IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received June 8, 2020, accepted June 26, 2020, date of publication June 30, 2020, date of current version July 20, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3006043

A Game Theory-Based Strategic Approach to Ensure Reliable Data Transmission With Optimized Network Operations in Futuristic Mobile Adhoc Networks

BURHAN UL ISLAM KHAN[1], (Graduate Student Member, IEEE), FARHAT ANWAR[1], (Member, IEEE), RASHIDAH FUNKE OLANREWAJU[1], (Senior Member, IEEE), BISMA RASOOL PAMPORI[2], AND ROOHIE NAAZ MIR[3], (Senior Member, IEEE)

[1]Department of Electrical and Computer Engineering, Kulliyyah of Engineering, International Islamic University Malaysia, Kuala Lumpur 50728, Malaysia
[2]Department of Information Technology, Central University of Kashmir, Srinagar 191201, India
[3]Department of Computer Science and Engineering, National Institute of Technology Srinagar, Srinagar 190006, India

Corresponding author: Burhan Ul Islam Khan (burhan.iium@gmail.com)

This work was supported by the Ministry of Higher Education Malaysia (Kementerian Pendidikan Tinggi) through the Fundamental Research Grant Scheme (FRGS) (Ministry Project ID: FRGS/1/2019/ICT03/UIAM/01/2) under Grant FRGS19-137-0746.

ABSTRACT The Mobile Ad-Hoc Network (MANET) incorporates a collaborative networking scenario, where dynamic host movement results in frequent topology changes. In MANET, nodes cooperate during route establishment, and the data packet must travel from source to destination through multi-hop intermediate links. The nodes in a MANET can be localized in a restricted zone, where manual intervention to set-up fixed infrastructural support is practically infeasible. However, cooperative packet forwarding and data transmission is quite a common scenario in the context of MANET. Still, due to dynamic topological changes, weak, intermittent links appear within one-hop communication. This leads to a higher possibility of packet drop events and also increases the retransmission scenario, which affects the energy performance of the network. Addressing this issue, the study models a novel and intelligent packet forwarding approach based on the game theory, where trust evaluation in terms of node reputation factor also plays a very vital role. The approach also enforces an incentive modelling to stimulate the cooperation between mobile nodes during the MANET routing scenario. The system is designed and developed with evolutionary game perspectives to meet the Quality of Services (QoS) requirements. The experimental analysis supports the proposed modelling design aspects. Also, it exhibits that the reputation and trust-based game increases the utility of packet-forwarding strategy with high throughput and negligible network overhead.

INDEX TERMS Cooperative packet forwarding, game theory, intermittent link failure, mobile adhoc networks (MANET), reliable data transmission.

I. INTRODUCTION

Mobile Adhoc Networks (MANETs) refer to a special type of wireless ad-hoc network, where nodes are mostly mobile and move independently in any direction with self-organizing capabilities [1], [2]. The key-features of MANET include its dynamic characteristics due to node mobility and also decentralized networking scenarios where the network forms for a temporary interval of time to accomplish a specific task. The term decentralized means that the network formation during the communication scenario does not incur dependency on pre-existing communication infrastructural backbones [3]–[5]. MANET includes a wide range of use-cases, like military communications, disaster management in restricted human areas, etc. The trend of the emphasized research in MANET is mostly concerned about the timely execution of the task with reliable data transmission and reception even if unreliable radio-link is present during the communication scenario [6]. A cooperative event of packet-forwarding is a modern approach to ensure the time-dependent high-throughput curve in MANETs. However, encouraging the other nodes in the MANET

The associate editor coordinating the review of this manuscript and approving it for publication was Quansheng Guan.

environment for packet forwarding for an individual node's self-interest is a very challenging task. If intermediate nodes are not appropriately chosen during the route-set up and packet forwarding between source to the destination node, then the possibility of intermittent link-breakage between one-hop neighbours increases. Further, the unreliable communication link also increases the probability of packet drops and retransmission events. This means the utility factor of different packet forwarding strategies will go down and also will affect the energy and throughput performance in MANET eventually [7], [8]. From the security viewpoint also, the cooperative packet forwarding strategies should be robust and flexible enough to deal with every possible route change and also adhere to the communication protocol directions without compromising the QoS and energy parameters. However, the traditional packet forwarding approaches are shrouded with a set of design limitations and fail to stimulate selfish nodes to cooperate in communication [9]. The prime reasons can be that in MANET, most of the mobile nodes usually operate with limited energy and memory capacity. This makes a node to become self-centered, and that way, it only participates in communication when it brings the node more benefits for its interest than cost [10], [11]. This way, the possibility of the presence of self-centered nodes set amid the other crucial networking components leads to disruption of the overall communication and network performance from both energy and security view-point [12]. Therefore, by addressing the design loopholes in the traditional data forwarding approaches, the proposed study realizes that it is essential to design a mechanism that can effectively encourage a node in packet forwarding even if the transmission happens through unreliable links. This way, a high throughput success rate is envisioned with maximum packet-delivery ratio. The mechanism jointly incorporates the game mathematical model along with a trust-based reputation evaluation strategy to increase the utility factor of packet forwarding schema. During the packet forwarding instances, trustworthiness of each node is validated and it also enforces cooperative rewards. The attack-resistant security modeling framework is formulated and evaluated with respect to baseline approaches, and the performance metric for validation includes energy, throughput, network burden, and also the rate of successful packet forwarding. The rest of the paper is organized as follows: Section II outlines some of the significantly related research approaches and their contributory aspects. Section III further objectifies the gap analysis followed by extended research methodology in section IV and the result and discussion in section V. Section VI presents the core findings of the study.

II. LITERATURE REVIEW

This section explores the most significant and related literature, which is studied for the investigational analysis purpose. Further, it outlines the research problem that corresponds to the design limitations of the existing system.

A. EVOLUTIONARY GAME THEORETICAL CONCEPT

The experimental analysis shows that the evolutionary game theoretical approach is most popular since through mathematics, it can analyze the strategic interactions among the MANET decentralized nodes, which act as decision-making agents. The authors in [13] introduced a non-cooperative game modelling to defend different attack scenarios in MANETs. The system model incorporated a novel intrusion detection mechanism where actions between a pair of the attacker and regular nodes are considered as a non-cooperative and non-zero game. Authors in [14] also proposed a similar approach to defend against maximum possible lethal security threats in MANET. The study of authors in [15] also directed their research towards cross-layer optimization. For this purpose, it has incorporated a game theory-based approach to improve the communication scenario in vehicular networks. Similarly, authors in [16]–[18] also improvised a cooperative game theoretical approach to alleviating the communication performance of MANETs by identifying the misbehaving nodes.

B. INCENTIVE-BASED CONCEPTUAL MECHANISM

For many years, there have been various research approaches to strengthen the cooperative packet-forwarding policies in MANET where incentive-based mechanisms encouraged self-centered nodes to behave like a normal node and participate in collaborative forwarding schema. In MANET, it is mostly observed that a regular node forwards self-generated data packets as well as of other nodes regardless of its resource utilization factor. On the other hand, a self-centered node or malicious node will tend to drop the data packets to reserve as much resources as possible to accomplish its intended task. This non-cooperative intention, in the long run, affects the communication performance from reliability and efficiency points of view. This incurs a situation where the network becomes susceptible to various forms of lethal attacks. The incentive-based strategies are classified into three major categories, which can be shown in Fig. 1. Virtual currency solutions include tamper-proof hardware, trusted thirty party, etc. Reputation value-based approaches can either be global reputation-based systems or local reputation based systems. Game theory-based solutions find categorization into one-stage game or repeated game.

The authors in [19] introduced a credit-based approach which is exclusively meant for the delay tolerant networks. The mechanism is designed based on a service-level priority. The outcome of the study shows that it is quite a useful schema. Still, the credit-based approaches are mostly found defenseless against collusion attacks and also do not ensure a higher detection rate when self-centered node identification is concerned. It also lacks energy efficiency, but the throughput performance is found entirely satisfactory. The authors in [20]–[22] also directed their research in a similar direction. The credit-based incentive mechanism refers to a policy where the node gets encouragement to route the data packets

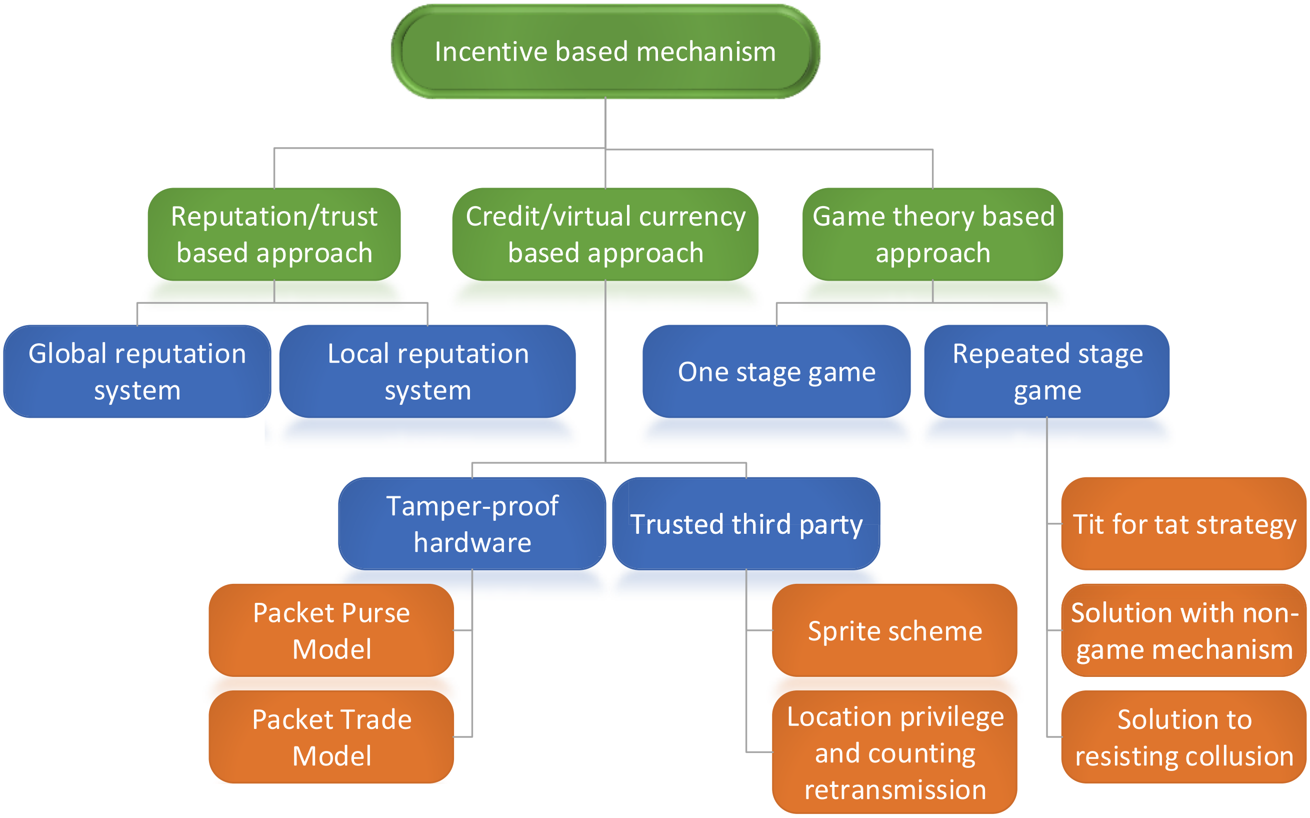
Incentive based mechanism
Reputation/trust based approach
Credit/virtual currency based approach
Game theory based approach
Global reputation system
Local reputation system
One stage game
Repeated stage game
Tamper-proof hardware
Trusted third party
Tit for tat strategy
Packet Purse Model
Sprite scheme
Solution with non-game mechanism
Packet Trade Model
Location privilege and counting retransmission
Solution to resisting collusion

FIGURE 1. Classification of Incentive-based mechanism.

at a specific cost attribute. In the context of trust and reputation-based mechanism, each node assesses its adjacent neighbour's reputation factor which is evaluated based on the node activities and depending upon the probabilistic factor, each node chooses its adjacent neighbour during the packet forwarding paradigm.

There exist different cooperative strategies which are explored by the authors in the studies [23]–[28], where game-theoretical approaches are applied to enhance the network performance concerning adequate QoS and energy factors. The closer inference of the studies exhibits how different types of cooperative strategic methods such as repeated games, non-cooperative games, evolutionary game approaches, etc. ensure a higher degree of packet forwarding among nodes with the incorporation of self-learning capabilities. This makes these approaches suitable and more applicable to the futuristic MANET intelligent applications. From a security viewpoint also, it can be stated that these approaches ensure better packet delivery ratio and energy performance to some extent. Also, the intensive mechanism with an evolving game approach can easily identify the self-centred node activities and the network intrusion it causes for its benefits. Another similar cooperative packet forwarding approach by the authors in [29] is designed based on the principle of dynamic incentive mechanism. In this approach, each node selects a specific strategy to identify a self-centred node within its vicinity and passively encourages it to cooperate in communication. After analyzing various research approaches, it is observed that cooperative packet forwarding based on the evolving game model can ensure a better throughput curve even if a noisy one-hop untrustworthy link is established between two nodes. Various approaches claim that the evolutionary game, if intelligently modelled and enhanced, can ensure not only better outcome in terms of energy but also an effective network performance. The approach, in many instances, has been found to effectively identify the possibility of the self-centred node activities in terms of intrusion and successfully engage them in cooperative packet forwarding. Thus, it is considered as one of the most suitable approaches to ensure better throughput and energy performance in dynamic MANET operations.

Further survey on various recent approaches related to malicious node detection and termination in MANET leads to a study by authors in [30] that introduced a distinct approach of computation termination of cluster head election mechanism and also employ a security mechanism based on Finite State Machines (FSM) to identify and mitigates threats in MANET. Another approach by the author in [31] also mechanized a security approach which can assist in safeguarding the information during distributed routing of MANET. The outcome of the study is observed quite promising but still the design lacks scope of improvisation as it is validated through only simulation study to secure information which travels across MANET. Another study by authors in [32] also worked in the similar line of research and envisioned for a better scope of optimization of AODV routing protocol by strengthening its conventional security features. However, the limitation of this approach is it is only robust against Black-hole attacks. Another study by the authors in [33] evaluated the performance of security aspects of DSR protocol in MANET routing environment. A local positioning approach to identify intruder node in MANET is found in the study of [34]. A novel authentication and security approach is mechanized in the study of authors in [35] to secure the communication and routing scenario in MANET. The outcome of the study shows that the approach takes considerably lesser time to validate the nodes who wants to join the network.

The further section outlines the research gap based on the theoretical analysis, which assists in formulating the proposed design methodology by taking the baselines as a reference model.

III. PROBLEM FINDINGS AND GAP ANALYSIS

The extensive survey and analysis of the existing studies reveal that most of the traditional approaches have design loopholes and can be described as follows:

- The cooperative data forwarding mechanisms and their strength factors are mostly overlooked during the design and development of security protocols and intrusion detection systems. Also, very few studies are found to analyze the problem of packet-forwarding between nodes with an efficient and evolving game approach. Studies have claimed that the game modelling approach can encourage cooperative data forwarding and can also increase the throughput performance in MANET routing [13], [14], [36].
- Despite having various advantages, limited studies have cited game-based decision modelling to assess individual node actions in MANET dynamic routing [28], [29], [37]. Additionally, in many cases, the one-hop data transmission model to simulate the self-centred node in packet forwarding is ignored.
- Most of the credit and reputation-based mechanisms are found suitable only when small and medium scale applications are concerned, but most of the time, not ideal with the large scale MANETs [20]–[22], [29].
- The existing techniques of incentive-based mechanisms encourage a self-centred node in cooperative packet forwarding and more likely to enhance the throughput performance. Still, due to the iterative process of retransmission, the energy consumption rate and network burden may increase [9], [19], [38].
- Most of the techniques do not involve a penalty mechanism if self-centred nodes are detected. But with a penalty, the self-centred node will either assist in packet forwarding or flee to another cluster of the network to save its limited resources. This way, the networking resources can be effectively utilized, and the possibility of packet drops will be minimized [39].
- Both credit and reputation-based mechanisms do not ensure energy-efficient performance and higher resiliency against collusion attacks. On the other hand, the reputation-based approach also individually does not guarantee higher detection accuracy of self-centred nodes in MANET [6], [7], [19], [22].
- The game theory-based approach lacks efficiency when it comes to throughput and energy performance and has not been studied much in the past [16]–[18].
- The analysis of the existing literature also shows that very few approaches jointly address the energy and network performance issues. This is because their intelligent game models might have provided convergence towards better throughput solution but do not ensure effective energy and delay performance in the real-time context from the application requirement viewpoint [23]–[27], [36], [37], [40].
- There are algorithms for identifying the self-centred nodes during the packet forwarding activities but very lesser studies concerned about designing the algorithms with minimal computational requirements such as memory, processing time, etc. [21], [22], [39]. From the time complexity view-point, if the packet forwarding algorithm follows the notion of distributed computing approach, then it should be a light-weight computational model that can be easily deployed for sustainable service delivery execution; besides having a positive influence on controlling the delay constraints in critical applications of MANET.

The current study thereby attempts to develop a robust joint-approach of game and reputation which can encourage and stimulate a non-cooperative node in maximum packet-forwarding and ensure a higher degree of throughput with minimal communication overhead and transmission burden in MANET.

IV. PROPOSED SYSTEM

The study presented in this paper introduces an evolving game-based intelligent packet-forwarding strategy, which is quite distinctive in terms of several design aspects. The policy is formulated with analytical philosophy, which combines a unique approach to assess several node interactions and packet forwarding in a MANET communication scenario. For this purpose, it considers both i) *Possibility of packet drops* along with ii) *Reward factor, which is computed from the node reputation assessment*. This way, the approach identified the self-centred nodes within the MANET environment and stimulated them to cooperate in the packet forwarding paradigm. It also strategized the game formulation to control the energy consumption of individual nodes during the period of data transmission and modulation. Fig. 2 shows an architectural block-based overview of the proposed concept.

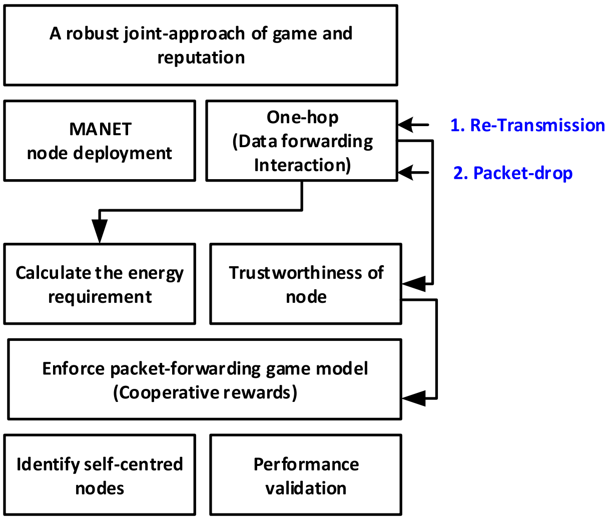
A robust joint-approach of game and reputation
MANET node deployment
One-hop (Data forwarding Interaction)
1. Re-Transmission
2. Packet-drop
Calculate the energy requirement
Trustworthiness of node
Enforce packet-forwarding game model (Cooperative rewards)
Identify self-centred nodes
Performance validation

FIGURE 2. Block-based architectural overview of the formulated approach.

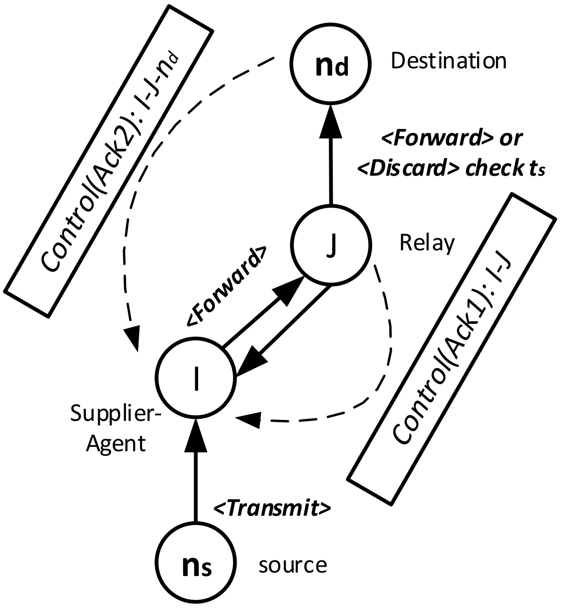

FIGURE 3. A packet forwarding instance between two nodes $< n_s, n_d >$.

A. SYSTEM OVERVIEW

Initially, the system considers a node deployment scenario in a specified region where each node is dynamic and can move freely in any direction. Further, system modelling also shows that it imposes a one-hop data forwarding schema to strengthen the node interaction process. Through this, it can avail access to identify the node who doesn't intend to participate in the packet forwarding. For this purpose, as highlighted in Fig. 1, the functional approach considers i) re-transmission schema, along with ii) assessment of packet dropping by a node who doesn't intend to cooperate in communication. The system design also checks the trustworthiness of a node and its unreliable associative link so that it can decide about its plan of action accordingly by computing the energy required for the retransmission.

The system is built from the perspective of one-hop data forwarding where incorporation of game theory modelling has added another advantage, i.e., it enforces cooperation among mobile nodes $\overrightarrow{m_n}$. The prime target is subjected to increase the successful data packet (msg) transmission with a very low network burden. The system also sets a timestamp (t_s) for packet re-transmission, which also ensures better energy utilization during the route formation process.

B. DATA TRANSMISSION MODELLING WITH COOPERATIVE FORWARDING

This study adopted one-hop data transmission modelling, where game theory is applied to assess the intention of self-centred nodes that have connectivity with the unreliable radio-links. Fig. 3 shows a scenario to showcase the data transmission modelling between two different nodes - source node (n_s) and destination node (n_d) though intermediate relays I and J.

Fig. 3 illustrates how through two intermediate relays where one relay node (n_r) acts as supplier-agent (SA) the communication takes place in terms of both control ($Ack1$) data packet and control ($Ack2$) data packet. Both the packets are control signal carrying information corresponding to the acknowledgement. Here, J is I's 1-hop neighbour when the destination node is considered within the formulated route.

C. PROPOSED GAME STRATEGY TO STIMULATE PACKET FORWARDING

In MANET, self-organizing nodes communicate with each other through intermediate relays, and the success rate of communication entirely depends on how cooperatively and collaboratively intermediate $\overrightarrow{m_n}$ interact with each other and choose their respective plan of action for data transmission. In general, it can be said that basically during the cooperative packet forwarding scenario, one adjacent neighbour of n_s which is I here acts as the SA and helps to forward n_s data to its nearest intermediate hop which is J. In this scenario, J either can accept the forward request or take action (A_F) which indicates that it has agreed upon forwarding the data packet at a certain cost. Anyhow, if the node is self-centred, then to maximize its profit, it won't utilize its resources for packet forwarding. In essence, it can discard the packet forwarding request with (A_D) and can drop the received packet. Considering the reputation model, it can be stated that in a system like MANET, if a node assists in forwarding maximum possible data packets, then it is supposed to gain reward for its higher reputation factor even if it has consumed its resources for cooperative packet forwarding.

On the other hand, a node can behave selfishly and attain a plan of action where it decides to drop the data packets. In this case, the node cannot gain reward or incentives as its reputation value goes down, which is assessed by its adjacent neighbours. In this scenario, although the node suffers a loss of not receiving a higher reputation factor, it also gains profit in terms of resource utilization factors.

The procedure of *msg* forwarding is designed and developed in a way where it operates with a pair of nodes in a graph $\rho(v, e)$ where ρ represents a graph of vertices and edges. Here, $v \rightarrow < SA, n_r >$ means the pair of nodes is restricted to $< SA, n_r >$ at every instance of communication. Out of all the corresponding nodes within the network population, a set of nodes will be selected for routing and packet forwarding at each instance of time-slot. Here considering each pair, 1-node will act as intermediate SA, and another will act as n_r.

The system also evaluates the node's reputation and trustworthiness during the packet retransmission schema. As shown in Fig. 3, it is quite clear that *SA* helps n_s in forwarding its data, but it can encounter unreliable radio-link during the transmission process. Before forwarding the data packet, SA waits for 1-hop Control (Ack1) from the relay node. If the relay node successfully receives the data packet, then it provides a confirmation message to the *SA* with one hop acknowledgement. During the transmission and re-transmission process, a time-stamp is set to limit the count of re-transmission. If that time expires, that means the *SA* has not yet received the one-hop acknowledgement from the relay agent, and it re-transmits the packet. If the relay node successfully receives the packet, then it can take two different sets of actions - either it can forward the data packet and cooperate in communication by engaging all its essential resources, or it can act like a self-centred node which has a minimal amount of residual energy. In another scenario, it can be stated that as two nodes interact with their plan of actions provided, they are concerned about their reputation factor. Then it can happen that after the successful reception of the data packet, the relay node will decide whether to forward the packet or to drop the packet depending upon the assessment of the *SA's* trustworthiness/reputation factor from security viewpoint. However, if that node acts like a self-centred node, then the possibility arises that to save its own constrained remaining energy, it may drop the data packet.

In the context of cooperative packet forwarding, it is also found that if the destination node successfully receives the data packet from the sender node, then it initiates a control message, which is the 2-hop acknowledgement to the SA node about the successful data transmission by the relay node. To save a significant amount of energy, this study also incorporated a novel threshold mechanism that set the cut-off value (t_s) for the retransmission process. The system modelling also initializes optimal deployment of $\overrightarrow{m_n}$ within a specific region A and considers a few sets of nodes for communication within a specified t_i. At the beginning of the communication, if the source and destination come closer and wish to communicate with each other through relay nodes, they can evaluate each other's trust factors by exchanging their reputation table. For this purpose, the system analytically incorporated a functional module, Ex (r_{Table}), which performs exchanging of the reputation attributes through control signals.

Further, the system also checks whether the relay nodes' energy is greater than a cut-off value or not; this is to ensure whether that relay node belongs to the category of a self-centred node or not. If energy is limited (it is lesser than the cut-off value) then, it may drop the packet to conserve its battery power. The system here also introduces another variable, which is t_s. The prime reason for introducing the upper limit by t_s is bounded significantly helps in energy conservation. The system again also checks for two acknowledgements from the destination if it doesn't find it within specified t_s. The system considers that the relay has not forwarded the *msg* to the destination. The whole process is progressively iterative till the upper bound of t_s if required, and the novelty is that the cooperative and collaborative aspect here enforces an intelligent communication by assessing the reputation factor about each node and which gets updated by the r_{Table} in subsequent stages. The system also learns in every stage, that means each node that becomes SA learns about the relay node reputation, and the relay node learns about SA reputation. This way, the system gets mature by the learning experience, and the communication between source and destination becomes effective in terms of energy, throughput, and delay.

The notation of important parameters that have been considered in the proposed algorithm formulation are highlighted in Table 1.

TABLE 1. Notation table for proposed algorithm.

Notation (Symbolic)	Description
m_n	Mobile node
t_s	Timestamp for packet re-transmission
n_s	Source node
n_d	Destination node
n_r	Relay node
'msg'	Control message
SA	Supplier agent
A_D	Node's action of reject (Declining)
A_F	Node's action of forward (Cooperating)
r_{Table}	Reputation table
t_i	Discrete time interval
d_c	Cost of successful data transmission

The algorithm is illustrated from the view-point of mathematical notions, and it represents the system of packet re-transmission with very lesser memory and processing overhead. The algorithm execution steps show how the formulated system modelled the process of retransmission during the communication scenario, which assists in assessing individual node trustworthiness and reputation factor. The analytical modelling of the above algorithm intelligently mechanizes the packet forwarding between a pair of nodes

Algorithm 1 A Cooperative *msg* Transmission and Forwarding Schema With Game-Based Collaborative Effort With Unreliable Links

```
1. Input: $n_s, n_d$, Area (A), $t_s$
2. Output: Cooperative msg transmission
3. Start
4. MANET node deployment with $\rho(v,e)$
5. $\overrightarrow{m_n}$ (count)= (400-900)
6. Enable mobility-model
7. for each time instance $(t_i)$
    a. select the subset of $\overrightarrow{m_n}$
    b. $< n_s, n_d - > Ex(r_{Table})$
    c. If$E(n_r) >$cut-off
        i. Set counter(p) and transmit msg till $p^{th}$ interval
        ii. Ensure control (Ack1), control (Ack2) received
        iii. Relay(msg) transmission success.
        iv. Update $r_{Table}$ of$SA$(I) and Relay (J)
    d. Else if control (Ack1) not received
        i. counter(p) = p $< t_s$, p++
    e. Else if control (Ack2) not received
        i. relay dropped packet
        ii. Update $r_{Table}$ of Relay (J)
    f. Else
        i. End Transmission
    g. End
8. End
```

$< n_s, n_d >$ where it set an upper bound of the *msg* retransmission with a numerical value of t_s.

As in wireless communication, the bridge between two nodes becomes unreliable due to various problems such as intermittent link breakage, channel fading, etc. Addressing this problem, the study thereby considers the fact during the modelling of the stochastic game based packet forwarding approach that owing to the intermittent link-breakage issue, channel instability is a quite common problem due to which data packets could be easily lost. To ensure a higher degree of reliable data forwarding, the sender node has to get acknowledgement from the receiver side about the confirmation of the data packet reception. But until and unless it arrives into that state (it receives the acknowledgement), the sender has to re-transmit the data packet, which leads to energy consumption to a greater extent. Therefore, the novelty of this approach is it impose a cut-off mechanism to assess the energy of each node and also impose cut-off to restrict the maximum number of retransmissions within a specified communication channel for a specific t_i. This also affects the network lifetime in terms of delay and other QoS parameters, thus setting up the t_s, which is bounded within a specified count and the retransmission count is denoted with counter(p) where the value of p increases until it reaches the maximum limit of t_s. In a typical instance of communication, nodes within 1-hop and 2-hop exchange their r_{Table} based on the acknowledgement exchange on receiving the *msg*. The r_{Table} here helps in intelligent route establishment, and it only outlines whether an adjacent neighbour can be utilized for effective communication or not. It is also observed that using the concept of bounding the counter value of re-transmission, the possibility of recovering the lost data increases within a weak radio link. Also, it conserves a significant amount of energy.

The algorithm steps also show that the system involves a graph-based MANET deployment, which is mobility enabled, i.e., each node can move in any direction. Further, the algorithm defines each condition, which is more likely to occur during the cooperative and non-cooperative packet forwarding. The study also analyses the memory and time complexity of this analytical algorithm through a numerical computing analysis, and that is extended further in the consecutive section of the study. The system modelling assumptions consider that with the variable network parameters and operating conditions in the channel, the value of t_s changes and also the normalized steps in the algorithm show that the data stored in the reputation table can be further utilized to train a better classification model. That way, node movement and its actions can be predicted from the machine-learning view-point. This could assist in better and accurate identification of self-centred nodes satisfying the delay constraints. The proposed solution, in one way, also represents optimized modelling which deals with both energy and performance aspects in a dynamic MANET environment. The reputation table is also calculated where *r-pow* refers to the remaining power of a node. That means in this formulated approach if a relay node encounters that it does not have a sufficient amount of remaining energy to forward other nodes' data packet, it intentionally drops the packet and gains a reputation of *r-pow*. An instance of the reputation table in the form of a pay-off matrix is shown for individual nodes (say, in this case for I, J, and n_d) in Table 2.

TABLE 2. Reputation and Pay-off Table for Node I, i.e. SA.

Pay-off allocation	I	J	n_d
I	r-pow	r- (I, J)	r- (I, n_d)
J	r- (J, I)	r-pow	r- (J, n_d)
n_d	r- (n_d, I)	r- (n_d, J)	r-pow

It means that to help the sender node I in forwarding its data packet, SA forwards the respective *msg* to J. Then, J obtains a reputation value of r-(I, J) which is maintained in the r_{Table} of I. This way, for every instance of communication, reputation values are allocated based on the assessment of the trustworthiness of adjacent nodes towards cooperation in forwarding the respective data packets.

The mathematical modelling to realize the successful packet transmission concerns two aspects - one is energy consumption and the other being data packet retransmission factor. Assuming a node having a probability of ν within a period in successful data packet forwarding and transmission within an unreliable radio link. The successful transmission probability for the maximum limit of t_s can be computed using (1) as:

$$\mu = 1 - (1 - \nu)^\wedge t_s \tag{1}$$

The study also indicated the cost of successful data transmission with d_c and that could be computed with respect to the number of packet retransmission count with $1 \leq p \leq t_s$. Here, the d_c can be derived using (2) as:

$$d_c = \sum p \times t_s \times \Phi\{p|p \leq t_s\} \tag{2}$$

From (2), it can be stated that with one interaction, if a packet does not reach the intended destination within a specified time interval, then the failure cost arises as $p \times t_s$. Here, Φ indicates the probability of the events that might occur, and a flag $F < 0|1 >$ is used to indicate the success or failure of the event.

The packet forwarding game modelling also considers that the nodes which are associated with the dynamic MANET are mostly self-centred and intend to drop the packet to save their energy. The game modelling also shows that their actions are distinctive, and that is incentive oriented. A self-centred node either selects A_F and forwards the packet with a cooperative packet forwarding strategy, or it obtains the action A_D, which is meant as a discard strategy. This state of actions is conditional and depends on the situation, whether a node maximizes its gain of resources/reputation or not. The plan of action each node attains between forwarding or declining according to the pay-off calculation and which is probabilistic mathematical modelling that represents each event that can occur during the packet forwarding scenarios.

1) PACKET FORWARDING SCENARIO-1

If two nodes I, J within the one-hop scope of communication select the A_F, that means the forward strategy is chosen by both the nodes. In this strategy, nodes I, J impose two actions that are forward and transmit, respectively.

2) PACKET FORWARDING SCENARIO-2

In this scenario, it may happen that only I selects the A_F action, which means I has two options - forward and transmit where J only selects the transmit strategy. This game modelling also states that a self-centred node has an intention to only send its data packet without cooperating in the packet forwarding scenario.

3) PACKET FORWARDING SCENARIO-3

In this scenario, both the nodes I and J may select $\mathrm{A_D}$. That means both the nodes act like self-centred nodes and only have one option, that is, transmit their respective data packets.

The pay-off calculation is done depending upon the probability of each node and their respective gain $\mathrm{g_{pay-off}}$. If both I and J opt the $\mathrm{A_F}$, then, in that case, the total pay-off can be computed using (3) as below:

$$\sum \Phi_k \{p\,|\,p \leq t_s\}\,.g_{pay-off}\ (I)_k = \sum \Phi\,\{p\,|\,p \leq t_s\}\,.g_{pay-off}\,(J) \tag{3}$$

Here, k indicates a positive integer and its value lies in the range $0 \leq k \leq 4$. Similarly, the pay-off for every gain of normal and self-centred nodes is calculated.

To ensure a higher degree of packet forwarding among nodes, a functional module based on the evolutionary game model is defined. It stimulates packet forwarding among the nodes by adjusting various control parameters. Also, it converges to a steady-state where t_s become smaller, which means the count of packet transmission will be optimized to save the node energy and even lost data recovery can happen faster. The study also subjected its mathematical modelling in a way where it is also observed that if nodes select a forward strategy, then it can obtain more gain collectively. This approach of incentive or reward allocation among the cooperative nodes has encouraged maximum possible nodes in packet forwarding. Thus, the schema of cooperative and collaborative reward policy helps nodes to select the action $A_{F,}$ and it converges to a stable state where the packet loss rate can be minimized. The study further targeted optimizing the channel reliability performance. The following section illustrates the experimental outcome, which validates the performance of the proposed approach in terms of different parameters. The study here compared the performance of this collective and stochastic evolutionary game model with four different existing baseline solutions, which are i) Repeated game approach, ii) Stochastic game approach followed by iii) no-cooperation and iv) Bargaining strategy respectively.

V. PEFORMANCE ANALYSIS

The experimental outcome is obtained after simulating the formulated numerical modelling in a mathematical computing platform. The system representation claimed that it accomplishes various research targets, such as minimizing the network load along with proper utilization of energy. In contrast, it also claims that the system will attain better throughput without compromising the delay constraints. Fig. 4 illustrates the comparative outcome of communication burden in the network where the other four approaches are taken as baselines for validation purposes. The numerical modelling is evaluated considering the MATLAB environment, where it includes a 400-900 number of mobile nodes and sink placement. The evaluation parameter-1(Network-burden) refers to the context where the system is able to handle the security in variable traffic conditions and during network elements processing. That means the security protocol design should not affect the network performance such as delay and other aspects. It is clear that through reputation updating and assessment the system reduces the network burden to a significant extent and in other words, it means it is efficiently utilizing the computational and network

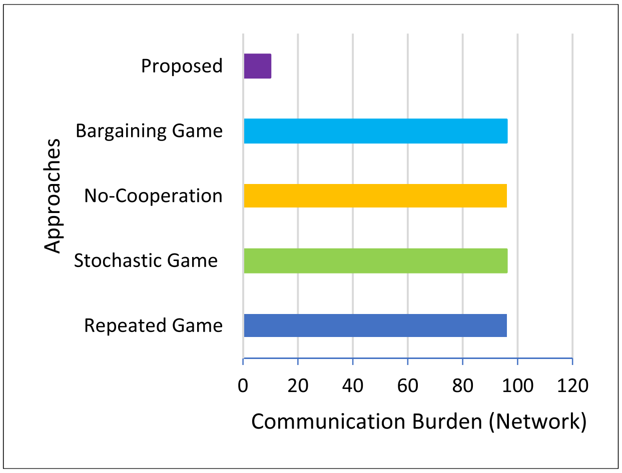

FIGURE 4. Analysis of network burden in variable traffic condition in Mpbs.

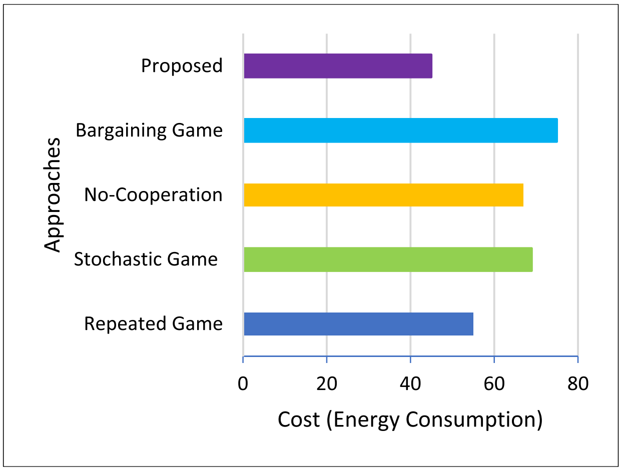

FIGURE 5. Analysis of cost of energy in Joule (J).

resources such as bandwidth. Similarly, in Fig. 5, cost of energy consumption (Parameter-2) shows how much energy is consumed during overall network operations by different approaches. (Parameter-3) throughput and (parameter-4) rate of packet drops indicates the outcome of the measures of successful packet transmission within a particular interval of time as shown in Fig. 6 and 7. (Parameter-5), time complexity shows in Fig. 8 how much time the proposed algorithm takes for execution and where each of the network operations are cumulatively involved.

The modelling and simulation of the system has been performed using MATLAB. This is because MATLAB is one of the most popular software-modelling environments owing to the common interfacing of its functionality with instruments for providing programming solutions, control and connectivity for rapid prototyping as well as testing. The hardware and software requirement considerations for employing MATLAB in this study have been given in Table 3.

The study also involves a set of self-centred nodes, which ranges from 1 to 90 to assess communication performance with different operating scenarios. Here, baseline game theoretical approaches such as the Bargaining game approach refers to a simple two player game where negotiation factor is involved during packet transmission with bargaining interactions. No-cooperation game means not a single individual relay node will cooperate during packet transmission and

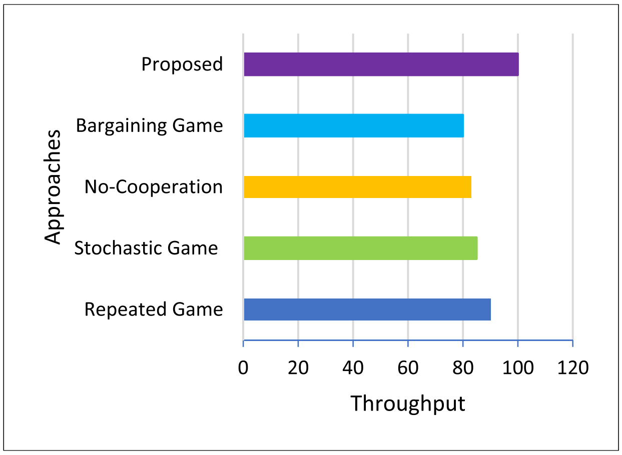

FIGURE 6. Comparative throughput analysis bits/sec.

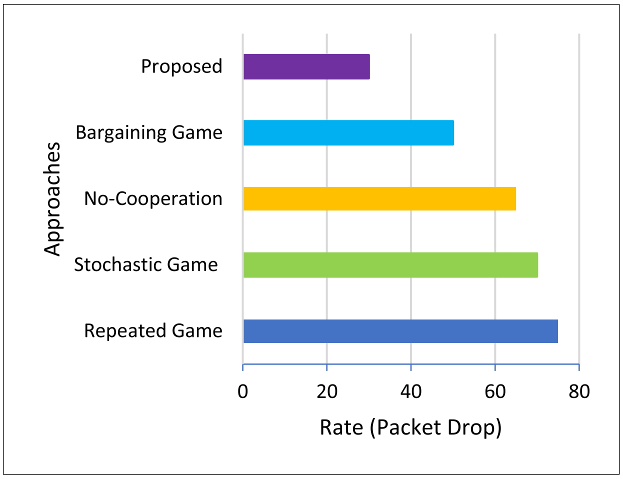

FIGURE 7. Comparative analysis of the rate of packet drops bits per sec.

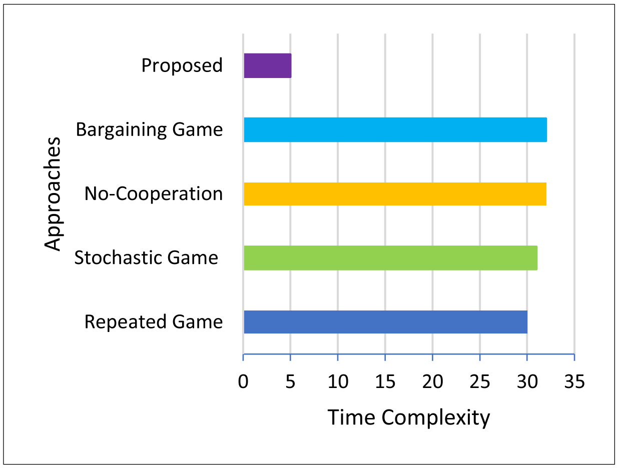

FIGURE 8. Comparative analysis of time complexity in Sec.

TABLE 3. MATLAB configuration requisites and environment set-up details.

Operating System (OS)	Windows 10 with type-64bit and x64
Processor	Inter® Core™ i5-600U CPU @2.00GHz
Clock-frequency	1.99 GHz
RAM	4.00GB
MATLAB Version	2019a

it is a game-based approach where competition between individual players can be seen. Stochastic game modeling refers to a dynamic game modeling where probabilistic transitions take place by different individual players in progressive stages. On the other hand, repeated game is a well-studied two-person game which employs repetition factors of different base-games.

The rate of successful packet transmission is also computed by the devised cooperative *msg* transmission and forwarding schema and the related equations, which also ensure negligible computational complexity and a higher throughput performance from the theoretical and experimental viewpoint. Analysis of throughput shows that the proposed method stimulates every node in choosing the action that corresponds to a higher degree of packet forwarding.

The proposed approach applies a cooperative evolution based game model to encourage each node in packet forwarding within timely instances that indicate that due to the optimized performance of cooperative packet forwarding, the possibility of packet drops is reduced to a significant extent. Also, the evolutionary game approach with the improved value of ν, the network burden is reduced with successful packet transmission and recovery. This way, the nodes also intended to maximize their utility in terms of pay-off. The system considers successful packet delivery even in unreliable links where channel fading with bandwidth limitation can take place. But despite these challenges, the system accomplishes better outcomes with the optimized cost of computation and communication, which result in minimizing the network burden.

The analysis also subjects the evaluation of the energy consumption cost that is also found significantly low in the case of the formulated approach. That means introducing the condition which lies under $p \leq t_s$ yields better energy performance since the count of retransmission is reduced in every instance of communication which mostly takes place between I and J where one node acts as SA and other node acts as a relay. The overall energy consumption is found approximately ∼50 J, which is quite low as compared to the different game-based cooperative and non-cooperative packet forwarding strategies shown in Fig. 5. Out of the other four conventional baseline modellings, a bargaining based game strategy yields higher energy consumption due to its much iterative steps of execution. A closer interpretation shows that the proposed approach and repeated game-based strategy exhibits better energy performance in contrast with the stochastic game, no-cooperation, and bargaining approach. The study also performed throughput analysis to validate the network performance for a different instance of t_i. The study incorporated 500 – 800 mobile nodes with a mobile sink wherein every instance of communication, topological changes take place depending upon the communication requirements and application demands and also based on the changes in network parameters, the throughput analysis is shown in Fig. 6.

The inference of the throughput performance shows that the proposed approach attains significantly higher throughput performance. This is because it reduces the possibility of packet drops with evolutionary intelligent game modelling where the system passively encourages every node (even self-centred node) to forward the data packet and to gain higher possible pay-off in terms of resources and reputation. A closer analysis shows that the proposed approach attains approximately 30% improvement in throughput performance as compared to the conventional baselines.

It is quite imperative that as the throughput performance in the proposed approach significantly improves, the rate of packet drop is also lesser in the case of the proposed system in comparison with the existing methods, as shown in Fig. 7. As the cooperative evolutionary game model stimulates every node in packet forwarding and also adds another distinctive feature of limiting the number of packet re-transmission, it has a significant impact on reducing the packet drop probability by adjacent nodes that can also be self-centred. But, to receive a higher incentive from the cooperative reward computation viewpoint, the self-centred node cannot opt for the decline strategy and performs both transmission and forwarding of the data packets. The study also incorporated another analysis that is performed considering the execution of the above mathematical algorithm plus Eq. (1) to (3). The numerical execution clearly shows that during the compilation stage and runtime scenario, the algorithm does not pose many dependencies on the primary memory and smoothly executes with progressive steps of execution, as shown in Fig. 9.

The memory requirement analysis also shows that the proposed system only consumes approximately 7 MB of memory. In contrast, other approaches consume much more memory, such as the bargaining game model, which consumes the maximum amount of memory, which is approximately 30 MB during the runtime execution stage.

The intelligent game modelling in a cooperative packet forwarding scenario has not only been found to stimulate the data transmission among nodes but also ensure the minimum time of execution, as shown in Fig. 8. The execution time of the proposed algorithm refers to the time of its simulation in the numerical computing environment. It includes all the communication activities within one communication cycle. The analysis indicates that the execution time of the proposed approach is 4 seconds, whereas, in the other methods, it is quite higher. That means the formulated

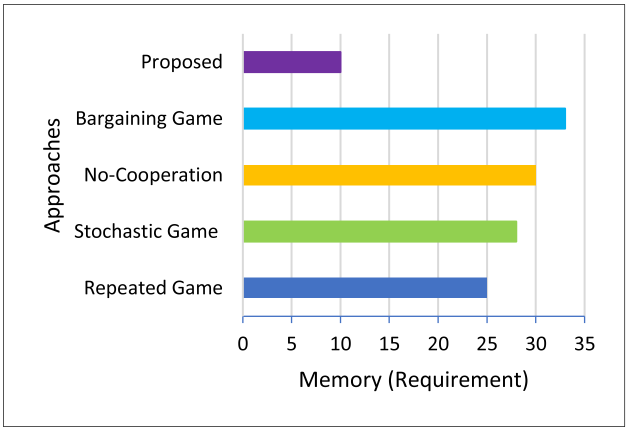

FIGURE 9. Comparative analysis of memory requirement in MB.

system significantly improves the computational performance along with the communication performance satisfying every possible network constraint. The experimental analysis mostly considers three crucial factors to study the outcome of the system towards improving the energy and network performance and how the evolutionary stable states appear during the game formulation. These factors are upper bound of re-transmission factor, cooperative reward factor, and the probability of successful packet forwarding with cooperative strategy and 1-hop modelling. In this study, the possibility of higher data packet transmission refers to the scenario where destination nodes receive more data packets with respect to the data transmitted by the source in the form of a ratio. The study also ensures that the system formulation significantly improves the network performance from all the possible QoS aspects, which is quite distinctive as compared to the benchmark systems. The proposed system encourages and stimulates the self-centred nodes in packet forwarding to a certain extent; thereby the possibility of successful packet transmission is quite higher despite the various scenarios of network dynamics.

The study also evaluated the network overhead parameter, which indicates the ratio between several packets forwarded and the number of successful messages transmitted. The experimental results also illustrated that the system handles the packet transmission in the unreliable radio links by introducing a cooperative intelligent game mode where the distribution of incentive-based on collective intelligence has taken this approach to a different extent. As the algorithm also evaluates the trust factors of each node based on their reputation, thereby the packet forwarding takes place with reliable communication, thus, in the long run, it sustains with reduced network overhead. The system also modelled the game based solution in a way where the notion of cooperative reward strategy stimulates a self-centred node to obtain the action which corresponds to relay or forward the data packet.

VI. CONCLUSION

In the MANET routing and communication scenario, it is essential to maximize the possibility of packet forwarding even in the presence of unreliable radio links. However, as MANET operates with resource-constrained self-configuring mobile nodes which usually move in any direction and the topology dynamically changes every time, in the absence of a centralized authority, it is challenging to ensure minimum energy consumption satisfying the QoS constraints with higher throughput outcome. The study introduces an intelligent packet forwarding approach based on an evolutionary one-hop packet forwarding game model that assesses the communication scenario in the presence of unreliable links. Targeting the real-time use cases, the study modelled the system considering strong assumptions and designed the packet forwarding schema with a cut-off value corresponding to the upper bound of re-transmission count. Here, the upper limit of retransmission count is modelled as $1 \leq p \leq t_s$ for a pair of nodes that can be I, J. The rate of convergence is also stabilized by evaluating the proposed game-based packet forwarding strategies. The condition of convergence to stable states is analyzed with respect to the prime three factors, which are upper bound of re-transmission factor, cooperative reward factor, and the probability of successful packet forwarding with collaborative strategy, respectively. The entire system model is evaluated in a numerical computing environment, and the outcome obtained is further analyzed, considering different parameters. The experimental result shows how these three prime factors positively influence the rate of convergence and also ensure higher throughput and lesser possibilities of packet drops. The quantified outcome also indicates that the energy performance improvement in the proposed system context is approximately 50% as compared to the conventional baseline solutions, and also the system outperforms other models in terms of throughput and communication burden. The throughput performance improvement is obtained approximately 30%, which is quite an effective outcome as the proposed system ensures a higher probability of successful data transmission with upper bounded re-transmission number. With a robust hypothetical basis, the study forms a theoretical base to provide a higher degree of packet forwarding in unstable radio links of dynamic MANET environments. It is also observed that the system significantly identifies the self-centred node intrusion and diverts them to cooperate in packet forwarding with lesser network overhead. Theoretical modelling is intended to solve the above-stated research issue to a significant extent.

The design of the framework takes baseline analytical approach as a reference model by evaluating the related studies of the past. However, the outcome shows that the rate of packet drop is reduced to a greater extent in the proposed approach but still it has a better scope to be improvised for different IoT network objects. Another significant point to be highlighted is the system evaluation only considers maximum 900 mobile nodes but it is observed that till 700 the network burden remains minimum for the system but it increases when the number of nodes are set to 900 due to increase in the size of data traffic. However, the system performance has not been evaluated taking IoT objects into consideration and also the computational complexity can be optimized to a greater extent. This work can be adapted for a future line of research which can include minimizing the complexity of network overhead and energy issue in IoT routing dynamics when scaled up with various networking entities and objects. The operating conditions also differ from the traditional approaches of routing and communication convention protocols. It also envisioned a less complicated and robust approach to manage the routing performance with more reliable operations in dynamic IoT.

ACKNOWLEDGMENT

The authors thank the two anonymous reviewers for their careful reading of the initial version as their many insightful comments and suggestions have helped improve and clarify this manuscript.

REFERENCES

[1] B. U. I. Khan, R. F. Olanrewaju, F. Anwar, A. R. Najeeb, and M. Yaacob, "A survey on MANETs: Architecture, evolution, applications, security issues and solutions," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 12, no. 2, pp. 832–842, 2018, doi: 10.11591/ijeecs.v12.i2.pp832-842.

[2] R. F. Olanrewaju, B. U. I. Khan, F. Anwar, B. R. Pampori, and R. N. Mir, "MANET security appraisal: Challenges, essentials, attacks, countermeasures & future directions," *Int. J. Recent Technol. Eng. (IJRTE)*, vol. 8, no. 6, pp. 3013–3024, 2020, doi: 10.35940/ijrte.E6537.038620.

[3] G. H. Raghunandan, G. H. Chaithanya, and R. Hajare, "Independent robust mesh for mobile adhoc networks," in *Proc. 4th Int. Conf. Electron. Commun. Syst. (ICECS)*, Coimbatore, India, Feb. 2017, pp. 125–128, doi: 10.1109/ecs.2017.8067852.

[4] S. Kumar, M. L. Saini, and S. Kumar, "A survey: Swarm based routing algorithm toward improved quality of service in MANET," *Int. J. Manage., Technol. Eng.*, vol. 8, no. 5, pp. 311–322, 2018.

[5] T. Jamal and S. A. Butt, "Malicious node analysis in MANETS," *Int. J. Inf. Technol.*, vol. 11, no. 4, pp. 859–867, Dec. 2019, doi: 10.1007/s41870-018-0168-2.

[6] A. S. Almazyad, "Reputation-based mechanisms to avoid misbehaving nodes in ad hoc and wireless sensor networks," *Neural Comput. Appl.*, vol. 29, no. 9, pp. 597–607, May 2018, doi: 10.1007/s00521-016-2555-6.

[7] K. Rama Abirami and M. G. Sumithra, "Preventing the impact of selfish behavior under MANET using neighbor credit value based AODV routing algorithm," *Indian Acad. Sci.*, vol. 43, no. 4, pp. 1–7, Apr. 2018, doi: 10.1007/s12046-018-0803-4.

[8] D. Bisen and S. Sharma, "Fuzzy based detection of malicious activity for security assessment of MANET," *Nat. Acad. Sci. Lett.*, vol. 41, no. 1, pp. 23–28, Feb. 2018, doi: 10.1007/s40009-017-0602-1.

[9] T. Seregina, O. Brun, R. El-Azouzi, and B. J. Prabhu, "On the design of a reward-based incentive mechanism for delay tolerant networks," *IEEE Trans. Mobile Comput.*, vol. 16, no. 2, pp. 453–465, Feb. 2017, doi: 10.1109/TMC.2016.2546910.

[10] G. Lau, M. Al-Sabah, M. Jaseemuddin, H. Razavi, and M. Bhuiyan, "Context-aware RAON middleware for opportunistic network," *Pervas. Mobile Comput.*, vol. 41, pp. 28–45, Oct. 2017, doi: 10.1016/j.pmcj.2017.07.004.

[11] B. U. I. Khan, R. F. Olanrewaju, F. Anwar, and A. Shah, "Manifestation and mitigation of node misbehaviour in adhoc networks," *Wulfenia J.*, vol. 21, no. 3, pp. 462–470, 2014.

[12] M. Rajesh, "A review on excellence analysis of relationship spur advance in wireless ad hoc networks," *Int. J. Pure Appl. Math.*, vol. 118, no. 9, pp. 407–412, 2018.

[13] T. Poongothai and K. Jayarajan, "A noncooperative game approach for intrusion detection in mobile adhoc networks," in *Proc. Int. Conf. Comput., Commun. Netw.*, Saint Thomas, VI, USA, Dec. 2008, pp. 1–4, doi: 10.1109/icccnet.2008.4787668.

[14] B. Paramasiva and K. M. Pitchai, "Modeling intrusion detection in mobile ad hoc networks as a non cooperative game," in *Proc. Int. Conf. Pattern Recognit., Informat. Mobile Eng.*, Salem, India, Feb. 2013, pp. 300–306, doi: 10.1109/ICPRIME.2013.6496490.

[15] J. Wang, P. Lang, J. Zhu, W. Deng, and S. Xu, "Application-value-awareness cross-layer MAC cooperative game for vehicular networks," *Veh. Commun.*, vol. 13, pp. 27–37, Jul. 2018, doi: 10.1016/j.vehcom.2018.04.001.

[16] C. Vijayakumaran and T. A. Macriga, "An integrated game theoretical approach to detect misbehaving nodes in MANETs," in *Proc. 2nd Int. Conf. Comput. Commun. Technol. (ICCCT)*, Chennai, India, Feb. 2017, pp. 173–180, doi: 10.1109/iccct2.2017.7972268.

[17] H. Tembine, E. Altman, and R. El-Azouzi, "Delayed evolutionary game dynamics applied to medium access control," in *Proc. IEEE Int. Conf. Mobile Adhoc Sensor Syst.*, Pisa, Italy, Oct. 2007, pp. 1–6, doi: 10.1109/mobhoc.2007.4428684.

[18] J. S. Baras and T. Jiang, "Cooperative games, phase transitions on graphs and distributed trust in MANET," in *Proc. 43rd IEEE Conf. Decis. Control (CDC)*, Nassau, Bahamas, Dec. 2004, pp. 93–98, doi: 10.1109/cdc.2004.1428612.

[19] Y. Xie and Y. Zhang, "A secure, service priority-based incentive scheme for delay tolerant networks," *Secur. Commun. Netw.*, vol. 9, no. 1, pp. 5–18, Jan. 2016, doi: 10.1002/sec.1372.

[20] L. Buttyán and J.-P. Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks," *Mobile Netw. Appl.*, vol. 8, no. 5, pp. 579–592, 2003, doi: 10.1023/A:1025146013151.

[21] B. Srikanth, "Detecting selfish nodes in MANETs," Ph.D. dissertation, Dept. Comput. Sci. Eng., Nat. Inst. Technol., Rourkela, India, 2014.

[22] S. Nobahary and S. Babaie, "A credit-based method to selfish node detection in mobile ad-hoc network," *Appl. Comput. Syst.*, vol. 23, no. 2, pp. 118–127, Dec. 2018, doi: 10.2478/acss-2018-0015.

[23] J. Zheng, Y. Wu, N. Zhang, H. Zhou, Y. Cai, and X. Shen, "Optimal power control in ultra-dense small cell networks: A game-theoretic approach," *IEEE Trans. Wireless Commun.*, vol. 16, no. 7, pp. 4139–4150, Jul. 2017, doi: 10.1109/TWC.2016.2646346.

[24] J. Zheng, Y. Cai, Y. Wu, and X. Shen, "Dynamic computation offloading for mobile cloud computing: A stochastic game-theoretic approach," *IEEE Trans. Mobile Comput.*, vol. 18, no. 4, pp. 771–786, Apr. 2019, doi: 10.1109/TMC.2018.2847337.

[25] K. Akkarajitsakul, E. Hossain, and D. Niyato, "Cooperative packet delivery in hybrid wireless mobile networks: A coalitional game approach," *IEEE Trans. Mobile Comput.*, vol. 12, no. 5, pp. 840–854, May 2013, doi: 10.1109/TMC.2012.46.

[26] Y. Li, X. Xu, Q. Cao, Z. Li, and S. Shen, "Evolutionary game-based trust strategy adjustment among nodes in wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 2, pp. 1–12, 2015, doi: 10.1155/2015/818903.

[27] S. Shen, L. Huang, E. Fan, K. Hu, J. Liu, and Q. Cao, "Trust dynamics in WSNs: An evolutionary game-theoretic approach," *J. Sensors*, vol. 2016, pp. 1–10, Apr. 2016, doi: 10.1155/2016/4254701.

[28] M. A. A. Al-Jaoufi, Y. Liu, Z.-J. Zhang, and L. Uden, "Study on selfish node incentive mechanism with a forward game node in wireless sensor networks," *Int. J. Antennas Propag.*, vol. 2017, pp. 1–13, Oct. 2017, doi: 10.1155/2017/8591206.

[29] Z. Chen, Y. Qiu, J. Liu, and L. Xu, "Incentive mechanism for selfish nodes in wireless sensor networks based on evolutionary game," *Comput. Math. Appl.*, vol. 62, no. 9, pp. 3378–3388, Nov. 2011, doi: 10.1016/j.camwa.2011.08.052.

[30] S. V. Sonekar, M. Pal, M. Tote, S. Sawwashere, and S. Zunke, "Computation termination and malicious node detection using finite state machine in mobile adhoc networks," in *Proc. 7th Int. Conf. Comput. Sustain. Global Develop. (INDIACom)*, New Delhi, India, Mar. 2020, pp. 156–161, doi: 10.23919/INDIACom49435.2020.9083710.

[31] R. N. Mir, "Secure distributed routing in mobile ad hoc networks using proactive secret sharing," in *Proc. 10th Int. Conf. Cloud Comput., Data Sci. Eng. (Confluence)*, Noida, India, Jan. 2020, pp. 459–463, doi: 10.1109/Confluence47617.2020.9058158.

[32] Y. Fu, G. Li, A. Mohammed, Z. Yan, J. Cao, and H. Li, "A study and enhancement to the security of MANET AODV protocol against black hole attacks," in *Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov. (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, Leicester, U.K., Aug. 2019, pp. 1431–1436, doi: 10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00259.

[33] R. Menaka, J. M. Mathana, R. Dhanagopal, and B. Sundarambal, "Performance evaluation of DSR protocol in MANET untrustworthy environment," in *Proc. 6th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Coimbatore, India, Mar. 2020, pp. 1049–1052, doi: 10.1109/ICACCS48705.2020.9074268.

[34] Y. M. Monakhov, M. Y. Monakhov, and A. V. Telny, "Method for local positioning of the node violating information security in mobile networks intrusion detection systems," in *Proc. Dyn. Syst., Mech. Mach. (Dynamics)*, Omsk, Russia, Nov. 2019, pp. 1–7, doi: 10.1109/Dynamics47113.2019.8944409.

[35] U. Amin and M. A. Shah, "A novel authentication and security protocol for wireless adhoc networks," in *Proc. 24th Int. Conf. Autom. Comput. (ICAC)*, Newcastle upon Tyne, U.K., Sep. 2018, pp. 1–5, doi: 10.23919/IConAC.2018.8748982.

[36] A. Sahnoun, A. Habbani, and J. El Abbadi, "A coalition-formation game model for energy-efficient routing in mobile ad-hoc network," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 1, pp. 26–33, 2018.

[37] X. Qin, X. Wang, L. Wang, Y. Lin, and X. Wang, "An efficient probabilistic routing scheme based on game theory in opportunistic networks," *Comput. Netw.*, vol. 149, pp. 144–153, Feb. 2019, doi: 10.1016/j.comnet.2018.11.022.

[38] N. Samian, Z. A. Zukarnain, W. K. G. Seah, A. Abdullah, and Z. M. Hanapi, "Cooperation stimulation mechanisms for wireless multihop networks: A survey," *J. Netw. Comput. Appl.*, vol. 54, pp. 88–106, Aug. 2015, doi: 10.1016/j.jnca.2015.04.012.

[39] A. Al Sharah, M. Alhaj, and M. Hassan, "Selfish dynamic punishment scheme: Misbehavior detection in MANETs using cooperative repeated game," *IJCSNS*, vol. 20, no. 3, pp. 168–173, 2020.

[40] S. S. Joshi and S. R. Biradar, "Communication framework for jointly addressing issues of routing overhead and energy drainage in MANET," *Procedia Comput. Sci.*, vol. 89, pp. 57–63, Jan. 2016, doi: 10.1016/j.procs.2016.06.009.

BURHAN UL ISLAM KHAN (Graduate Student Member, IEEE) received the B.Tech. degree in CSE from IUST, Kashmir, and the M.S. degree in CIE from International Islamic University Malaysia (IIUM), Kuala Lumpur, in 2014, where he is currently pursuing the Ph.D. degree in engineering. He has been involved in varying roles as that of a Software Engineer, a Research Analyst, and an Assistant Professor. His current research interests include designing one time password schemes, employing mechanism design, and game theory to protect ad-hoc networks.

FARHAT ANWAR (Member, IEEE) received the Ph.D. degree in electronic and electrical engineering from the University of Strathclyde, U.K., in 1996. Since 1999, he has been with International Islamic University Malaysia, where he is currently working as a Professor with the Department of Electrical and Computer Engineering. He has published extensively in international journals and conferences. His research interests include QoS in IP networks, routing in ah-hoc and sensor networks, computer and network security, network simulation and performance analysis, the IoT, and biometrics.

RASHIDAH FUNKE OLANREWAJU (Senior Member, IEEE) was born in Kaduna, Nigeria. She received the B.Sc. degree (Hons.) in software engineering from the University of Putra Malaysia, in 2002, and the M.Sc. and Ph.D. degrees in computer and information engineering from International Islamic University Malaysia (IIUM), Kuala Lumpur, in 2007 and 2011, respectively. She is currently an Associate Professor with the Department of Electrical and Computer Engineering, IIUM, where she is leading the Software Engineering Research Group (SERG). Her current in hand projects revolve around MapReduce optimization techniques, compromising secure authentication and authorization mechanisms, secure routing for ad-hoc networks, and formulating bio-inspired optimization techniques. She is an Executive Committee Member of technical associations, such as the IEEE Women in Engineering, the Arab Research Institute of Science and Engineers, and so on. She represents her university, IIUM, at Malaysian Society for Cryptology Research.

BISMA RASOOL PAMPORI received the B.Tech. degree in computer science and engineering from the Islamic University of Science and Technology, India, in 2015, and the M.Tech. degree in information technology from the Central University of Kashmir, India, in 2018. She has several publications with respect to her work in the field of network security, the IoT, and adhoc networks.

ROOHIE NAAZ MIR (Senior Member, IEEE) received the B.E. degree (Hons.) in electrical engineering from the University of Kashmir, India, in 1985, the M.E. degree in computer science and engineering from IISc Bangalore, India, in 1990, and the Ph.D. degree from the University of Kashmir, in 2005. She is currently a Professor and the HoD of the Department of Computer Science and Engineering, NIT Srinagar, India. She is the author of many scientific publications in international journals and conferences. Her current research interests include reconfigurable computing and architecture, mobile and pervasive computing, blockchain technology, and security and routing in wireless ad-hoc and sensor networks. She is a Fellow of IEI and IETE India, and a member of IACSIT and IAENG.