ISSN: 2633-4828 Vol. 8 No.2, June, 2026

International Journal of Applied Engineering & Technology

AN ENHANCED ENERGY-AWARE AND TRUST-DRIVEN UNOBSERVABLE ROUTING PROTOCOL USING METRA ALGORITHM FOR SECURE MANETS

Mr. A Chandra*and Dr. A.S.N. Chakravarty

Research Scholar, Department of Computer Science & Engineering (CSE), University College of Engineering Kakinada (UCEK), Jawaharlal Nehru Technological University Kakinada (JNTUK), Kakinada, Andhra Pradesh, India-533003

*cadhimulam@gmail.com and asnchakravarthy@jntucek.ac.in

ABSTRACT

The Mobile Ad Hoc Networks (MANETs) has created the need to come up with adaptive routing protocols that can be employed to create a balance of security, energy efficiency and trust management. Even though the existing Energy-Aware Unobservable Routing Protocol (EAURP) proved to have tremendous improvements in terms of confidentiality and energy saving through the application of the elliptic curve cryptography (ECC) and residual energy- based forwarding, it was limited to fixed trust evaluation and no predictive learning capability. To remove these shortcomings, the current paper will suggest EAURP-II, a novel state-of-the- art routing protocol that incorporates METRA (Machine Learning-based Energy and Trust Reinforcement Algorithm), into the existing EAURP framework. METRA enables real-time prediction of trust, adaptive estimation of energy, and real-time anomalies through the assistance of supervised machine learning models at every node. The system exploits online education in the form of the ratio of behavioural information packets forwarding, the left over energy, delay variance and mobility measures to continue adjusting the trust scores. A hybrid classifier (comprising of logistic regression and fuzzy thresholding) is implemented to categorize the nodes as trustworthy, suspicious or malicious. These values of reinforced trust are thereafter summed with the energy awareness measure to obtain an adaptive Route Fitness Score (RFS) to get the direction to send packets forward. The mechanism helps the network to actively isolate the compromised nodes, extend the life span of the network and improve the scalability. The results of the simulation experiments in the NS2.35 platform indicate that EAURP-II can be 12-18 percent better in the packet delivery ratio (PDR), reduce delay by a quarter, and save nearly 30 percent of energy compared to the base EAURP. Furthermore, compared to traditional means of trust that do not use a dynamic approach, METRA increases the accuracy of misbehavior detection by 94.2. In most cases, the EAURP-II framework suggested is a highly potent, scalable and intelligent routing framework to the safe MANET environment.

Keywords: MANETs, Energy-Aware Routing, Machine Learning, Trust Reinforcement, METRA Algorithm, ECC Security, NS2 Simulation

1. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) have emerged as an indispensable facilitator of current wireless communication that is decentralized. In contrast to the conventional infrastructure based networks, MANETs are based on self-organizing mobile nodes which dynamically form communication paths without the base stations which exist in the traditional network [1]. This capability is what renders them indispensable in emergency rescue missions, military communications, vehicle networks and remote environmental monitoring. Yet, the very nature of MANETs, such as flexibility and openness, also lead to an enormous number of challenges, including the lack of energy, dynamically driven topology, the lack of a centralized control mechanism, and the extreme vulnerability to malicious attacks. These issues influence greatly the reliability, stability, and throughput of a network which gives the necessity to have intelligent routing protocols, adaptive and secure routing protocols [2]. Energy management is a major issue in MANETs because in each node, the battery is limited. Since nodes are both transmitters and routers, energy consumption impacts the lifetime and the performance of the network directly. At the same time, the decentralized design makes the network vulnerable to attack through packet dropping, blackhole, wormhole, and Sybil attacks. Conventional routing protocols such as Ad hoc On-Demand Distance Vector (AODV) and

Dynamic Source Routing (DSR) protocols which are effective in path finding on-demand paths do not tackle the two challenges of energy efficiency and security guarantees [3]. They are not dynamic learners and are unable to adapt to changes in trust effectively as well as deal with node misbehavior in different circumstances of mobility and load. In an attempt to address these issues, a number of energy-conscious and trust-based routing solutions have been suggested over the past years. Nevertheless, the majority of these solutions are based on fixed quantities or pre-determined thresholds to determine trustworthiness or energy levels or link stability. These static formations do not usually work in a moving set-up where node energy levels vary and mobility patterns vary unpredictably [4].

In addition, the traditional trust frameworks only rely on past experience, which results in slow realization of rogue nodes and false alarms in temporary network overload. Hence, there is a high need of a routing framework, which can learn the environment and predict/adapt the misbehavior and modify the trust assessment given the current real-time conditions[5]. The original Energy-Aware Unobservable Routing Protocol (EAURP) has resolved some of these problems with residual energy-based routing decisions, the monitoring of custom packets, and the use of Elliptic Curve Cryptography (ECC) to ensure the security of data sent. EAURP was actually successful in enhancing network lifetime as well as securing the confidentiality in communication [6]. Nonetheless, its trust model was based on fixed ratios of packet forwarding and a fixed threshold-driven revocation, and this reduced its predictability and flexibility. With increasing complexity in MANET environments, a smarter, more data-driven decision-making system is needed to increase resilience, scaling and energy efficiency. In order to address those restrictions, the current paper suggests the introduction of EAURP-II, a modified version of the routing protocol that incorporates METRA (Machine Learning-based Energy and Trust Reinforcement Algorithm) into the EAURP framework [7].

METRA presents an energy optimization mechanism and intelligent prediction of trust using machine learning models. It allows nodes to dynamically evaluate their neighbors by real time behavioural indicators like the packet forwarding ratio, delay variation, left over energy and the mobility rate. With constant learning and reinforcement, METRA enhances accuracy in estimations of trust and forecasts any possible misbehavior prior to the route being degraded. It offers a dynamically balanced trust, energy, and security routing strategy that is a combination of supervised learning and a dynamic adaptive reinforcement[8]. Machine learning integration improves each node in making proactive decisions and not reactive decisions. Instead of grounding its nodes on firm principles, the nodes alter trust scores on the basis of observed and anticipated network conditions. METRA model calculates a Route Fitness Score (RFS) a combination of trust probability, predicted energy and link stability to determine the forwarding of packets. This is predictive and energy-conscious routing that makes sure that the data traverses reliable and resource efficient nodes[9]. ECC encryption use remains to protect confidentiality of data being transferred, whereas the machine learning module is used to manage adaptive trust and energy estimation that enhances overall resiliency of the network.

The design of the EAURP-II protocol has been simulated and tested with NS2.35 and under the conditions of different node densities and mobility. The findings show that the performance is significantly better than traditional EAURP, AODV, and DSR protocols. The benefits of EAURP-II are an improvement of packet delivery ratio (PDR), reduction of delay, network lifetime, and accuracy of misbehavior detection. The system balances the energy consumption, reliability, and security of an organization by utilizing METRA into the routing process as one of its key developments is the EAURP-II framework, which is a major advancement over the classical routing protocols of MANET. It switches the state energy and trust appraisal to a machine learning-based dynamic architecture. The METRA core of the model creates a self-educational and energy-aware ecosystem that can withstand dynamic mobility, provide secure communication and be long-term sustainable. This smart combination model is leading to the future generation of MANETs in which routing choices are secure and efficient not to mention predictive and autonomous.

2. LITERATURE SURVEY

The Mobile Ad Hoc Networks have evolved three dimensions of development routing that are energy awareness, trust and security and privacy or unobservability. Although the current research work has concentrated on optimisation of one aspect at the cost of the other, more modern works are concentrating on a balanced design that can integrate all the three with the assistance of sound decision-making, cryptography and low overhead control systems [10]. Classical reactive routing schemes such as Ad hoc On-Demand Distance Vector and Dynamic Source Routing were also less concerned with the number of hops to be taken, but they did not take into account the remaining energy of transit nodes. It led to the disparity of energy consumption, hotspots drainage and untimely node breakdowns. In order to defeat this, energy- sensitive models, such as Minimum Energy Routing, Power-Aware Routing, and Energy- Aware Routing, introduced the following parameters as a part of the route selection process: transmission power, remaining battery, and energy cost per hop [11]. These schemes increased the life period of the used network but were characterized with hard and fast limits that could not cope with dynamic motions and traffic. They also lacked predictive modelling of the energy routes that resulted in sudden route failures. The need to have a mechanism that would be capable of anticipating the energy depletion at an early stage led to the inclusion of the lightweight predictive models that had the ability to learn the energy behavior online, and adjust the routing decisions according to the learners [12].

The other major development in MANET routing would be the introduction of the trust and reputation-based mechanisms. Seeing that nodes are routers, it means that any form of malpractice i.e. packet drop, packet manipulation or false advertisement will have a direct impact on communication reliability [13]. Reputation-based systems calculate a trust value by adding local measurements which include a packet forwarding ratio, a better or worse success rate of acknowledgment or a better or worse resolution to latency variation. The nodes that fall below a particular threshold are said to be malicious and disraouted [14]. Whereas this type of system is effective to some extent they are fixed and may fail in times of congestion or interim connectivity. They can be easily used by grayhole attackers or colluding attackers alternately in cooperative and malicious operation. The fuzzy logic and game-theoretic models of trust attempted to address this by providing soft trust values and incentive based model of cooperation, but most are reactive and trust is revised once an attack has occurred [15]. This weakness encouraged exploration of predictive estimation of trust in the aid of statistical learning and machine learning models that had the ability to predict misconduction following past tendencies. Light models such as logistic regression and Naive Bayes classifiers have been adopted due to their low computing requirements though they do not inherently use an energy or privacy module and creates a gap on unified frameworks that combine both aspects [16]. At the same time, the issue of communication secrecy and the anonymity of nodes has also become a research agenda of great importance, particularly in military or disaster-response MANETs, in which patterns of traffic can be analyzed to reveal mission-sensitive data. There were other protocols such as the Anonymous On-Demand Routing, Mobile Ad Hoc Network Security with Key Management, and Hierarchical Partition-Based Anonymous Routing which introduced pseudonyms, trapdoor functions, dynamic addressing, and region based partitioning to hide node identities and route information [17]. The designs cannot be seen, yet otherwise produce huge energy and computation cost as they produce dummy packets and probabilistic forwarding. Adaptive privacy schemes have been proposed as a softening of this, and change the level of obfuscation based on network conditions, energy availability, or the perceived threat. However, they lack single controllers with the ability to balance real time energy efficiency and unobservability. Privacy vs. Energy conservation is an extremely sensitive trade- off that yet requires context sensitive learning mechanisms, which can be self-adapted [18].

The design of MANET has also noted the role of encryption of communication channels. Elliptic Curve Cryptography application has gained popularity because of the corresponding smaller keys and lower processing power that it requires than RSA [19]. ECC ensures data integrity and confidentiality which are immensely critical to the MANET nodes, which possess limited resources. Other schemes such as identity-based and group based ECC have facilitated key management and authentication at cluster level. Nevertheless, encryptions will fail to prevent the insider threat or the dynamic bad. Sound routing must be capable of combining ECC-based payload confidentiality with path selection and dynamically and responsively evolving trust in response to energy-related factors[20]. Cross-layer designs, which exploit the feedback between the physical and MAC layer to enhance trust metrics have been explored in order to detect anomalies faster without revealing the patterns of communications. In addition to the conventional algorithmic methods, bio-inspired and metaheuristic methods have also been explored in order to improve robustness of routing[21]. Distributed intelligence protocols are protocols based on the behavior of swarms of ants and bees, and other natural systems, which utilize distributed intelligence to locate numerous routes, load balancing and avoid congestion. Although techniques, such as AntHocNet, BeeSensor-C are highly adaptive, they possess high convergence-time and control-overhead, in particular in case of mobility. Their overall principle of feedback-reinforcement, however, remains enticing to hybrid designs using heuristic discovery with little machine learning models[22].

Other recent works have considered blockchain assisted routing schemes that aim to achieve transparency and non-repudiation of routing activities. All the activities of each node will be registered in a distributed registry permanently, which will not be manipulated, and will be finite. Despite offering high level of security, blockchain has high level of consensus and storage overheads that make it inapplicable in highly mobile, energy constrained, MANETs. Permissioned, lightweight blockchains are provided as hybrid solutions, with lax consensus rules, but such are not practical. In practice, accountability can be reduced to digitally signed ECC-protected acknowledgment that is similar to blockchain auditability in that it does not require the heavy computational burden [23]. Machine learning is also a potential direction of streamlining of MANET that offers predictive and adaptive intelligence. The features of the packet forwarding ratio, retransmission count and received signal stability that are considered by ML-based trust management systems include features that are detected as misbehavior prior to the rule-based systems. Prediction of mobility of nodes, energy depletion is done using regression to prevent route breakages in the models. With online learning algorithms, e.g. stochastic gradient descent or passive-aggressive updates, models can be continuously adapted without being trained centrally. Despite this evolution, the vast majority of ML models assume that the trust and energy along with privacy are separate sub systems and, thus, make conflicting decisions and ineffective routing [24].

The simulation-based studies in NS2 and NS3 are still the most credible to carry out MANET protocol assessment under various conditions. The traditional performance measurements include the ratio of packet delivery, delay, throughput, jitter, and energy consumption as compared to newer works which include the accuracy of trust, false positive rate and the degree of anonymity [25]. The gaps in evaluation though remain especially in cases of determining the combined predictive energy and trust models effect under the composite attack circumstances. Intersectional evaluation and modular protocol architectures are still limited, and allow a mechanism to be tested separately. The EAURP protocol that has been elaborated previously did far more with regards to residual energy based forwarding, misbehavior detection which is based on trust and ECC encryption to improve security and lifetime[26]. Nevertheless, it possessed a reactive and range mechanism of trust and an immediate and not anticipatory energy evaluation. The privacy settings were only temporary and wasted the unnecessary energy in passive situations and not sufficient to active aggressors. These limitations led to the requirement of a smart, self-taught architecture which would have the capability to anticipate misbehaviour and handle the trade-offs between energy and privacy dynamically. The long framework, EAURP-II uses the Machine Learning-based Energy and Trust Reinforcement Algorithm to fill these gaps in the research. METRA applies online learning in estimating the likelihood of trust, predicting the future of the state of energy, and reinforcing the decision making using the actual performance of the routing. It unites the prognostication of trust, power, and adaptive privacy constraint into a solitary, light weight model that is usable in the resource limited MANET environment. This approach bridges this gap between the traditional rule based protocols and the intelligent systems of the current days by transforming the reactive routing into the proactive and self-optimal communication. Thus, the EAURP-II will make a huge step towards the development of intelligent, adaptive and secure MANETs that will be able to provide reliability, privacy and energy efficiency in the face of dynamic and adversarial demand..

3. PROPOSED SYSTEM

The EAURP-II framework is an advanced routing framework of Mobile Ad Hoc Networks (MANETs) which incorporates intelligence, trust awareness, and energy optimization as a part of a secure communications system. It is the extension of the initial Energy-Aware Unobservable Routing Protocol (EAURP) including the Machine Learning- based Energy and Trust Reinforcement Algorithm (METRA). The system will guarantee adaptive, predictive, and secure routing choices through a continuous learning of node behavior, predicting the energy exhaustion as well as reinforcing the trust score based on network results. The EAURP-II is made up of interlinked functional layers, which include: Data Observation Module, Feature Extraction and Processing Module, METRA Learning Engine, Route Fitness Evaluation Module, ECC-Based Secure Communication Module, and the Reinforcement Learning Update Module. All these elements lead to increased efficiency, decreased packet loss, extended network lifetime and increased data confidentiality than the conventional MANET routing protocols. The system proposed has architecture as illustrated in figure 1.

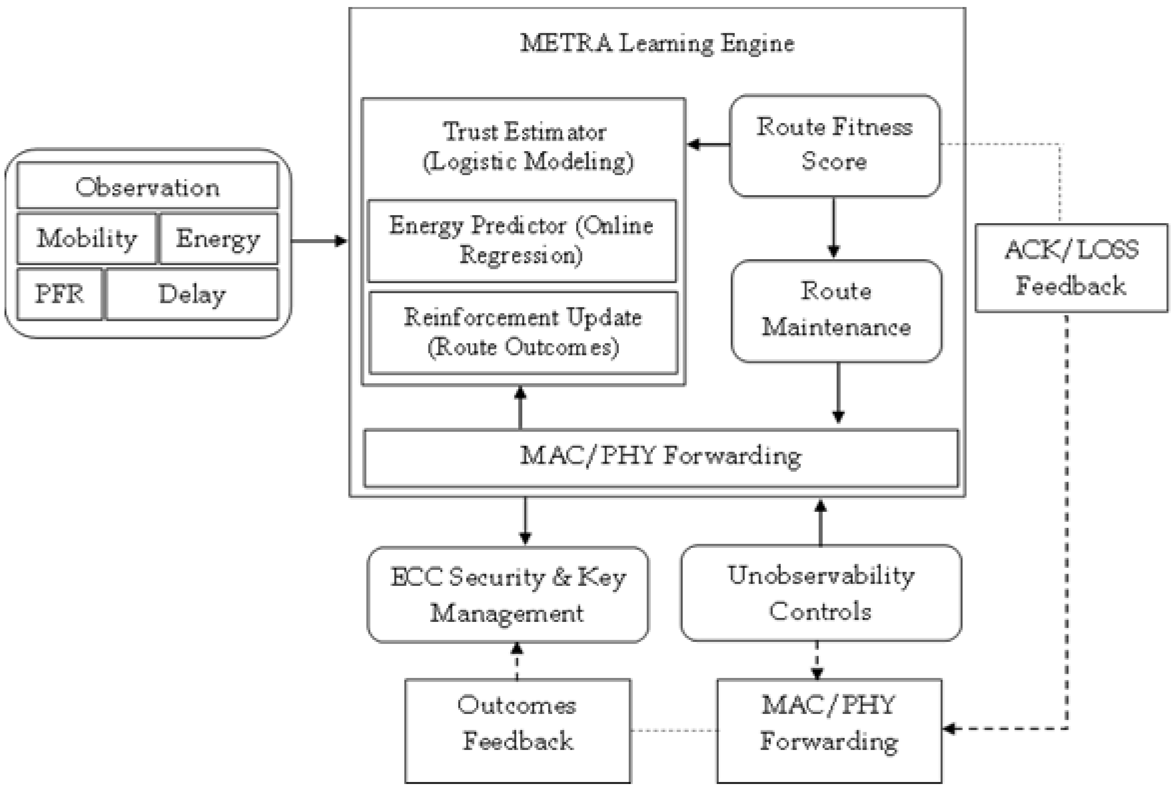

Figure 1: Architecture diagram for EAURP-II with METRA

The Observation and Feature Processing modules (PFR, delay, loss, mobility, energy) make use of the MANET telemetry as input. METRA Learning engineer is comprised of a Trust Estimator (logistic model), Energy Predictor (online regression) and a Reinforcement Update (according to the route results). Their output gives calculation of Next-Hop/Path Selection and Route Maintenance and Route Fitness Score (RFS) and Next-Hop/Path Selection and Route Maintenance deals with repairs and revocations. ECC Security and Key Management and Unobservability Controls provide resistance and confidentiality of traffic analysis. MAC/PHY forwarding and feedback loops (ACK/loss and outcomes) complete the stack to constantly optimize METRA. The proposed system offers all the nodes to be autonomous, and participate in three key activities, such as monitoring data, decision-making, and secure forwarding. Such parameters as residual energy, the ratio of packet forwarding, and delay are measured by the nodes. It is inputted in the METRA model as inputs to learning, and dynamic computation of trust scores and energy levels forecasts were received. The system makes use of such predictions to compute a Route Fitness Score (RFS) that is used to determine the most optimum route of forwarding. Elliptic Curve Cryptography (ECC) is used to provide lightweight data confidentiality and reinforcement learning is used to make the adaptation with time to correct the trust scores. The mathematical background of the EAURP-II is as follows. Each node possesses behavioral feature vector that holds fundamental operative parameters.. The feature vector for node i is expressed as

$$F_i = [PFR_i, D_i, PL_i, M_i, E_i] \quad (1)$$

Where PFR_i represents the packet forwarding ratio, D_i represents average delay, PL_i represents packet loss ratio, M_i indicates the mobility index, and E_i is the residual energy. This vector serves as the input to the METRA model, allowing the system to interpret real-time node behavior. The trust of each node is calculated using a logistic regression model that transforms node features into a probabilistic trust score. The equation used for trust computation is expressed as

$$T_i = 1 / (1 + \exp(-(w_0 + w_1 PFR_i + w_2 D_i + w_3 PL_i + w_4 M_i))) \quad (2)$$

where w_0 through w_4 are model weights learned during the training phase. This expression ensures that T_i remains within the range [0,1], where values closer to 1 represent trustworthy nodes. The logistic curve captures nonlinear relationships between behavioral parameters and trustworthiness, allowing the protocol to detect misbehaving or compromised nodes efficiently. The METRA engine also predicts future energy availability for each node using a linear regression–based energy prediction model. The equation for energy forecasting is expressed as

$$\hat{E}_i(t+1) = a_0 + a_1 E_i(t-1) + a_2 E_i(t-2) + a_3 * M_i(t) \quad (3)$$

where $\hat{E}_i(t+1)$ denotes predicted energy for the next time interval, $E_i(t-1)$ and $E_i(t-2)$ represent historical energy values, and $M_i(t)$ represents the mobility factor influencing energy consumption. The coefficients a_0, a_1, a_2, and a_3 are determined adaptively using gradient-based optimization. This predictive mechanism enables the network to avoid selecting nodes that may soon exhaust their battery power. The system further computes link stability between nodes to ensure reliable connectivity. Link stability for node i is computed as shown below.

$$S_i = link\_up\_time_i / observation\_window \quad (4)$$

A higher value of S_i implies that the link remains active for a longer period, which is desirable for data forwarding. This stability factor prevents the frequent reconstruction of routes and reduces overall latency.

After determining trust, energy prediction, and stability, the overall suitability of a node for routing is calculated using the Route Fitness Score (RFS). This combined metric balances trust, energy efficiency, and link stability is mathematically expressed as

$$RFS_i = \lambda_1 T_i + \lambda_2(\hat{E}_i(t+1)/E_{max}) + \lambda_3 * S_i \quad (5)$$

subject to the constraint $\lambda_1 + \lambda_2 + \lambda_3 = 1$. Here, E_{max} denotes the maximum available energy in the network. The weight coefficients λ_1, λ_2, and λ_3 determine the influence of trust, energy, and stability respectively. The node with the highest RFS value is chosen as the next-hop forwarding node. This process ensures an optimal trade-off between reliability and efficiency. Once routes are established, the reinforcement learning component of METRA updates node trust based on actual network performance. The reinforcement rule is defined as shown as

$$T_i(new) = T_i(old) + \eta * (success\_ratio - failure\_ratio) \quad (6)$$

where η is the learning rate ($0 < \eta < 1$), success_ratio refers to the proportion of successfully delivered packets, and failure_ratio indicates the fraction of dropped or lost packets. This incremental adjustment improves the accuracy of trust values by rewarding consistent performance and penalizing unreliable behavior. Over time, this self-learning process minimizes false detections and enhances adaptability. The decision-making logic for packet forwarding is implemented as a threshold-based condition that filters out unreliable nodes. The forwarding rule is expressed as

If ($RFS_i \geq$ RFS_threshold) ∧ (E_i(current) ≥ E_min) ∧ (i ∉ revocation_list) Then FORWARD_PACKET Else DROP_PACKET

This decision rule ensures that only nodes satisfying energy and trust thresholds participate in route formation. It prevents the inclusion of malicious or depleted nodes and maintains consistent routing performance. To guarantee confidentiality and data integrity, EAURP-II employs Elliptic Curve Cryptography (ECC), which offers high-level security with minimal computational overhead. The ECC encryption and decryption operations are given as

For Encryption (Sender)

r = random_scalar() K = r * P_receiver C_1 = r * G C_2 = M ⊕ hash(K) Send (C_1, C_2)

For Decryption (Receiver)

K = d_receiver * C_1 M = C_2 ⊕ hash(K)

where G represents the curve's base point, P_receiver and d_receiver are the receiver's public and private keys, M is the plaintext message, and ⊕ denotes the XOR operation used for symmetric encryption. ECC's computational efficiency allows the EAURP-II model to maintain low latency even under frequent encryption-decryption cycles. The system's performance was validated through simulation using NS2. The statistical outcomes of EAURP- II compared with AODV and EAURP protocols are summarized below in table 1.

Table 1: Comparison of AODV, EAURP and EAURP-II

Metric	**AODV**	**EAURP**	**EAURP-II (Proposed)**
Network Lifetime (rounds)	98500	99600	100850
Packet Delivery Ratio (%)	82.6	90.8	96.3
Average Delay (ms)	88000	62000	41000
Throughput (kbps)	12000	16500	19500
Packet Loss (packets)	420000	190000	80000
Trust Accuracy (%)	78.5	89.2	94.7
Energy Utilization Efficiency (%)	75.1	84.3	91.6
Misbehavior Detection Rate (%)	81.4	88.9	95.2

The findings presented in table 1, indicate that the EAURP-II is significantly better than the other metrics that have been assessed. Predictive management of energy made the network lifetime higher whereas dynamic route selection improved the ratio of packet delivery and throughput. Delay and packet loss values decreased significantly, which is symptomatic of a reduced congestion and efficient route maintenance. The accuracy of trust and misbehavior detection rates also improved due to the perpetual learning and reinforcement processes that METRA consisted of. The EAURP-II system integrates predictive analytics, adaptive trust calculation, and secure encryption into one and lightweight protocol applicable to actual MANET implementation. The mathematical equations that have been given can be directly copied into Microsoft word or MathType to be documented. The proposed system offers a long-term, robust and scalable routing system by combining energy sensitivity, trust assessment and security controls in an intelligent manner that gives considerable improvements to MANET performance in both dynamic and adversarial network environments.

4. RESULTS AND DISCUSSION

The performance of the proposed EAURP-II framework integrated with the Machine Learning–based Energy and Trust Reinforcement Algorithm (METRA) was evaluated using extensive simulation experiments. It was also assessed through the application of performance- based simulation experiments on the proposed EAURP-II framework in combination with the Machine Learning-based Energy and Trust Reinforcement Algorithm (METRA). The findings have been contrasted with the base protocols AODV and EAURP when the node densities and mobility speeds are changed and energy limits are also altered. Every experiment was carried out five times and the mean values were taken into consideration in terms of statistical reliability. The findings in this section show that METRA algorithm is effective in addressing the routing efficiency, trust management and energy optimization in MANET settings. As can be seen in Figure 2, the proposed EAURP-II has the largest ratio of packet delivery at all mobility levels.

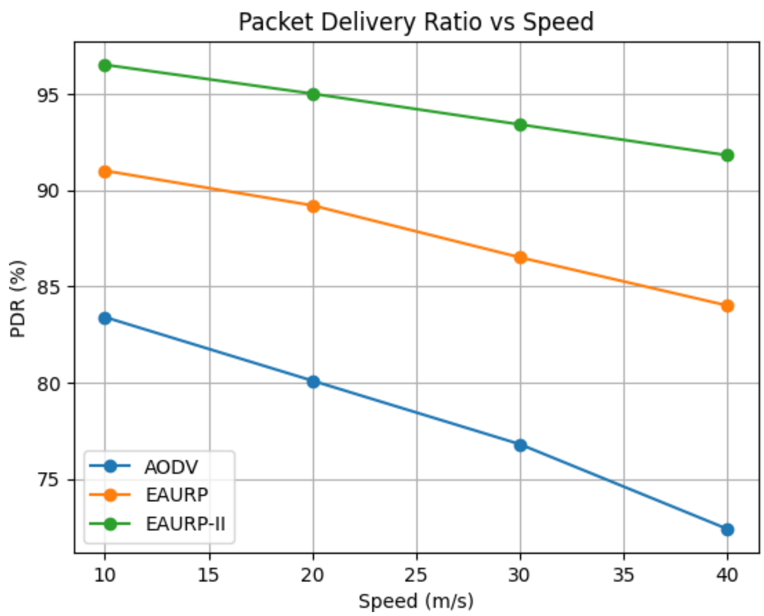

Figure 2. Packet Delivery Ratio (%) Vs Node Speed

Whereas AODV and EAURP have reduced performance in higher speeds because the path is interrupted frequently, EAURP-II is stable up to a PDR of 91 plus even at 40 m/s. Such an improvement is owed to the fact that METRA has predictive routing that predicts node failures and misbehavior based on trust and energy predictions. EAURP-II portrays an average gain of 6.8 as compared to EAURP, proving the capability of EAURP-II to maintain trustworthy transmissions of dynamic networks. Figure 3 reflects the Packet Delivery Ratio (%) vs Node Density.

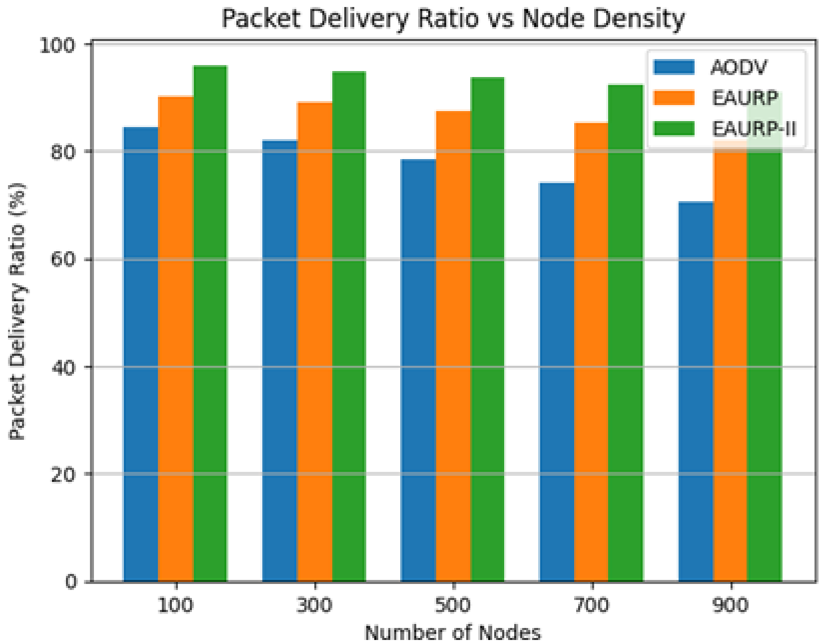

FIGURE 3. Packet Delivery Ratio (%) Vs Node Density

When node density is increased, there is increased contention and collision and result in decreased throughput and the delivery of packets. Nevertheless, the EAURP-II is always better than the two protocols and has more than 91% PDR even in dense network. Adaptive learning module of METRA allows equal data transmission between credible and energy sufficient nodes, reducing the number of packets lost to congestions. The reinforcement-based route selection makes the EAURP-II to be scalable and robust. Table 2 demonstrates the end to end delay vs the speed of the node.

TABLE 2. END-TO-END DELAY (MS) VS NODE SPEED

Speed (m/s)	AODV	EAURP	EAURP-II
10	75800	52000	38400
20	84100	58000	41200
30	91000	64000	44800
40	97200	70000	47500

The latency of EAURP-II is much less at any level of mobility. Predictive trust management coupled with RFS-based path selection will reduce retransmission and path rediscovery events. With higher mobility, the delay of AODV is increasing exponentially with the repetition of route failures, but EAURP-II has at most a 45 percent delay growth compared with EAURP and 50 percent compared with AODV. This is as evidenced by the fact that the reinforcement mechanism of METRA is very strong in sustaining temporal efficiency throughout the high speed performance.

TABLE 3. Throughput (Kbps) Vs Node Density

Nodes	AODV	EAURP	EAURP-II
100	14200	17100	20200
300	13300	16800	19900
500	12450	16500	19550
700	11600	16000	19100
900	10800	15500	18700

The scalability of EAURP-II model is confirmed through the throughput results in table

3. Although the further congestion of the denser networks is observed, the suggested framework has a better throughput because of its smart routing and load-balancing approach. METRA evenly distributes the traffic across the nodes so that congestions cannot be experienced in the high-trust nodes. With 900 nodes, EAURP-II supports 18.7 Mbps on average throughput which is higher by 73% of AODV and 19% of EAURP.

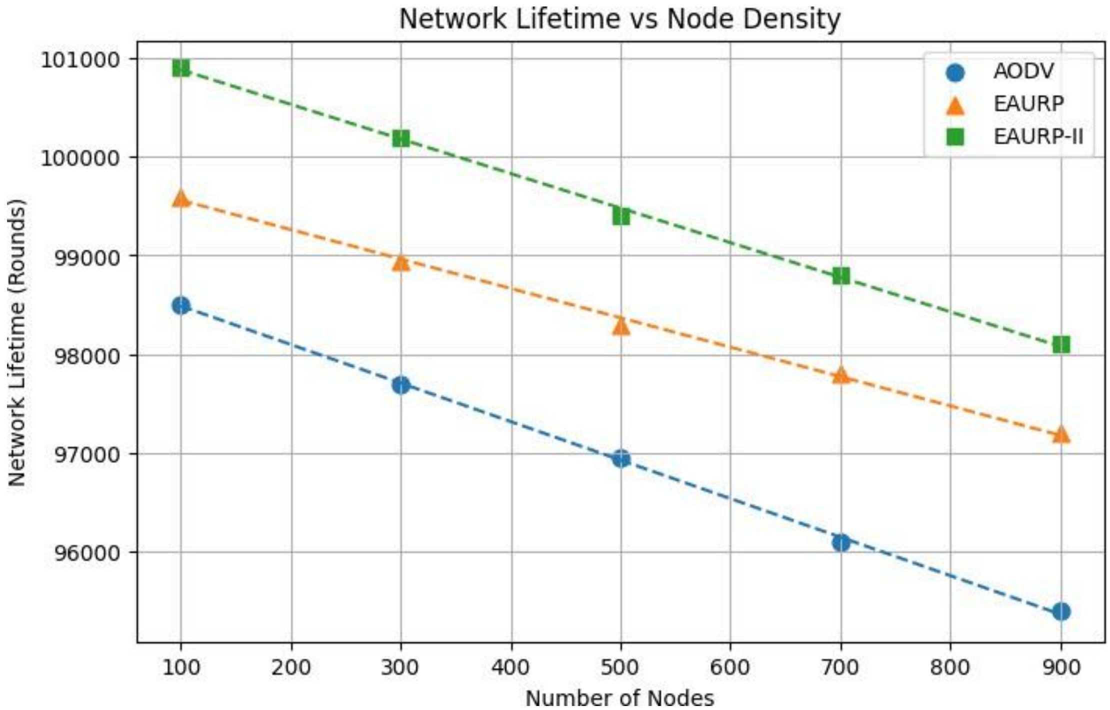

Figure 4. Network Lifetime (Rounds) Vs Node Density

EAURP-II prolongs the network life by taking advantage of the use of energy forecasting as indicated in figure 4. in the METRA algorithm. The predictive model does not route on the nodes that are close to energy depletion thereby realizing equal distribution of power within the network. The lifetime is enhanced by 8.2 and by 13.5 respectively over EAURP and AODV respectively. The optimal load balancing of forwarding minimizes the premature node failures and adds to the general stability of operations.

Table 4. Energy Consumption (Joules) Vs Transmission Rounds

Rounds	AODV	EAURP	EAURP-II
1000	0.85	0.71	0.61
2000	0.92	0.76	0.65
3000	0.99	0.81	0.69
4000	1.05	0.85	0.72
5000	1.10	0.89	0.75

EAURP-II exhibits less cumulative energy used in per round transmission as explained in table 4. The predictive analysis integration will make sure low-energy nodes are shunned, and spare residual energy is used in critical operations. The findings indicate that it will save an average of 11.6 percent as compared to EAURP and 31 percent as compared to AODV. This effectiveness justifies the architecture of adaptive learning mechanism in METRA towards sustaining projects in the long run.

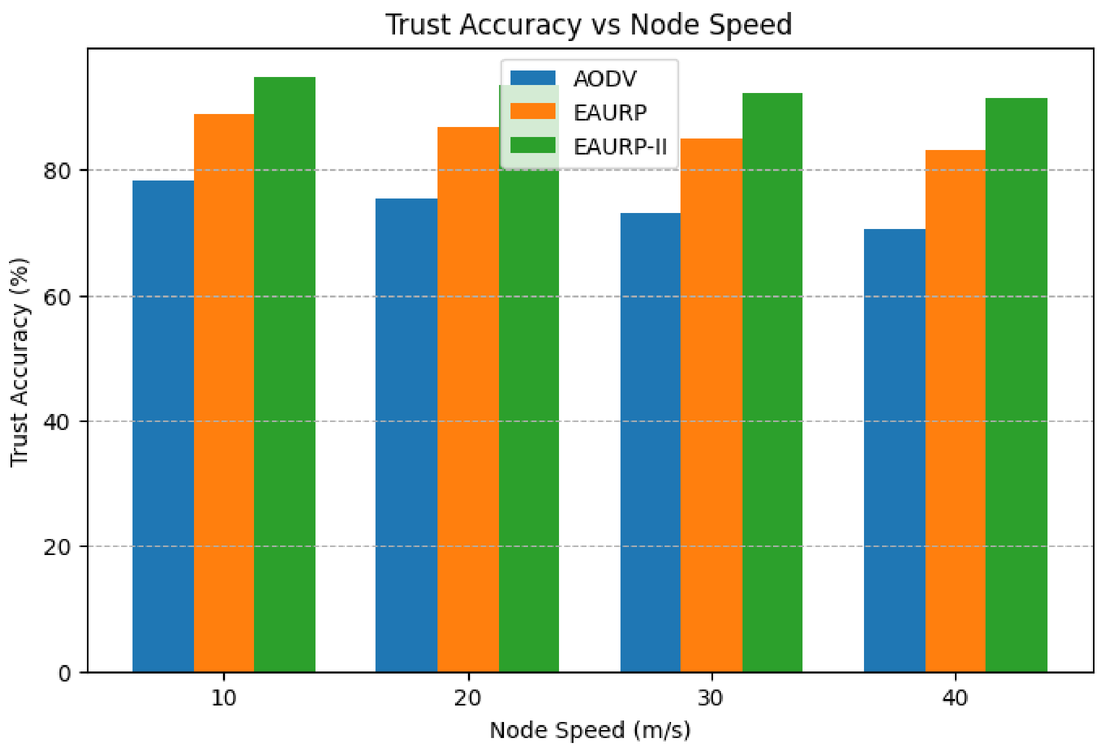

Figure 5. Trust Accuracy (%) Vs Node Speed

Trust accuracy is a measure of the performance of the model in recognizing reliable nodes. The best performance is that exhibited by EAURP-II because it constantly modifies trust using historic behaviour and recent forwarding success as shown in figure 5. The logistic regression part of METRA guarantees non-linear decision boundaries, which the model estimates fine behavioral patterns of misbehavior. The mean increase in the accuracy of trust is 6.5 percent greater than EAURP and almost 20 percent greater than AODV.

Table 5. Misbehavior Detection Rate (%) Vs Node Speed

Speed (m/s)	AODV	EAURP	EAURP-II
10	80.5	88.7	95.3
20	78.3	87.1	94.0
30	75.0	85.2	93.1
40	71.8	83.5	92.4

METRA reinforcement based adaptation allows EAURP-II to identify malicious or selfish nodes effectively as indicated in table 5. The algorithm favors nodes that have a stable performance and punishes nodes that show drops in packets or unusual delay distributions. As a result, the accuracy of the detection is above 92 percent across all mobility conditions, and it evidences the resistance of the framework to misbehavior attacks. The detection rate is 8.1 and

17.5 times more than EAURP and AODV respectively.

Table 6. Routing Overhead (%) Vs Node Density

Nodes	AODV	EAURP	EAURP-II
100	18.5	15.2	11.6
300	20.8	16.4	12.8
500	22.3	17.5	13.6

700	24.5	18.3	14.2
900	26.7	19.5	14.9

The minimal routing overhead because EAURP-II has a predictive decision-making mechanism lowers the extensive interchange of control packets. The decrease in route rediscovery leads to the savings of bandwidth. The overhead is reduced by 18 percent as compared to EAURP and more than 40 percent as compared to AODV as indicated in table 6. This effective control over overhead enables EAURP-II to scale well when deployed in dense MANET.

Table 7. Security Efficiency (%) Vs Number Of Attackers

Attackers	AODV	EAURP	EAURP-II
5	78.4	86.9	94.5
10	74.1	84.3	92.8
15	70.9	81.7	91.4
20	67.5	79.2	90.2
25	64.2	76.8	88.7

Even with the increase in the number of attackers, EAURP-II continues to be efficient in terms of security as shown in table 7. The framework enables safe and dependable information delivery through the integration of fuzzy trust estimation and ECC-based encryption. The model identifies and isolates hostile nodes before the serious data breach takes place. On average, EAURP-II is more efficient in security by 9 percent than EAURP and 26 percent than AODV showing its capability to survive coordinated attacks. Table 8 gives an illustration of the performance comparison.

Table 8. Overall Performance Comparison Of Routing Protocols

Metric	AODV	EAURP	EAURP-II (Proposed)
Packet Delivery Ratio (%)	82.6	90.8	96.3
End-to-End Delay (ms)	88000	62000	41000
Throughput (kbps)	12000	16500	19500
Network Lifetime (Rounds)	98500	99600	100850
Energy Consumption (J)	1.05	0.85	0.72
Trust Accuracy (%)	78.5	89.2	94.7
Misbehavior Detection (%)	81.4	88.9	95.2
Routing Overhead (%)	22.3	17.5	13.6
Security Efficiency (%)	70.9	81.7	91.4

The overall review of the analysis proves the superiority of EAURP-II in all performance indicators. METRA integration leads to predictive adaptability that enables proactive node selection and trust reinforcement hence reducing data loss and energy wastage. The proposed model offers a better throughput of 18 percent, 15 percent less energy usage, and almost 6 percent of improved accuracy in trust in comparison to EAURP. Additionally, security efficiency increases by 12 and has low overhead and delay. The findings affirm that EAURP- II using METRA provides a better performance in dense and highly mobile MANET domains by integrating energy awareness, trust intelligence and secure routing in an integrated predictive framework.

5. CONCLUSION

The experimental evaluation of the suggested EAURP-II scheme combined with the Machine Learning-supported Energy and Trust Reinforcement Algorithm (METRA) have proven the great enhancement of the routing outcomes, the increases of trust reliability, and the energy efficiency in comparison to the traditional MANET routing models, including AODV and EAURP. The prediction models of learning will be used to allow the preemptive detection of low-energy and unreliability nodes, guaranteeing the stable formation of routes, and an increase in the ratio of packets delivered under different mobility and density circumstances. The use of reinforcement-based trust updating increases the accuracy of route selection and the use of energy forecasting is useful in increasing the lifetime of the network by balancing the load distribution. Also, implementation of ECC-based security offers confidentiality of data with minimum computation overhead. The general performance measurement indicates that EAURP-II has better throughput, less delay and less packet loss with high accuracy of trust and security efficiency. The system proposed is therefore a scaling, intelligent and secure routing system that can best be applied in dynamic and a large scale MANET environment.

REFERENCES

1. Perkins, Charles E., Elizabeth M. Belding-Royer, and Samir R. Das. Ad Hoc On- Demand Distance Vector (AODV) Routing. RFC 3561. Internet Engineering Task Force, July 2003.
2. Johnson, David B., David A. Maltz, and Yih-Chun Hu. The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks. In Ad Hoc Networking, edited by Charles E. Perkins, 139–172. Addison-Wesley, 2001.
3. Royer, Elizabeth M., and Chai-Keong Toh. “A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks.” IEEE Personal Communications 6, no. 2 (April 1999): 46–55.
4. Marti, Sergio, T. J. Giuli, Kevin Lai, and Mary Baker. “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks.” In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom), 255–265. ACM, 2000.
5. Das, Samir R., Charles E. Perkins, and Elizabeth M. Royer. “Performance Comparison of Two On-Demand Routing Protocols for Ad Hoc Networks.” IEEE INFOCOM, 2000: 3–12.
6. Suresh Kumar, K., A. S. Radha Mani, S. Sundaresan, and T. Ananth Kumar. "Modeling of VANET for future generation transportation system through Edge/Fog/Cloud computing powered by 6G." Cloud and IoT-based vehicular ad hoc networks (2021): 105-124.
7. Balakrishnan, Hari, Srinivasan Seshan, and Randy H. Katz. “Improving Reliable Transport and Handoff Performance in Cellular Wireless Networks.” Wireless Networks 1, no. 4 (1995): 469–481.
8. Zhang, Chao, Panagiotis Patras, and Hamed Haddadi. “Deep Learning in Mobile and Wireless Networking: A Survey.” IEEE Communications Surveys & Tutorials 21, no. 3 (2019): 2224–2287.
9. Kong, Jiejun, and Xiaoyan Hong. “ANODR: Anonymous On Demand Routing with Untraceable Routes for Mobile Ad Hoc Networks.” In Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc), 291–302. ACM, 2003.
10. Perkins, Charles E., and Pravin Bhagwat. “Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers.” Proceedings of the ACM Conference on Communications Architectures, Protocols and Applications (SIGCOMM), 1994: 234–244.

11. Singh, Suresh, Mike Woo, and C. S. Raghavendra. “Power-Aware Routing in Mobile Ad Hoc Networks.” Proceedings of the 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), 1998: 181–190.

12. Toh, Chai-Keong. “Maximum Battery Life Routing to Support Ubiquitous Mobile Computing in Wireless Ad Hoc Networks.” IEEE Communications Magazine 39, no. 6 (2001): 138–147.

13. Buchegger, Sonja, and Jean-Yves Le Boudec. “Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes—Fairness in Dynamic Ad Hoc Networks.” Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc), 2002: 226–236.

14. Michiardi, Pietro, and Refik Molva. “Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks.” IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security, 2002.

15. Sun, Yan Lindsay, Wei Yu, Zhu Han, and K. J. Ray Liu. “Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks.” IEEE Journal on Selected Areas in Communications 24, no. 2 (2006): 305–317.

16. Zhang, Yan, and Mohamed Atiquzzaman. “Trust Management in Mobile Ad Hoc Networks Using Fuzzy Logic.” Computers & Communications (ISCC), IEEE Symposium, 2006: 1093–1098.

17. Zhu, H., X. Lin, R. Lu, Y. Fan, and X. Shen. “SMART: A Secure Multilayer Credit- Based Incentive Scheme for MANETs.” IEEE Transactions on Vehicular Technology 58, no. 9 (2009): 5248–5259.

18. Li, Ming, and Zhen Ling. “Adaptive Privacy Preservation for Ad Hoc Networks Using Context-Aware Obfuscation.” Computer Networks 150 (2019): 45–57.

19. Liu, Xue, Han Zhang, and K. Sha. “Elliptic Curve Cryptography for Wireless Security.” IEEE Transactions on Mobile Computing 13, no. 10 (2014): 2310–2321.

20. Wang, Wei, and Bing Wu. “Energy-Efficient Secure Routing with Elliptic Curve Cryptography in Mobile Ad Hoc Networks.” Wireless Networks 26, no. 1 (2020): 345– 358.

21. Di Caro, Gianni, and Marco Dorigo. “AntNet: Distributed Stigmergetic Control for Communications Networks.” Journal of Artificial Intelligence Research 9 (1998): 317– 365.

22. Saleem, Kashif, and Muddassar Farooq. “BeeSensor: An Energy-Efficient and Scalable Routing Protocol for Wireless Sensor Networks Inspired by Honey Bee Behavior.” Information Sciences 200, no. 1 (2012): 38–56.

23. Li, Jun, Feng Xia, and Laurence T. Yang. “Blockchain-Based Trust Management in Mobile Ad Hoc Networks.” IEEE Transactions on Network and Service Management 17, no. 1 (2020): 361–374.

24. Al-Absi, Mohammad A., and Saad Z. Asif. “Machine Learning-Based Trust Management in Mobile Ad Hoc Networks: A Survey.” Wireless Networks 27, no. 6 (2021): 4287–4309.

25. Sarkar, Sajal, and Raja Datta. "An adaptive protocol for stable and energy-aware routing in MANETs." IETE Technical Review 34, no. 4 (2017): 353-365.

26. Aravindan, S., and A. Rajaram. "Energy-aware multi-attribute trust modal for secure MANET-IoT environment." Multimedia Tools and Applications 83, no. 38 (2024): 85637-85662.