-51783. https://doi.org/10.1109/ACCESS.2021.3069992

[11] Haqiqatnejad, Alireza, Farbod Kayhan, and Björn Ottersten. "Energy-efficient hybrid symbol-level precoding for large-scale mmWave multiuser MIMO systems." *IEEE Transactions on Communications* 69, no. 5 (2021): 3119-3134. https://doi.org/10.1109/TCOMM.2021.3058967

[12] Wu, Jia, Zhigang Chen, and Ming Zhao. "An efficient data packet iteration and transmission algorithm in opportunistic social networks." *Journal of Ambient Intelligence and Humanized Computing* 11 (2020): 3141-3153. https://doi.org/10.1007/s12652-019-01480-2

[13] Lin, Yaguang, Xiaoming Wang, Fei Hao, Yichuan Jiang, Yulei Wu, Geyong Min, Daojing He, Sencun Zhu, and Wei Zhao. "Dynamic control of fraud information spreading in mobile social networks." *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 51, no. 6 (2019): 3725-3738. https://doi.org/10.1109/TSMC.2019.2930908

[14] Lin, Yaguang, Zhipeng Cai, Xiaoming Wang, and Fei Hao. "Incentive mechanisms for crowdblocking rumors in mobile social networks." *IEEE Transactions on Vehicular Technology* 68, no. 9 (2019): 9220-9232. https://doi.org/10.1109/TVT.2019.2930667

[15] Wang, Biao, Ge Chen, Luoyi Fu, Li Song, and Xinbing Wang. "Drimux: Dynamic rumor influence minimization with user experience in social networks." *IEEE Transactions on Knowledge and Data Engineering* 29, no. 10 (2017): 2168-2181. https://doi.org/10.1109/TKDE.2017.2728064

[16] Han, Wendie, Rui Zhang, Lei Zhang, and Lulu Wang. "A Secure and Receiver-Unrestricted Group Key Management Scheme for Mobile Ad-hoc Networks." In *2022 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 986-991. IEEE, 2022. https://doi.org/10.1109/WCNC51071.2022.9771870

[17] Gharib, Mohammed, Zahra Moradlou, Mohammed Ali Doostari, and Ali Movaghar. "Fully distributed ECC-based key management for mobile ad hoc networks." *Computer Networks* 113 (2017): 269-283. https://doi.org/10.1016/j.comnet.2016.12.017

[18] Kamble, Swapnil B., and Vivek V. Jog. "Efficient key management for dynamic wireless sensor network." In *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, pp. 583-586. IEEE, 2017. https://doi.org/10.1109/RTEICT.2017.8256663