IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 8, 2021, accepted April 12, 2021, date of publication April 14, 2021, date of current version April 29, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3073343

Game Theory Analysis and Modeling of Sophisticated Multi-Collusion Attack in MANETs

BURHAN UL ISLAM KHAN[1], FARHAT ANWAR[1], (Member, IEEE), RASHIDAH F. OLANREWAJU[1], (Senior Member, IEEE), MISS LAIHA BINTI MAT KIAH[2], (Senior Member, IEEE), AND ROOHIE N. MIR[3], (Senior Member, IEEE)

[1]Department of Electrical and Computer Engineering, Kulliyyah of Engineering, International Islamic University Malaysia (IIUM), Kuala Lumpur 53100, Malaysia
[2]Department of Computer System and Technology, University of Malaya (UM), Kuala Lumpur 50603, Malaysia
[3]Department of Computer Science and Engineering, National Institute of Technology (NIT), 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 Mobile Adhoc Network (MANET) has been a core topic of research since the last decade. Currently, this form of networking paradigm is increasingly being construed as an integral part of upcoming urban applications of Internet-of-Things (IoT), consisting of massive connectivity of diverse types of nodes. There is a significant barrier to the applicability of existing routing approaches in conventional MANETs when integrated with IoT. This routing mismatch can lead to security risks for the MANET-based application tied with the IoT platform. This paper examines a pragmatic scenario as a test case wherein the mobile nodes must exchange multimedia signals for supporting real-time streaming applications. There exist two essential security requirements viz. i) securing the data packet and ii) understanding the unpredictable behavior of the attacker. The current study considers sophistication on the part of attacker nodes. They are aware of each other's identity and thereby collude to conduct lethal attacks, which is rarely reflected in existing security modeling statistics. This research harnesses the potential modeling aspect of game theory to model the multiple-collusion attacker scenario. It contributes towards i) modeling strategies of regular/malicious nodes and ii) applying optimization principle using novel auxiliary information to formulate the optimal strategies. The model advances each regular node's capability to carry out precise computation about the opponent player's strategy prediction, i.e., malicious node. The simulation outcome of the proposed mathematical model in MATLAB ascertains that it outperforms the game theory's baseline approach.

INDEX TERMS Colluder, game theory, mobile adhoc network, multi-collusion attacker, multistage game, secure routing.

I. INTRODUCTION

The advanced wireless devices and communication standards provisions next-generation networks that synchronize a MANET as a bridge or sub-network to facilitate many opportunistic applications. The MANET utilities are becoming more popular than ever because it inherits characteristics of flexibility and support of mobility in the unpredictable environmental conditions where establishing a fixed infrastructure is not feasible [1]. This possibility of the utility's extensibility is becoming popular because the evolution of the Software-Defined Network (SDN) inclusion brings centralized control instead of the MANET's distributed nature constraints. One such application network architecture is described as hydropower plant monitoring by collaborating the mobile node with the SDN controller [2]. The security perspective explores the potentialities of combined or exponential possibilities as additional vulnerabilities are imposed due to the inclusion of SDN and MANET vulnerabilities alone. The devices and communication protocols' heterogeneities provide higher opportunities to the invaders to collaborate into the existing network, and a weak or interoperable authentication process substantiates many collusive attacks to happen. The ever-gaining popularity of mobile computing and telecommunication for voice and video-based communication gets its extension with BitTorrent like video streaming system through the MANET even if in the harsh conditions but a simple effort intruder evades the possibilities

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

of failure of such systems [3]. Another extensive use of the MANET is to realize the vehicular network's safety and information and entertainment applications. The attacks in this networking paradigm aim to exhaust the computing and memory resources, energy usage, and the communication channel bottleneck challenges. An attack pattern resembling cooperative caching character further poses resource utilization challenges [4], [5].

The design challenges for routing protocols in very high-speed scenarios of the nodes for the desired quality of service face the radio link disruptions' attribution. An attacker's intent to do so further complicates the design of the routing process [6]. A content-centric MANET faces similar challenges due to path disruptions [7]. The use of MANET, along with the Internet of Things (IoT), enables opportunistic connectivity. However, at the same time, it also brings a unique challenge in the combined IoT and MANET collaborative network that demands a suitable and effective authentication mechanism for the device verifications [8], [9]. Moreover, MANET and Wireless Sensor networks' convergence facilitates a unified platform for the real sense of global connectivity through the IoT system. The adversary always attempts to bring data routing challenges in these heterogeneity conditions against the optimal link-state routing protocols [10].

Recent discussions of ongoing research work towards transmitting video and multimedia messages between vehicular nodes are given in the works [11]–[15]. Such work currently addresses issues about congestion [11], quality of experience [12], streaming video among vehicles [13], improving routing scheme [14], and route reliability [14]. Such research contributes to evolving up with novel multimedia exchanging operations in the vehicular network for an upcoming application. This is the primary motivating factor to showcase that the vehicle's futuristic communication will be high-end streaming multimedia data. However, security is not the primary concern of such research attempts. Apart from this, the surveillance systems in the strategic conditions adopt unmanned mobile vehicles or devices as in MANET to acquire real-time images or video of situations. The intruders may attempt to bring disturbances into the time slot scheduling processes [15]. An e-payment system in the disaster area faces connectivity challenges as the conventional payment system is communication infrastructure dependent. Such a system requires multilevel endorsements, where the intruders may try to impose communication overheads [16]. MANET plays an essential role in bridging communication links in all those harsh conditions where the infrastructure-based networks frequently face the network partitions, so securing MANET for such situations is quite significant [17]. Security has always been a primary concern in MANET owing to its decentralized mechanism of communication. MANET is exposed to various forms of lethal threats [18]–[21]. During the past decade, the security of MANETs has been studied by many researchers [22]–[24]. Out of all the different security threats, a collusion attack is one potential security threat in MANET, where there is a smaller number of standardized solutions at present. Therefore, there is a need to evolve up with a solution where multi-attacker collusion can be addressed for the mobile nodes, facilitating secure dissemination of heavier data in MANET.

The proposed work is an extension of our prior game model [25], [26] towards malicious behavior detection. A novel game modeling has been carried out towards multi-attacker collusion threat in MANET with a cost-effective solution. The contribution of the proposed study is briefed as follows: i) To explore the possible connections between different forms of threats of multi- collusion attack over disruption, it creates over the network behavior, ii) The proposed system formulates the multi-collusion attack in the form of the optimization problem to explore a better solution for effective controlling of the disruption, iii) The model also introduces a concept of auxiliary information which improves the identification performance if the identifier node is furnished with this information, iv) A multilevel game model is developed which formulate the identification followed by prevention of the multi-collusion attack.

The present manuscript's organization is as follows: Section II briefs about the existing approaches to resist a collusion attack, highlighting the encountered unaddressed issues from existing studies follows it. Section III briefs about the proposed methodology. Deliberation of the system design carried out is also discussed in this section, while the implemented game strategy modeling is illustrated in Section IV. Section V discusses the optimized risk mitigation modeling, and the discussion of the outcomes of the simulation study is carried out in Section VI. The summary of the paper is provided in Section VII, and references are listed at the end.

II. EXISTING APPROACHES

Various existing approaches have been contributed towards resisting collusion attacks in the case of MANET. This section discusses the frequently adopted approaches for securing MANET, followed by a briefing of significant research problems.

A. FREQUENTLY ADOPTED APPROACHES

There are various categories of approaches being identified in the existing system, which are briefed as follows:

1) COLLUSION-AVOIDANCE SCHEME

This approach is mainly associated with identifying the colluded data and implements a policy to resist them. Most of the current methods have used routing based on multipath [27], [28], which is significant for collusion. A collusion avoidance strategy has been used to address such issues [29]. Another recent work carried out in [30] has used blockchain technologies and digital signatures to resist spoofing and colluding attacks. The study ensures a better form of decentralized security in an ad-hoc network.

2) ENCRYPTION-BASED SCHEME

These schemes apply a specific form of message encoding in ad-hoc networks. They are also relatively straightforward towards specific vulnerable scenarios in communication. The authors' work in [31] has employed flooding for identifying adversaries while the prevention towards it is carried out by using an encryption-based approach. Various works of literature have also emphasized resisting collusion considering vehicular ad-hoc networks. The approaches presented by authors in [32]–[34], and [35] have mainly used an encryption-based strategy first to identify collusion attacks and then resist them. These models also compute trust and confirm its decision about the colluders in a specific communication environment. Another detection-based approach is proposed in [36], where an acknowledgment is utilized to identify a collusion attack. A validation-based strategy to avoid collusion packets within the network is carried out in [37]. An observation-based detection approach is also seen in the work [38], where multiple collusion attacks have been addressed.

3) TRUST-BASED SCHEME

The trust-based approach is a frequently used approach for resisting collusion in MANET. The technique used in [39] emphasizes validating the neighboring mobile nodes' recommended trust. Another unique trust-based model has been presented in [40], where a clustering mechanism is applied along with extensive rule constructs in fuzzy logic. The model offers punishment/rewards based on the actions taken by the nodes. A similar direction of work has also been carried out in [41]. The unnecessary mobile nodes are eliminated from the clustering process by considering two essential parameters, viz., the rate of route encounters and several standard transmissions.

4) GAME-THEORY-BASED SCHEME

At present, game theory has been making a mark in securing mobile ad-hoc network communication. Typical cases of such implementations are presented in the works of [42]–[47], and [48]. These authors have presented different modeling approaches; however, the game model's baseline considering two players is nearly identical. The distinction is carried out in constructing different identification and resisting logic. A review of these literary works shows that such models are generally based on the concept of malicious-behavior identification where the extent of using conventional encryption is significantly less. Hence, this gives insight into how game theory's adoption is a cost-effective modeling practice for understanding unpredictable malicious nodes' uncertainty behavior. However, less work is carried out considering the collusion attack, specifically using game theory. The next section discusses the issues of literature.

B. RESEARCH PROBLEM

As highlighted in the first part of Section II, there are various forms of approaches towards resisting collusion threats in mobile Adhoc networks. All the approaches are proven to contribute towards solving security threats to some extent; however, still, certain issues are explored to be unaddressed, which are briefed as follows:

- *Less emphasis over collusion-based security threats*: The majority of MANET's collusion-based problems are represented concerning routing issues and not much towards security issues. Whereas, in reality, it brings irreversible consequences if a collusion attack is carried out. Existing approaches emphasize conventional forms of other attacks in MANET, e.g., Sybil attack, wormhole attack, denial of service, etc. Still, a small number of studies are carried out towards addressing collusion attacks in MANET.
- *Incomplete Scenario of Collusion Attack*: Majority of the collusion attack in MANET has only considered the presence of attacker (or colluder) and its security solution calls for resisting them. However, the scenario which is not considered is that an attacker will not instantly introduce a collusion attack without judging the security strength of an environment that it is targeting to intrude. The attacker must assess the cost of attack and gain obtained from introducing a collusion attack to intrude. In the initial communication phase, the value of gain obtained from the attack is less than the cost incurred in launching the collusion attack. The attacker node will attempt to gain trust by assisting in data forwarding. The attack only happens when the gain of attack is more than the cost. Such a realistic assumption is found to be lacking in any form of conventional encryption-based approach.
- *Computationally Complex Solution*: Several commonly employed approaches, e.g., trust-based evaluation, encryption, game theory, etc., are computationally intensive processes owing to the inclusion of sophisticated logic. The trust-based approach requires a constant update and thus needs to be iterative in its operation. The encryption-based method needs memory to store and manage its secret key, while the game theory-based approach requires strategy modeling using practical logic. Although the existing approach has a proven better result, there is no sufficient evidence about their cost-effectiveness nature of implementation. Without controlling computational cost, a security solution is likely offered in MANET at the expense of violating the practical constraint of resource-limited mobile nodes.

Therefore, there is a need for developing a novel and cost-effective approach for offering much-needed security. Game theory has been identified to contribute to efficient modeling provided the logic of strategy adopted is developed considering the practical scenario of MANET. Therefore, a new version of game modeling is carried out to address the proposed system's above issues.

Table 1 highlights the trade-off factor being explored from existing dominant approaches towards securing a MANET collusion attack.

TABLE 1. Summary of research Tradeoff.

Schemes	Capabilities	Trade-off
Collusion Avoidance	-Enhanced routing operation	-Lacks comprehensive detection of colluders
Encryption-based	-Identification of colluders -Sophisticated ciphering of data	-High-end encryption demands consistent resource availability -Identification specific to one form of attack pattern
Trust-based	-Effective clustering mechanism -Can rule out the anomaly in the detection process	-Intermittent trust update allows dynamic adversaries to access-trust information
Game Theory-based	-Can frame-up practical world condition	-Lacks fairness in assuming higher strength for an attacker

A closer look into the table will highlight that although existing security approaches offer enhanced capabilities, they are still insufficient to offer a higher degree of resiliency in dynamic threat scenarios. The existing collusion avoidance mechanism mainly focuses on routing operation, whereas the attacker's full-fled identification is still not included. Encryption-based approaches are efficient if the attacker's identity is known; however, they are limited to a specific form. Apart from this, they demand more resources to carry out their operation, which is slightly unpractical concerning resource-restricted nodes. From a trust-based scheme, it is noticed that the available studies within it have higher possibilities to rule out anomalies associated with malicious nodes. However, when the topology is dynamic, updating trust is very much important. The majority of the on-demand routing approaches in MANET use stale information (e.g., Adhoc On-Demand Distance Vector routing), which has a higher likelihood of getting compromised when subjected to the dynamic topology. Out of all these approaches, game theory is a much better version as it offers a compact mathematical model considering all possible attacks. It also assists in identifying the malicious nodes based on the written logic of game interactivity. However, all the major work studies associated with game theory identify attacker identification with multiple theories based on staged games. Such a scheme lacks fairness for malicious node potential, without which potential adversary modeling cannot be carried out. This problem is addressed in current work where an optimized risk mitigation strategy is formulated considering potential adversaries.

III. PROPOSED METHODOLOGY

The proposed system primarily emphasizes modeling game theory as a solution to security issues considered in the study, i.e., multi-collusion attack. It was seen from prior Section II and Section III that existing solutions based on game theory have better chances of modeling the security system. The prime threat of communication in MANET is its dynamic topology and its decentralized approach to implementation. Due to this, it is nearly impossible for a common node to check the authenticity of another node that is attempting to get itself connected to the former. In such a case, a regular node relies only on its decision capabilities in such an uncertain scenario. This is the perfect situation where game modeling fits in. Harnessing the potential concept of game theory, the common node can be imparted with the potential to realize the degree of severity of intrusion and can identify the malicious behavior. Apart from this, the applicability of the game theory in real-world networking has been discussed in the works of [49], [50], and [51]. According to these findings, game theory perfectly suits in controlling the node behavior over wireless networks. This fact offers significant justification for realizing game theory as the most suitable solution in modeling practical world communication in MANET.

A. ARCHITECTURE MODELLING

It should be noted that there is no commercial application of game theory in MANET. Owing to the usage of this novice concept in MANET, it is still under the roof of research and development. However, the research mentioned above work offers better credibility and mathematically constructed justification to advocate game theory usage in MANET.

Adopting a mathematical approach, the proposed system is a dedicated, cost-effective architecture that applies game theory to model multi-attacker collusion threat in MANET. The study considers a dynamic and decentralized environment, where the mobile nodes exchange multimedia signals among each other as a part of supporting any upcoming IoT applications using MANET. Therefore, this implementation's sole idea is to ensure secure signal transmission by providing a decentralized and dynamic assessment of the open-end mobile nodes in the transmitting nodes' vicinity. The proposed system has jointly modeled both regular node and malicious node in its game framework. There is a higher chance that malicious nodes will never introduce any attack in the preliminary communication stages. It is because they will have a lesser trust, which increases the risk of getting themselves caught. Therefore, the proposed model hypothesizes that when any node acquires a certain form of sensitive information called auxiliary information, it will have the right next move for its opponent. This gives the proposed model a chance to prove its resistivity against a potential multi-collusion attacker. However, for an extended discussion of the model, regular and attacker operations are discretely discussed under different environments. The architecture developed as a solution is exhibited in Fig. 1.

The security is imposed in the proposed system by two phases. In the first phase, this implementation's core idea is as follows: the transmitting node embeds a secret digital code within the data and forwards it to the receiver. In contrast, the receiver assesses the received data, extracts the secret digital code, and authenticates themselves and the received data. The core emphasis is developing a unique game model and modeling multi-adversaries of collusion in the second phase. The game modeling approach consists of constructing the strategies for both regular and adversary nodes, capable

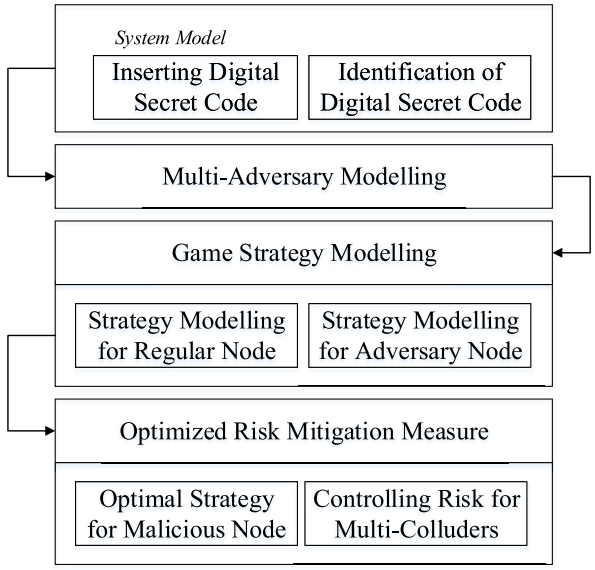

FIGURE 1. Architecture of proposed game model for resisting multi-attacker collusion threat in MANET.

of sensing each opponent's countermeasures. The proposed system also introduces a novel optimized approach towards risk mitigation, which can deploy an analytical means to estimate auxiliary information. This auxiliary information is used by players (regular/malicious mobile nodes) of the multistage games to assess the degree of severity of the risk incurred in adopting a particular set of actions. The proposed system's contribution is to perform a correct measure of risk associated with the adoption of attacker strategy, and hence a potential adversarial model is built. Finally, the model assists in offering an optimal strategy and controlling risk for multi-colluders in the presence of MANET's dynamic environment. The model, therefore, contributes mainly towards intrusion detection as well as prevention system. The next section discusses system design.

B. SYSTEM DESIGN

The proposed system deploys a unique game theory model to model the multi-collusion attack and countermeasure to resist this form of attack. The proposed modeling is carried out considering three distinct modules viz. incorporation of the digital code in the relayed signal from a mobile node, identification of digital code, and adversary modeling using game theory.

1) INCORPORATION OF DIGITAL CODE

This module is responsible for inserting a unique digital secret code within the signal forwarded from one mobile node to another in MANET. Due to the lack of any centralized trusted authority in MANET, this digital code is forwarded without any authorization, extracted by the user to obtain the same digital code. The extraction process offers information about the origination point of data leakage. The proposed system formulates a mathematical expression for this incorporation of secret digital code,

$$g_a(t) = [S(t)|\alpha_a(t)] \tag{1}$$

In the above expression (1), the function $g_a(t)$ is a digital code incorporation process that performs concatenation of original signal $S(t)$ and secret digital code $\alpha_a(t)$ considering t^{th} chunk of the host signal and the number of specific users a. To secure the digital code for achieving non-traceability, the proposed system uses $\tau(t)$ as an imperceptibility parameter used to fine-tune the energy associated with the incorporated digital secret code. To prevent multiple collusion attacks, the proposed study correlates the secret digital code $\alpha_a(t)$ for the neighboring chunks of data for the similar mobile nodes a with themselves. The proposed system defines a mathematical expression to compute the correlation of the host chunk of signal with the temporal difference as follows:

$$\Phi[a] \rightarrow \lambda^{\Delta t}[\Phi(S(t))] \tag{2}$$

In the above expression (2), the variable Φ represents the evaluation of the coefficient of correlation occurring between two secret digital codes $\alpha_a(t_1)$ and $\alpha_a(t_2)$ taken randomly. Hence, in expression (2), $\alpha = \{\alpha_a(t_1), \alpha_a(t_2)\}$ the estimation of the coefficient of correlation is as follows:

$$\Phi\left(v(\alpha_a(t_1), v(\alpha_a(t_2)\right) = \frac{c\left(\alpha_a(t_1), \alpha_a(t_2)\right)}{\sqrt{v(\alpha_a(t_1).v(\alpha_a(t_2)}} \tag{3}$$

The above expression (3) is used for computation of the LHS part of the expression (2), considering c as covariance. In contrast, the RHS part includes a variable λ associated with the scaling factor using exponent $\Delta t = |t_1 - t_2|$. The numerical range of the scaling factor λ is [0 1] used to fine-tune the signal quality, possibly affected by the proposed system's mitigation process. It will eventually mean that the quality of resistivity will be optimal when the value of λ is higher. There is also a possibility of degradation in the signal's quality with an embedded digital secret code. On the other hand, if the value of the scaling factor λ is reduced, then the signal quality will be less degraded. Still, there is also a higher possibility of collusion attack in the presence of multiple attackers.

2) IDENTIFICATION OF THE DIGITAL CODE

After the previous process of incorporating the digital code is carried out, it will permit the mobile node (owner of content) to confirm a suspicious copy of the signal data. Identifying the adversary can be carried out with the usage of correlation-based identification of secret digital code. The extraction of the secret digital code $\alpha'_a(t)$ by the receiver, the mobile node can be carried out by obtaining the difference of extracted frame $g'_a(t)$ and signal $S(t)$. Using a statistical approach, the proposed system permits all users that have the possession of received chunk of data t as follows:

$$\eta_a(t) = \frac{\alpha_a^T(t).\alpha'_a(t)}{\sqrt{\alpha_a^T(t).\alpha_a(t)}} \tag{4}$$

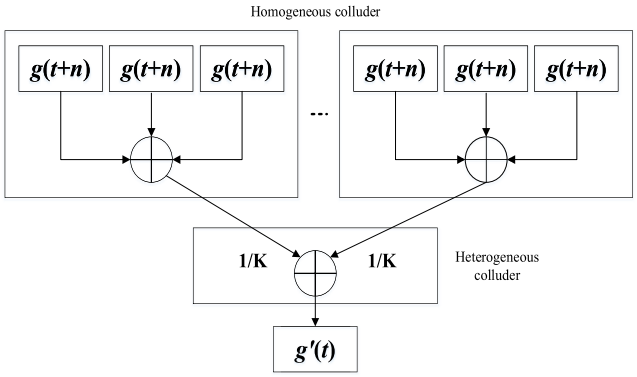

FIGURE 2. Proposed model of multi-attacker collusion with different levels of severity concerning digital code incorporation.

In the expression (4), η is the statistically computed identity of digital code where a threshold value of the identification cut_{off} is used for the number of attackers in one chunk of signal t as i satisfying the condition that $\eta_i\,(t) > cut_{off}$.

3) MULTI-ADVERSARY MODELLING FOR COLLUSION

The proposed study considers the use case of a multi-collusion attack where K is the number of cumulative attackers. With reference to Fig. 2, all the adversaries carry out the collusion attack with the aid of a time-based elimination process over the sequential chunks of the data relayed by the mobile nodes in MANET. This leads to higher chances of collusion among attackers to initiate multi-collusion attacks. In the proposed system, the secret digital code for all the signals associated with multiple adversaries is not dependent on each other, and they are distributed identically. Hence, assuming that all the adversaries share a similar risk, they will be assigned with an equal weight coefficient for all the severity levels in implying collusion attack.

Therefore, the mathematical representation of a mobile node's colluded signal in MANET is given as,

$$g'_a\,(t) = \sum_{k=1}^{K} K^{-1}[\sum_{i=-h}^{h} \beta_i.g_a(t+1)] \tag{5}$$

In the above expression (5), the variable β_i The adversary selected to control the disruption that occurred due to collusion considering specific constraints of risk. The variable K is the total attackers present at the instantaneous time. On the other hand, the regular node performs an estimation of β_i selected by the adversary to enhance the identification performance.

IV. GAME STRATEGY MODELLING

From our prior work [52], it is proven that an attacker node, irrespective of its kind, initiates computation of trust before launching an attack. This computation of trust is carried out by neighborhood monitoring of the target mobile nodes, where the attackers mainly assess the risk of getting caught. It was also known that game modeling was carried out in our prior work where regular nodes and malicious nodes are considered specific sets of actions and strategies to be deployed. The complete modeling was carried out to achieve the Nash Equilibrium stage. A similar strategy is adopted in the proposed system, assuming that a common node utilizes the secret digital code of the existing chunk of signal data to assess the risk statistics associated with adversary identification. Assuming that the adversary uses a known set of attack strategies to corrupt the secret digital code, the common node will perform an amendment over the statistics of the identification to enhance the performance of the identification of malicious nodes.

Similarly, if the adversaries possess the knowledge of the regular node's mitigation strategy, they will further alter their strategy accordingly. This is done to ensure the fairness incorporation in the multistage game using Nash Equilibrium. Hence, the proposed system formulates a game modeling of multi-attacker collusion. The strategy to be adopted by either of the nodes depends on their opponents' mobile nodes' strategy in MANET. Using our initial modeling concept [43], the proposed study considers that a coefficient γ exists, responsible for determining the best set of strategies adopted by the mobile nodes. Henceforth, the coefficient γ can be represented as auxiliary information required to be computed by both types of mobile nodes.

A. ADOPTED STRATEGY OF REGULAR NODE

In this part of the proposed study, the regular nodes assume that the malicious node adopts a known linear strategy with γ to launch an attack over the secret digital code. In such a case, the common node will perform an amendment towards the identification statistics discussed in the prior section. Assuming that the regular node makes use of different permutation and combination of the secret digital code linearly (to reduce the cost of attack as per the concept present in [52]), i.e., $\alpha_a\beta$ to assess the statistics of identification, the mathematical expression of the statistics associated with the identification can be stated as,

$$\eta'_a\,(t) = d_1.d_2[\delta(e_s + K^{-1}\sum_{i=1}^{K} \alpha_i)] \tag{6}$$

In the above expression, the variable d_1 will signify $1/(|\alpha_a\beta|)$ and $d_2 = \beta^T\alpha_a^T.\gamma_a$. A closer look at expression (6) will show that $\eta'_a\,(t)$ is a normal distribution. Hence, the form of the expression constructed will offer higher reliability in identifying adversaries if they are multiple. The expression (6) is also applicable and valid if the attacker formulates any dynamic strategy for launching an attack. Therefore, to facilitate the reliable identification of the adversary by the regular node, the proposed system further computes the probability of risk associated with the adversary as,

$$\text{risk} = H_1 - d_3.H_2 \tag{7}$$

The above expression (7) is used for computing the risk probability *risk*, assuming that the probability of outlier detection is τ. The first component H_1 will represent $[w.(|\Lambda\beta|)]^{-1}$ whereas the second component $d_3 = (1/K)E$ and the third component H_2 will signify $[(\beta^T\alpha_a^T\alpha_a\gamma)/|\alpha_a\beta|]$

respectively, where w is Gaussian tail function. Therefore, according to the game theory model discussed in [43], it will mean that a regular node will opt for the better version of the score of β to increase the higher feasibility of capturing the accurate information of the colluders. This operation will also pose a more significant threat to the attacker. Further, a closer look at expression (7) will also mean that if the risk factor *risk* is maximized, it will also increase the score of $E(H_2)$ that will finally yield a novel version of the variable γ_χ, which is equivalent to γ_β. The above formulation of the regular node to perform identification states that if the regular node estimates the adversary's information to deploy the linear elimination process with the better version of γ_β to intrude the secret digital code, then it is feasible for the regular node to deploy $\alpha_a \gamma_\beta$ to estimate the statistics of the identification. This offers a reliable and optimal performance of identification on behalf of the regular node.

B. ADOPTED STRATEGY OF MALICIOUS NODE

To deploy the concept of rational sequentially discussed in our prior work [52], the proposed system offers equal fairness potential to the adversary nodes. In this case, the adversary can possess the information of strategy adopted by the regular node. The attacker will know about adopting the linear elimination process adopted by the regular node with γ_β to estimate the statistics of identification. In such a case, the adversary will attempt to minimize risk by deploying the next version of the linear elimination process to attack the secret digital code. Considering a novel coefficient for an attacker as β to launch an attack, the amended form of the statistics associated with the identification is as follows:

$$\eta_a^{''}(t) = d_1'.d_2'[\delta(e_s + K^{-1}\sum_{i=1}^{K}\alpha_i)] \tag{8}$$

In the above expression (8) for new identification statistics $\eta_a^{''}(t)$, the variable d_1' will signify $1/(|\alpha_a\gamma|)$ and $d_2' = \gamma^T.\alpha_a^T.\beta$. A closer look into expression (8) will show that it is nearly equivalent to the expression (6), and hence they both satisfy the demands of normal distribution. A similar strategy of risk associated with the identification of the attacker can be now stated as,

$$\text{risk} = H_1 - d_3.H_2 \tag{9}$$

This expression (9) represents the computed value of risk probability *risk*. This is carried out with an assumption that there is an inclusion of outlier τ. The primary component H_1 bears a similar representation of $[w.(|\Lambda\beta|)]^{-1}$ while the secondary component represents $d_3 = (1/K)E$. The component H_2 will signify $[(\gamma^T\alpha_a^T\alpha_a\beta)/|\alpha_a\gamma|]$.

The prime objective function of the proposed system will be to minimize this risk probability such that the value of $\beta_T a_\beta$ resides between the higher and lower value of the disruption χ and χ_0 respectively, owing to utilization of γ_χ for the multi-attacker collusion. However, it is known that the proposed system makes use of the Gaussian tail function $w(x)$, which is a function with linear reducing order where the objective function can be amended as follows:

$$\begin{aligned} f_{\text{obj}}(x): \ & arg_{\min}(H_2) \\ & \text{s.t. } [\chi = \beta_T a_\beta < \chi_0] \end{aligned} \tag{10}$$

which is very much similar to the following

$$\begin{aligned} f_{\text{obj}}(x): \ & arg_{\min}(\beta, l) \\ & \text{s.t. } H_2 - l|\Lambda\beta| < 0 \\ & \text{s.t. } [\chi = \beta_T a_\beta < \chi_0] \end{aligned} \tag{11}$$

The above objective function is a research problem that is now feasible to solve iteratively for accomplishing the state of optimized identification.

$$\begin{aligned} & f_{\text{obj}}(t): H_2^t - l|\Lambda\beta^t| \\ & \text{s.t. } [\chi = \beta_T^t a\beta_t < \chi_0] \end{aligned} \tag{12}$$

For all the above expressions (10)-(12), the product of l^T and β^t is unity (i.e., 1). The evaluation of a variable l over $(t+1)$ is carried out as $H_2/|\Lambda\beta^t|$. This formulation will further lead to two possible cases: i) Considering all the individual iterations, if the value of l is less than 0, then the proposed system formulates a convex optimization problem while numerical strategy can be used to obtain the global solution of the objective function, ii) Similarly, in case of the value of l to be more than 0, then the proposed system formulates non-convex optimization problem, that can be solved for obtaining the optimal local outcome using the approach discussed in [53].

V. OPTIMIZED RISK MITIGATION MEASURE

The prior section has discussed sequential rationality in the presented game modeling of two players (regular/malicious nodes). According to this formulation, the auxiliary information is utilized by both the players to deploy the optimal strategy. This strategy of adopting a discrete set of both the players' actions about adopting respective actions is based on the auxiliary information. However, in the real-world scenario, the malicious node will be required to apply their action at the initial level. Only after this adoption of action by the malicious node will the regular node use their mitigation strategy fixed in nature and act as an apriori information already possessed by the malicious node. In such a condition, the best policy that the malicious node can adopt is by solving the mathematical expression (10).

On the contrary, another scenario in the worst case will be when the attacker's strategy's complete information has a regular node. In such a case, the regular node adopts exactly the similar strategy adopted by the malicious node. Therefore, when such a condition arrives, the proposed system deploys an optimal risk mitigation measure. This implementation is carried out in two phases. The first phase is about the optimal strategy for malicious nodes, while the second phase is about controlling multi-colluder's risk.

A. OPTIMAL STRATEGY FOR MALICIOUS NODE

This strategy is adopted by the malicious node, which is assumed to deploy a linear elimination process considering β_β to launch a collusion attack over the secret digital code. In such a case, the regular node is anticipated to use $\alpha_a\beta_\chi$ to perform the optimal computation of identification statistics. In such a case, the new statistics of the identification is computed as follows:

$$\eta_a^{'''}(t) = d_1.d_2[\delta(e_s + K^{-1}\sum_{i=1}^{K}\alpha_i)] \tag{13}$$

In the above expression (13), the variable d_1 will signify $1/(|\alpha_a\beta_\chi|)$ and $d_2 = (\beta_\chi)^T\alpha_\alpha^T.\beta_\beta$. Further, the optimal mechanism also re-computes the risk factor *risk* as follows:

$$\text{risk} = H_1 - d_3.H_2 \tag{14}$$

As shown in expression (14), the evaluation of risk is carried out similarly with no change of H_1 and d_3. However, the component H_2 will now signify $[(\beta_\chi^T\alpha_a^T\alpha_a\beta_\beta)/|\alpha_a\beta_\chi|]$. In this case, a regular node will opt for an optimal value of β_χ to increase the chances of risk for attackers. Therefore, the attacker's possible situation will be when the regular node will have possession of complete information of the intrusion strategy of the malicious nodes β_β. In such a case, the new assessment of the risk is carried out as follows:

$$\text{risk}\left(\beta_\chi\right) = arg_{max}(\text{risk}) \tag{15}$$

From the perspective of the expression (15), it can be said that a smart attacker will possess the information about the collusion identification strategy adopted by the common node. In such a case, the malicious node can opt for optimal usage of β_β to reduce the possibility of risk as per expression (15). The proposed system further revises the expression (15) to explore an elite outcome of β_β, which is shown as follows:

$$f_{\text{obj}}(\text{risk}) = arg_{\min}[arg_{\max}(\text{risk}(\beta_\chi)) \tag{16}$$

Hence, expression (16) will be the only alternative strategy for the attacker to adopt considering sequential rationality. Apart from this, it is known from the regular node risk assessment (expression (9)) that $\chi_\chi = \chi_\beta$, which can be now used for amending the expression (17) as follows:

$$f_{\text{obj}}(\text{risk}) = arg_{\min}(H_1 - d_3.H_2) \tag{17}$$

In the above expression (17), the variable H_1 and d_3 remain the same, but H_2 is now amended as $|\alpha_a\beta|$, where the value of $\beta^T a\beta$ resides between the lower and optimal value of χ, i.e., χ and χ_0. A similar strategy like the previous section can be used for formulating the problem of optimization i.e.

$$\begin{aligned} f_{\text{obj}}(x): \; & arg_{\min}(\left|\alpha_a\beta^t\right| - l^t\left|\Lambda\beta^t\right|) \\ & \text{s.t. } \chi = \beta^{tT}a^t < \chi_0 \end{aligned} \tag{18}$$

In the above expression (18), it can be seen that as l^t is greater than 0, the problem of optimization in the proposed system is non-convex in its form. Hence, a similar strategy used in [44] can be adopted to solve this. Therefore, the proposed system offers a simplified form of computational modeling of multi-attacker collusion and its optimal strategy selection using game theory.

B. CONTROLLING RISK FOR MULTI-COLLUDERS

The prior section discussed the optimal strategy that can be adopted by the colluders to resist the possibility of getting themselves exposed by the regular node. This section discusses another alternative approach that an attacker can further utilize to control risk from multi-colluders. In this mechanism, the attacker will corrupt the colluded copy to significantly minimize the risk of being exposed by the regular node in MANET. In this case, the challenge associated with introducing corruption along with collusion can be modeled mathematically as:

$$g'(t) = \sum_{a=1}^{K} K^{-1}\left[\sum_{i=-h}^{h} R\right] + H \tag{19}$$

In the above expression (19), the proposed system inserts malicious code to degrade the secret digital code's sensitive information. In this case, the variable H signifies artifacts introduced in the digital code.

$$\eta_a^{''''}(t) = d_1.d_2[\delta(e_s + K^{-1}\sum_{i=1}^{K}\alpha_i)] \tag{20}$$

In the above expression (20), the variable d_1 will signify $1/(|\alpha_a\beta_\chi|)$ and $d_2 = (\beta_\chi)^T\alpha_\alpha^T.\beta_\beta$, as well as the problem associated with the optimization, can be solved using the following objective function:

$$\begin{aligned} f_{\text{obj}}(x): \; & arg_{\min}(\left|\alpha_a\beta^t\right| - l^t\left|\Lambda\beta^t\right| + J) \\ & \text{s.t. } \chi = \beta^{tT}a^t < \chi_0 \end{aligned} \tag{21}$$

In the above expression (21), the additional variable J represents variance, and a similar concept is applied here by using [40] for evaluating the optimal local solution.

Therefore, the proposed system introduces explicit mathematical modeling capable of identifying multi-collusion attacks and resisting them with auxiliary information. Unlike existing game modeling approaches in MANET, the proposed system offers potential fairness in modeling multi-collusion attackers and offers solutions to resist them. Table 2 highlights all the notations that were employed for illustrating the game mathematical model.

VI. RESULT ANALYSIS

To assess the proposed game modeling of multi-collusion attack, the proposed study considered deploying 500 mobile nodes in the simulated area of 1000×1000 m^2 with a coverage range of 10 m. With the scripting carried out in MATLAB, the proposed system considered transmitting a real-time multimedia signal. A dataset of multimedia signals is used with high-definition videos that are considered a sign to be forwarded. To initiate the standard assessment, the proposed system considered the dataset from [54], which consists of all the multimedia files by extension of *.avi* files with a different variant of sizes of frames (90-1998 frames) as

TABLE 2. Symbols used in modeling.

Symbols	Meaning
$g_a(t)$	The function of the secret digital code
t	Specific signal frame
S	Original Signal Frame
α_a	The frame of secret digital code in multimedia
a	User
$\tau(t)$	Imperceptible parameter
Φ	Coefficient of correlation
λ	Scaling factor
Δt	Absolute signal difference
c	Covariance
v	Variance
$\eta_a(t)$	Digital code statistics for detection
$g'_a(t)$	Colluded signal
K	Total attackers at instantaneous time
β	Disruptive control parameter
h	Total signals
γ_a	Optimal coefficient
w	Gaussian Tail Function
χ/χ_0	The high and low range of disruption
δ	Network coefficient

well as resolution (176 × 144 to 325 × 240). The size of the data varies from 298 KB to 8.10 MB. All these multimedia datasets are collected in the form of frame sequences in order to assess the successful operation of the proposed logic in MATLAB. After the proof-of-concept is obtained from this dataset, the proposed system captures high-definition images with 1080 Megapixel from a digital camera and assess the proposed script in such images. The outcomes are recorded for 500 high-definition images and used for obtaining the numerical values for plotting the graphical outcomes. The proposed system uses a video processing toolbox in MATLAB to process the input multimedia file for both standard and high-definition multimedia. Although the standard dataset has ready images to be used, the proposed system still extracts the frame sequences from the multimedia video file to assess the effect of network and security over the MANET system. A similar process is applied for high-definition multimedia files by extracting the stream of images from the multimedia files. Each source mobile node allocates the stream of images in the form of a payload to its destination node, assuming malicious mobile node presence. All the streams being forwarded undergo the process of security algorithms discussed in the prior section.

A. ASSESSMENT OF MODEL

The proposed system used orthonormalization of vector sets using linear algebra to generate secret digital code followed by its scaling. The proposed implementation performed non-blind identification where the segregation of the core signal of the mobile host node is carried out from the colluded copy. The common node evaluates the statistics of identification to track the adversary. The proposed system's assessment is carried out by considering the parameter for the probability of outliers in identification configured to 10^{-5}. The proposed system assumes the experiment's risk to be a mean probability of accurate identification considering specific iteration rounds. The result is gathered by considering K's value to be 2 and 4, respectively, for two test multimedia files during the entire analysis. The proposed study evaluates risk in the form of probability to offer better inference and increase its applicability over dynamic scenarios. Similarly, the disruption parameter is calculated as the average value of the mean difference of two signals, i.e., the original signal and colluded signal. Hence, they bear no physical units. The proposed system considers a hypothetical model and experimental model to carry out comparative analysis for the convergence test. The hypothetical model consists of tentative values of risk obtained from assigning objective function in the worst case, while the experimental outcome is obtained by simulating the mobile nodes randomly. The risk is assessed concerning the signal quality received at the other end, and disruption of signal quality is defined as the statistical difference between the original and obtained signal.

Fig. 3 highlights that the increase in the number of attackers K doesn't significantly impact the proposed system concerning experimental and hypothetical outcomes. The degree of disruption of the signal is low for a higher value of K, and risk is spontaneously being minimized in a faster manner. The next part of the analysis shown in Fig. 4 is the continuation of the investigation towards exploring the possible relationship between risk and disruption for the increasing set of test iterations. With a higher risk probability, there is an eventual disruption (Fig. 4(a)) considering the value of $K = 2$. However, if K's value is incremented to 4 (Fig. 4(b)), the degree of network disruption is significantly reduced to approximately 50%. This curve pattern eventually exhibits that the proposed system can significantly control risk in MANET's dynamic topology.

B. ASSESSMENT OF COMPARATIVE ANALYSIS

The next part of the analysis is about assessing convergence performance using the statistical model given in [53]. A closer look at the graphical outcome shows that the model offers faster convergence in a reduced number of iterations considering the uniform constraint associated with the *risk* parameter. A closer look at Fig. 4(a) shows that in the presence of attackers $K = 2$, the proposed system exhibits dual nature of disruption of signal. The disruption is lower for a higher value of risk ($= 0.2$) while it increases with the lowered risk ($= 0.05$). This eventually means that the proposed game model can map the dynamic strategy of the attacker during collusion. The performance is found much better in Fig. 4(b), wherewith an increased value of attacker $K = 4$, the disruption performance is further enhanced. The value of disruption significantly reduces here in comparison to its primary outcome. This eventually shows that the proposed system can maintain effective consistency in

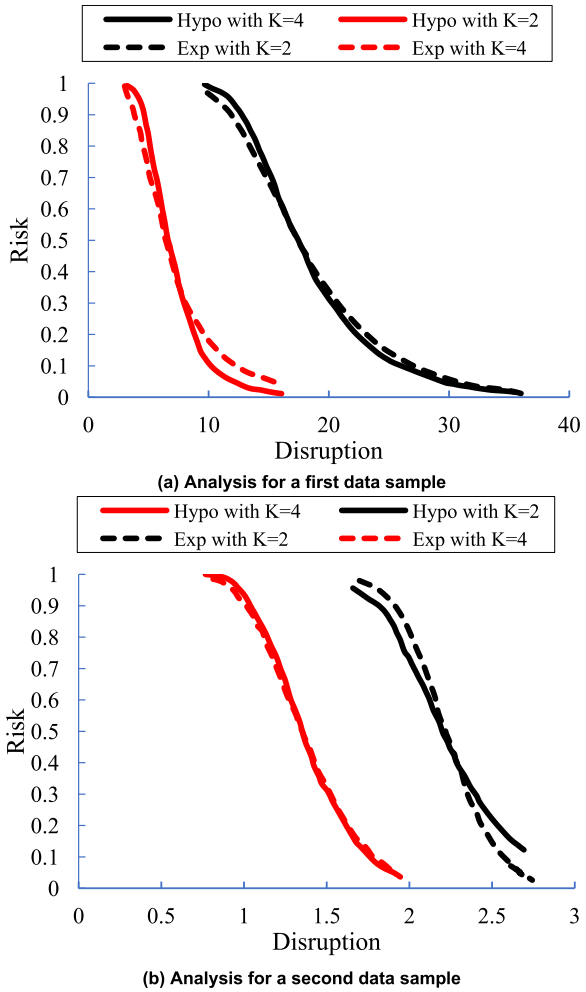

FIGURE 3. Comparative analysis of risk considering K = 2 and K = 4 for the experimental and hypothetical system.

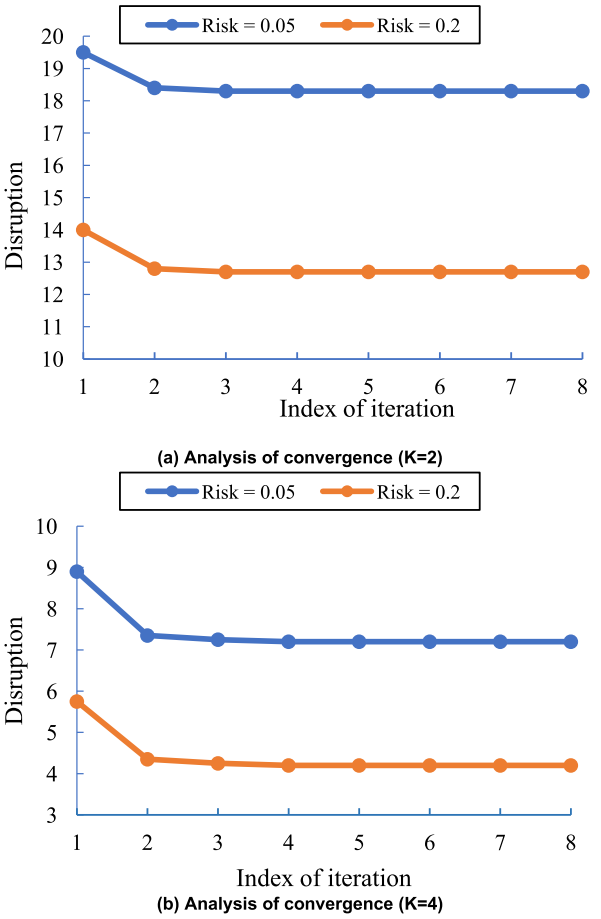

FIGURE 4. Comparative analysis of risk considering K = 2 and K = 4 for the experimental and hypothetical system.

reducing the degree of disruption. This outcome also exhibits scalability performance, which is extensively well with the game's increased stage in the proposed model. This outcome can witness a perfect Nash equilibrium.

The outcome of the proposed system has been compared with prior works i) the baseline work carried out by authors in [55], and ii) our previous model of multi-attacker collusion [52].

The first baseline work [55] has constructed Bayesian signaling with more emphasis both types of nodes' utilities. This process has been carried out in compliance with sequential rationality. This model is developed based on the neighborhood monitoring process. The belief, disbelief, and uncertainty calculation are carried out, followed by an investigational study with a different form of the multistage game process. The outcome has shown that this study uses a unique incentive policy which discourages the malicious node while adopting the strategy to attack and encourage the regular node while performing reporting operation. Therefore, this model is a good baseline model that can identify the user's malicious behavior and resist them from participating in the data forwarding process. Although this process is applicable for any form of attack, it has been analyzed over jamming/interference attack. This approach is extended in the next version of our prior work [52], considering the multi-attacker node collusion model.

Apart from this, the work carried out by Marchang *et al.* [57] as well as Amraoui *et al.* [58] also bear similar adoption of a game-based design approach. The work of Marchang *et al.* [57] has developed a probabilistic security system by controlling their active monitoring time using multi-player game logic. The study outcome exhibited better resource-saving at different levels of security to monitor anomaly behavior. On the other hand, the work carried out by Amraoui *et al.* [58] has presented a game-theory-based scheme to control topology dynamicity in MANET. The prime reason behind selecting these works is that it is required to assess the degree of resource utilization and transmission cost for the proposed game-theory-based framework. Along with capability to resist multi-collusion attacks, it is also essential to understand the proposed game logic's internal processing capability. The analysis is carried out based on identification performance and throughput performance mainly. A similar test environment is allotted for all the systems under consideration to achieve measurable and quantified comparison.

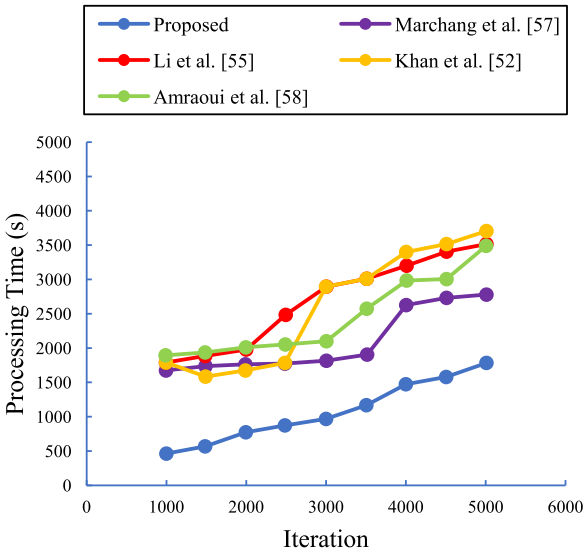

FIGURE 5. Comparative analysis of processing time concerning 6000 iteration rounds.

As the present study bears a similar game theory adoption methodology, a comparison is being carried out considering the above four baseline works. A similar test environment is considered where the assessment is done concerning processing time, resource utilization, and cost of transmission to carry out this analysis.

C. ANALYSIS OF PROCESSING TIME

It is essential to understand some inherent characteristics of a collusion attack, which can be used as an indicator for performing the assessment. In the case of a collusion attack, the adversary performs integration of different copies of digital data, which leads to the generation of a new copy of data. The process responsible for carrying out this operation is not much spoken about in any existing literature. Various forms of explicit processes, e.g., linear combination, replacement, averaging, etc. The prime agenda of this process is to generate a new copy; so that old information is lost. The process becomes sophisticated, and operation intensive of the attack is of multiple collusion while a significant amount of time is consumed for this process. Therefore, this part of the analysis assesses the processing time required to estimate the proposed system's effectiveness concerning processing time. To map with the practical world scenario, the proposed system has considered 6000 rounds of iteration. Each round consists of increasing the number of requests from the node to participate in data forwarding processing. Applying the proposed concept, the study assumes its unawareness of the legitimacy of such a joining request. Hence, a computation is required to be carried out to evaluate its degree of severity if such a joining request is permitted or aborted. An effective security approach should offer a reduced processing time compared to the multi-attacker's time to carry out collusion in MANET.

Moreover, in the presence of multiple attackers of MANET's decentralized communication region, the chances of attacks are higher. A closer look into Fig. 5 highlights no significant difference in the processing time curve with an increasing round of simulation for both the baseline systems. On the other hand, the proposed system is found to exhibit a significant difference in its outcome of much-reduced processing time. Following is the justification for this significant difference in outcome: The implementation strategy of authors in [55] has not mitigated collusion attack, but their model is capable enough to identify the colluders' behavior. According to this strategy, their model deploys a Bayesian equilibrium strategy where target nodes' uncertainty values are observed concerning dynamic thresholding. However, both existing models of [55] and [52] will be required to continuously carry out neighborhood monitoring to confirm the target node's malicious nature. This consumes a significant amount of time over increased iteration even if [52] model considers multi-attacker collusion. Similarly, Marchang *et al.* [57] have included excessive management of control messages iteratively, leading to increased processing time to perform data transmission. On the other hand, the baseline work of Amraoui *et al.* [58] is found better compared to other baseline works of [55] and [52] owing to the adoption of optimized link-state routing. This approach has a better topology control feature; however, when this approach is exposed to the adopted threat of multi-collusion attack, it witnesses an increase in overhead due to the inclusion of hello message and topology control command in its control message. The complete mechanism of secure routing becomes highly time-intensive over increasing rounds of iteration.

The proposed system mitigates this problem by computing the difference between the colluded frame and the original frame, where disruption is obtained to formulating the decision. Hence, half of the process for identifying malicious nodes is reduced in the proposed system, which results in faster processing and the identification process compared to the existing baseline approach. Apart from this, the proposed system's optimal strategy has used an auxiliary information γ for both regular node and malicious node, thereby formulating a robust, speedy, and cost-effective detection time considering the probability of outlier, i.e., τ. In this case, the common node will choose to apply an optimal value to increase the probability of correct identification of attackers. However, this process is nearly similar to the baseline system except that the baseline system allocates incentives for all the adopted actions.

In contrast, the proposed system doesn't offer the allocation of any incentives. This process extensively cuts down the processing time as it has non-inclusion of processing or allocating any incentives. Apart from this, the use-case scenario for adopting the worst interactivity between both nodes chosen for the proposed system is highly practical and not found in the baseline system.

D. ANALYSIS OF RESOURCE UTILIZATION

The mobile nodes in MANET drain consistent amounts of resources while performing communication in dynamic

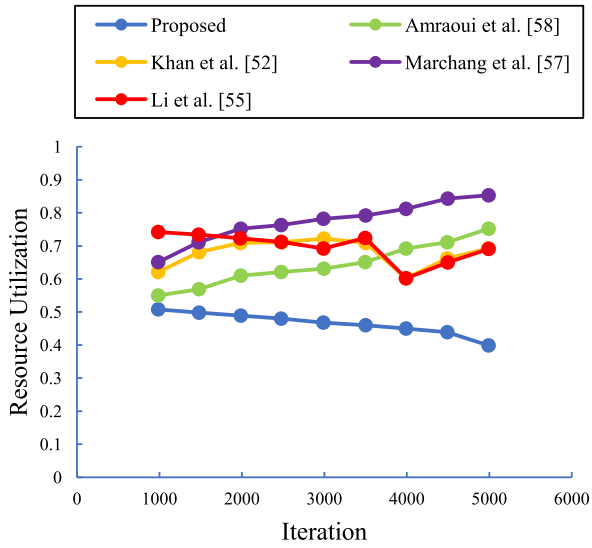

FIGURE 6. Comparative analysis of resource utilization versus 6000 iteration rounds.

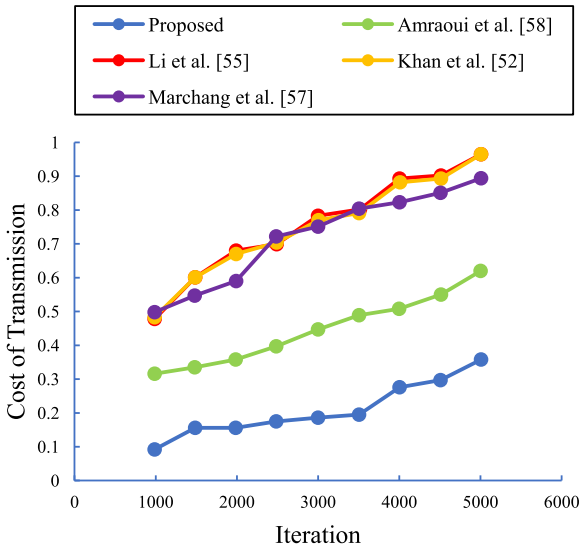

FIGURE 7. Comparative analysis of cost of transmission versus 6000 iteration rounds.

and decentralized topology. The rate of depletion of energy is significantly high when security protocols are added to the network layer. Three types of resources are potentially used right from establishing and communicating over the dynamic environment scenario viz. i) energy, ii) memory, and iii) channel capacity.

Energy is required for performing transmission, receiving, and processing of the data. Memory is required to store the transactional information, routing table information, and storing secret keys when any encryption-based algorithms are used in MANET. Channel capacity is another essential resource that is strongly affected when the core data packet with the embedded security token increases the usage. The proposed system uses probability to perform the computation of all the above three resources to determine the effect of resources over secure communication in MANET. The resource assessment is carried out in probability limits [0 1], making the model applicable to be fine-tuned for practical world scenarios.

All the nodes are assigned the highest value of resources to find the following trend exhibited in Fig. 6. The trend shows a trace of fluctuation of the resource utilization in the baseline approach after 3000-4000 iteration. The prime reason behind this fluctuation of the baseline approach is that it uses its resources iteratively to compute the uncertainty in the trust computation if the probability of several declines is found similar to the probability of cooperation. In such a case, the belief and disbelief factors equal, which reason for initiating iterative computation of uncertainty. In doing so, many resources are utilized more progressively towards capturing the information of attack. Hence, the baseline model [52], [55] is only applicable to multi-collusion attacks if all the attackers deploy a similar attack strategy. A similar phenomenon is also observed for the baseline work of Marchang *et al.* [57] and Amraoui *et al.* [58], which, when subjected to multi-collusion attack, results in increasing dependency on the resources. However, they are capable of significant resource conservation if exposed to a single collusion attack. The prime reason behind this is that the monitoring is spontaneous throughout the simulation time for baseline models, whereas the proposed study offers on-demand operation to conserve resources significantly.

However, if the attack strategy alters, then much computation is required to upgrade the baseline approach's dynamic threshold; it also accounts for resource utilization. The proposed system doesn't have any such inclusion, and using a simplified optimization strategy, both the nodes can know each other's strategy just by one stage of the calculation. For this reason, resource utilization is much stabilized compared to the existing baseline approach.

E. ANALYSIS OF COST OF TRANSMISSION

Considering that the mobile nodes follow certain protocols of resource allocation approach in MANET, it is eventual that all the mobile nodes will be allocated with a specific set of operations and deploy a particular set of actions. To execute such actions, the mobile nodes will be incurring certain costs while performing transmission. The proposed system deploys the distributed cost model discussed in [56] to compute the cost of transmission to adhere to the standards. Cost is considered under probability limits similar to resource utilization parameters. This scheme is meant for accessing the data by the mobile nodes in MANET, where the cost model is found to be supportive of effective content distribution. The outcome of comparison for the cost of transmission for both proposed and baseline systems is exhibited in Fig. 7.

The graphical outcome shown in Fig. 7 shows no significant difference between the baseline approaches. The reason behind this is that both approaches use similar core modeling of game theory with a distinction that the first model [55] doesn't use colluding attack and the second model [52] considers collusion attack. The increasing level of cost of transmission over Marchang *et al.* [57] accounts for its iterative

intrusion detection system where payoffs allocated are based on observing the current trend of malicious behavior of colluder node. However, the proposed system considers both current and computes the probabilities of intrusion in upcoming rounds of operation. This not only controls the cost of transmission but also results in secure communication. A closer look into the work of Amraoui *et al.* [58] shows better cost of transmission compared to all the other baseline models as the complete routing operation is based on sequence number and control message of topology control which makes the routing more deterministic resulting in lowered dependencies on energy to be allocated with higher variance. However, the proposed model is an improvement over the second model, where a reduced number of steps and processes are included with faster execution. There is a significant justification for this outcome. The proposed system reviews the trends of the *risk* value and the disruption caused due to multi-attacker collusion based on the relative information obtained from auxiliary data. The proposed system's whole idea is based on the inter-dependencies of both the players' strategies, i.e., regular node and malicious node.

Each player undertakes its strategy based on their opponent's strategy, which is defined by a few computation steps, unlike the baseline approach. The proposed study computes absolute risk, followed by an assessment by the regular node to obtain information about an attacker's strategy to introduce a collusion attack. The regular node makes use of auxiliary information to select the best strategy accordingly. This operation is followed by the malicious node's further assessment for adopting auxiliary information by the regular node to capture information about the malicious node. Thus, the malicious node alters its strategy accordingly to safeguard itself. As a result, both the nodes' behavior can be obtained in our initial graphical analysis in the form of disruption (Fig. 2 and Fig. 3). In this analysis, it is found that the risk value associated with the malicious node significantly increases if the regular node makes use of the auxiliary information. The system can only reduce the probability of identifying the malicious node considering that the malicious node correctly possesses auxiliary information of the regular node. Hence, auxiliary information has a significant level of contribution towards accurate identification in the proposed game modeling. This eventually means that a player with an appropriate estimation of auxiliary information can lead the proposed model of the game and is also capable of estimating the specific risk factor associated with it. This is an improved alternative to the pure strategy adopted in the work [55] and the prior model [52]. This results in much reduction of transmission cost in the proposed system compared to the existing baseline system.

VII. CONCLUSION

One of the significant issues discussed in this paper is the authenticity of the data exchanged between two mobile nodes. This is of considerable concern when MANET applications supporting streaming applications are integrated with an IoT. To safeguard the exchanged data, encryption is usually used; however, the proposed system chooses its design differently. The proposed system develops a mechanism of embedding a secret digital code that is resistive to collusion. However, one of the essential demands for its security is to illustrate the unpredictable behavior of colluders in MANET clearly. The proposed system assists in giving clarity in understanding this behavior using a game modeling approach. The proposed system studies the potential risk factor associated with the disruption caused by the signal concerning the embedded digital secret code. According to this proposed implementation, the game model performs monitoring of both the players' strategies to improvise the identification of malicious nodes based on the supportive information associated with the opponent node. The study outcome shows that the adoption of the optimal strategy of identification by the regular node can offer complete disclosure of the approach adopted by the malicious node. The study outcome shows reduced processing time, decreased resource utilization, and reduced transmission cost in MANET, thereby showing a cost-effective game modeling towards multi-attacker collusion. Therefore, it can be seen that the proposed study has presented a joint design of behavior of legitimate and malicious nodes using game-logic. The study's significant contribution is that it offers faster identification of malicious nodes without any prior information in the detection model. Apart from this, the result shows an extremely lesser dependency on resources, which makes the model more practical to be adopted in practical world scenarios. Our next phase of the implementation will be continued with developing a stringent attack environment when MANET is integrated into different communication technology. The idea is to increase the scope of attack resistance capability over a larger and more complicated scale of communication environment. Hence, more inclination towards evolving an optimization-based detection and prevention strategy will be carried out to improve our game-based security model in MANET further.

ACKNOWLEDGMENT

The authors are thankful to the four anonymous reviewers for their careful reading of the initial manuscript as their many insightful comments and suggestions have helped a lot in improving and clarifying the contents of the paper.

The authors express their personal appreciation for the effort of Ms Mushtari Abdul Jaleel, Mr Munshi Awan Abass and Mr Zaid Bin Reyaz in proofreading and editing the paper.

REFERENCES

[1] V. Tilwari, R. Maheswar, P. Jayarajan, T. V. P. Sundararajan, M. N. Hindia, K. Dimyati, H. Ojukwu, and I. S. Amiri, "MCLMR: A multicriteria based multipath routing in the mobile ad hoc networks," *Wireless Pers. Commun.*, vol. 112, no. 4, pp. 2461–2483, Jun. 2020, doi: 10.1007/s11277-020-07159-8.

[2] X. Chen, T. Wu, G. Sun, and H. Yu, "Software-defined MANET swarm for mobile monitoring in hydropower plants," *IEEE Access*, vol. 7, pp. 152243–152257, 2019, doi: 10.1109/ACCESS.2019.2948215.

[3] C. K. da Silva Rodrigues and V. E. M. Rocha, "BT-MANET: A novel BitTorrent-like algorithm for video on-demand streaming over MANETs," *IEEE Latin Amer. Trans.*, vol. 17, no. 01, pp. 78–84, Jan. 2019, doi: 10.1109/TLA.2019.8826698.

[4] S. Glass, I. Mahgoub, and M. Rathod, "Leveraging MANET-based cooperative cache discovery techniques in VANETs: A survey and analysis," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2640–2661, 4th Quart., 2017, doi: 10.1109/COMST.2017.2707926.

[5] B. U. I. Khan, R. F. Olanrewaju, R. N. Mir, S. H. Yusoff, and M. L. Sanni, "Trust and resource oriented communication scheme in mobile ad hoc networks," in *Intelligent Systems and Applications*, Cham, Switzerland: Springer, vol. 751, 2016, pp. 414–430, doi: 10.1007/978-3-319-69266-1_20.

[6] M. Sedrati and A. Benyahia, "Multipath routing to improve quality of service for video streaming over mobile ad hoc networks," *Wireless Pers. Commun.*, vol. 99, no. 2, pp. 999–1013, Mar. 2018, doi: 10.1007/s11277-017-5163-6.

[7] X. Wang and X. Zhu, "Anycast-based content-centric MANET," *IEEE Syst. J.*, vol. 12, no. 2, pp. 1679–1687, Jun. 2018, doi: 10.1109/JSYST.2016.2619374.

[8] M. Ponguwala and S. Rao, "E2-SR: A novel energy-efficient secure routing scheme to protect MANET-IoT," *IET Commun.*, vol. 13, no. 19, pp. 3207–3216, Dec. 2019, doi: 10.1049/iet-com.2019.0039.

[9] Q. Ye and W. Zhuang, "Token-based adaptive MAC for a two-hop Internet-of-Things enabled MANET," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1739–1753, Oct. 2017, doi: 10.1109/JIOT.2017.2679119.

[10] W. A. Jabbar, W. K. Saad, and M. Ismail, "MEQSA-OLSRv2: A multicriteria-based hybrid multipath protocol for energy-efficient and QoS-aware data routing in MANET-WSN convergence scenarios of IoT," *IEEE Access*, vol. 6, pp. 76546–76572, 2018, doi: 10.1109/ACCESS.2018.2882853.

[11] A. Ullah, S. Yaqoob, M. Imran, and H. Ning, "Emergency message dissemination schemes based on congestion avoidance in VANET and vehicular FoG computing," *IEEE Access*, vol. 7, pp. 1570–1585, 2019, doi: 10.1109/ACCESS.2018.2887075.

[12] S. Jelassi, A. Bouzid, and H. Youssef, "QoE-driven video streaming system over cloud-based VANET," in *Communication Technologies for Vehicles* (Lecture Notes in Computer Science), vol. 9066. Cham, Switzerland: Springer, 2015, pp. 84–93, doi: 10.1007/978-3-319-17765-6_8.

[13] E. B. Smida, S. G. Fantar, and H. Youssef, "Video streaming forwarding in a smart city's VANET," in *Proc. IEEE 11th Conf. Service-Oriented Comput. Appl. (SOCA)*, Paris, France, Nov. 2018, pp. 1–8, doi: 10.1109/SOCA.2018.8645770.

[14] C.-M. Huang, T.-H. Lin, and K.-C. Tseng, "Data dissemination of application service by using member-centric routing protocol in a platoon of Internet of vehicle (IoV)," *IEEE Access*, vol. 7, pp. 127713–127727, 2019, doi: 10.1109/ACCESS.2019.2936456.

[15] J. S. Lee, Y.-S. Yoo, H. S. Choi, T. Kim, and J. K. Choi, "Energy-efficient TDMA scheduling for UVS tactical MANET," *IEEE Commun. Lett.*, vol. 23, no. 11, pp. 2126–2129, Nov. 2019, doi: 10.1109/LCOMM.2019.2936472.

[16] B. Ojetunde, N. Shibata, and J. Gao, "Secure payment system utilizing MANET for disaster areas," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 49, no. 12, pp. 2651–2663, Dec. 2019, doi: 10.1109/TSMC.2017.2752203.

[17] S. Zahid, S. A. Abid, N. Shah, S. H. A. Naqvi, and W. Mehmood, "Distributed partition detection with dynamic replication management in a DHT-based MANET," *IEEE Access*, vol. 6, pp. 18731–18746, 2018, doi: 10.1109/ACCESS.2018.2814017.

[18] R. Meddeb, B. Triki, F. Jemili, and O. Korbaa, "A survey of attacks in mobile ad hoc networks," in *Proc. Int. Conf. Eng. MIS (ICEMIS)*, Monastir, Tunisia, May 2017, pp. 1–7, doi: 10.1109/ICEMIS.2017.8273007.

[19] M. Karthigha, L. Latha, and K. Sripriyan, "A comprehensive survey of routing attacks in wireless mobile ad hoc networks," in *Proc. Int. Conf. Inventive Comput. Technol. (ICICT)*, Coimbatore, India, Feb. 2020, pp. 396–402, doi: 10.1109/ICICT48043.2020.9112588.

[20] P. Roshani and A. Patel, "Techniquesto mitigate grayhole attack in MANET: A survey," in *Proc. Int. Conf. Innov. Inf., Embedded Commun. Syst. (ICIIECS)*, Coimbatore, India, Mar. 2017, pp. 1–4, doi: 10.1109/ICIIECS.2017.8276064.

[21] E. G. Mwangi, G. M. Muketha, and G. K. Ndungu, "A review of security techniques against black hole attacks in mobile ad hoc networks," in *Proc. IST-Africa Week Conf. (IST-Africa)*, Nairobi, Kenya, May 2019, pp. 1–8, doi: 10.23919/ISTAFRICA.2019.8764862.

[22] M. Goyal, S. K. Poonia, and D. Goyal, "Attacks finding and prevention techniques in MANET: A survey," *Wireless Commun. Mobile Comput.*, vol. 10, no. 5, pp. 1185–1195, 2017.

[23] K. J. Abhilash and K. S. Shivaprakasha, "Secure routing protocol for MANET: A survey," in *Advances in Communication, Signal Processing, VLSI, and Embedded Systems*. Singapore: Springer, 2020, pp. 263–277, doi: 10.1007/978-981-15-0626-0_22.

[24] O. Fasunlade, S. Zhou, and D. Sanders, "Comprehensive review of collaborative network attacks in MANET," in *Proc. IEEE 44th Annu. Comput., Softw., Appl. Conf. (COMPSAC)*, Madrid, Spain, Jul. 2020, pp. 1542–1545, doi: 10.1109/COMPSAC48688.2020.00-36.

[25] B. U. I. Khan, F. Anwar, R. F. Olanrewaju, B. R. Pampori, and R. N. Mir, "A novel multi-agent and multilayered game formulation for intrusion detection in Internet of Things (IoT)," *IEEE Access*, vol. 8, pp. 98481–98490, 2020, doi: 10.1109/ACCESS.2020.2997711.

[26] B. U. I. Khan, F. Anwar, R. F. Olanrewaju, B. R. Pampori, and R. N. Mir, "A game theory-based strategic approach to ensure reliable data transmission with optimized network operations in futuristic mobile ad hoc networks," *IEEE Access*, vol. 8, pp. 124097–124109, 2020, doi: 10.1109/ACCESS.2020.3006043.

[27] Z. Chen, W. Zhou, S. Wu, and L. Cheng, "An adaptive on-demand multipath routing protocol with QoS support for high-speed MANET," *IEEE Access*, vol. 8, pp. 44760–44773, 2020, doi: 10.1109/ACCESS.2020.2978582.

[28] T. Zhang, S. Zhao, and B. Cheng, "Multipath routing and MPTCP-based data delivery over manets," *IEEE Access*, vol. 8, pp. 32652–32673, 2020, doi: 10.1109/ACCESS.2020.2974191.

[29] L. Suresh P., R. Kaur, M. S. Gaur, and V. Laxmi, "A collusion attack detection method for OLSR-based MANETS employing scruple packets," in *Proc. 3rd Int. Conf. Secur. Inf. Netw. (SIN)*, 2010, pp. 256–262, doi: 10.1145/1854099.1854151.

[30] G. Liu, H. Dong, Z. Yan, X. Zhou, and S. Shimizu, "B4SDC: A blockchain system for security data collection in MANETs," *IEEE Trans. Big Data*, early access, Mar. 17, 2020, doi: 10.1109/TBDATA.2020.2981438.

[31] Z. Zhang and J. Wang, "MCAR: Multi-path-based collusion avoidance routing for wireless ad-hoc networks," in *Proc. 7th Int. Conf. Netw., Commun. Comput. (ICNCC)*, 2018, pp. 177–181, doi: 10.1145/3301326.3301355.

[32] M. Zarezadeh and H. Mala, "Determining honesty of accuser nodes in key revocation procedure for MANETs," *Mobile Netw. Appl.*, vol. 24, no. 3, pp. 903–912, Jun. 2019, doi: 10.1007/s11036-018-1144-6.

[33] R. Abassi, A. B. C. Douss, and D. Sauveron, "TSME: A trust-based security scheme for message exchange in vehicular ad hoc networks," *Hum.-Centric Comput. Inf. Sci.*, vol. 10, no. 1, pp. 1–19, Dec. 2020, doi: 10.1186/s13673-020-00248-4.

[34] K. Fan, J. Wang, X. Wang, H. Li, and Y. Yang, "Secure, efficient and revocable data sharing scheme for vehicular fogs," *Peer-to-Peer Netw. Appl.*, vol. 11, no. 4, pp. 766–777, Jul. 2018, doi: 10.1007/s12083-017-0562-8.

[35] W. Yong-hao, "A trust management model for Internet of vehicles," in *Proc. 4th Int. Conf. Cryptogr., Secur. Privacy*, Jan. 2020, pp. 136–140, doi: 10.1145/3377644.3377664.

[36] H.-M. Sun, C.-H. Chen, and Y.-F. Ku, "A novel acknowledgment-based approach against collude attacks in MANET," *Expert Syst. Appl.*, vol. 39, no. 9, pp. 7968–7975, Jul. 2012, doi: 10.1016/j.eswa.2012.01.118.

[37] F. Kandah, Y. Singh, W. Zhang, and C. Wang, "Mitigating colluding injected attack using monitoring verification in mobile ad-hoc networks," *Secur. Commun. Netw.*, vol. 6, no. 4, pp. 539–547, Apr. 2013, doi: 10.1002/sec.681.

[38] Poonam, K. Garg, and M. Misra, "Detection and mitigation of attacks by colluding misbehaving nodes in MANET," in *Proc. Int. Conf. Netw. Secur. Appl.*, Chennai, India, 2010, pp. 181–190, doi: 10.1007/978-3-642-14478-3_19.

[39] R. Abassi, "Dealing with collusion attack in a trust-based MANET," *Cybern. Syst.*, vol. 49, nos. 7–8, pp. 475–496, Nov. 2018, doi: 10.1080/01969722.2018.1541598.

[40] K. Singh and A. K. Verma, "TBCS: A trust based clustering scheme for secure communication in flying ad-hoc networks," *Wireless Pers. Commun.*, vol. 114, no. 4, pp. 3173–3196, Oct. 2020, doi: 10.1007/s11277-020-07523-8.

[41] T. Maragatham, S. Karthik, and R. M. Bhavadharini, "TCACWCA: Transmission and collusion aware clustering with enhanced weight clustering algorithm for mobile ad hoc networks," *Cluster Comput.*, vol. 22, no. S6, pp. 13195–13208, Nov. 2019, doi: 10.1007/s10586-017-1574-0.

[42] X. Chen, Y. Sun, Y. Ou, X. Zheng, Z. Wang, and M. Li, "A conflict decision model based on game theory for intelligent vehicles at urban unsignalized intersections," *IEEE Access*, vol. 8, pp. 189546–189555, 2020, doi: 10.1109/ACCESS.2020.3031674.

[43] N. Kumar, S. Misra, N. Chilamkurti, J.-H. Lee, and J. J. P. C. Rodrigues, "Bayesian coalition negotiation game as a utility for secure energy management in a vehicles-to-grid environment," *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 1, pp. 133–145, Jan. 2016, doi: 10.1109/TDSC.2015.2415489.
[44] X. Ji, Y. Liu, X. He, K. Yang, X. Na, C. Lv, and Y. Liu, "Interactive control paradigm-based robust lateral stability controller design for autonomous automobile path tracking with uncertain disturbance: A dynamic game approach," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 6906–6920, Aug. 2018, doi: 10.1109/TVT.2018.2834381.
[45] N. Li, D. W. Oyler, M. Zhang, Y. Yildiz, I. Kolmanovsky, and A. R. Girard, "Game theoretic modeling of driver and vehicle interactions for verification and validation of autonomous vehicle control systems," *IEEE Trans. Control Syst. Technol.*, vol. 26, no. 5, pp. 1782–1797, Sep. 2018, doi: 10.1109/TCST.2017.2723574.
[46] M. Hu, G. Xie, H. Gao, D. Cao, and K. Li, "Manoeuvre prediction and planning for automated and connected vehicles based on interaction and gaming awareness under uncertainty," *IET Intell. Transp. Syst.*, vol. 13, no. 6, pp. 933–941, Jun. 2019, doi: 10.1049/iet-its.2018.5353.
[47] S. Xia, F. Lin, Z. Chen, C. Tang, Y. Ma, and X. Yu, "A Bayesian game based vehicle-to-vehicle electricity trading scheme for blockchain-enabled Internet of vehicles," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 6856–6868, Jul. 2020, doi: 10.1109/TVT.2020.2990443.
[48] M. Kaliappan and B. Paramasivan, "Enhancing secure routing in mobile ad hoc networks using a dynamic Bayesian signalling game model," *Comput. Electr. Eng.*, vol. 41, pp. 301–313, Jan. 2015, doi: 10.1016/j.compeleceng.2014.11.011.
[49] D. Lin, Q. Wang, and P. Yang, "The game theory: Applications in the wireless networks," in *Game Theory—Applications in Logistics and Economy*.London, U.K.: IntechOpen, 2018, doi: 10.5772/intechopen.79508.
[50] S. Kim, *Game Theory Applications in Network Design*. Hershey, PA, USA: IGI Global, 2014.
[51] J. C. Oh and K. Mehrotra, "Game theory and social networks," in *Encyclopedia of Social Network Analysis and Mining*, New York, NY, USA: Springer, 2018, doi: 10.1007/978-1-4939-7131-2_175.
[52] B. U. I. Khan, R. F. Olanrewaju, F. Anwar, and R. N. Mir, "ECM-GT: Design of efficient computational modelling based on game theoretical approach towards enhancing the security solutions in MANET," *Int. J. Innov. Technol. Exploring Eng.*, vol. 8, no. 7, pp. 506–519, May 2019.
[53] A. L. Yuille and A. Rangarajan, "The concave-convex procedure (CCCP)," *Neural Comput.*, vol. 15, no. 4, pp. 915–936, 2006, doi: 10.1162/08997660360581958.
[54] (2006). *-Database: Image & Video Clips (1)*. See.xidian.edu.cn. Accessed: Apr. 6, 2021. [Online]. Available: https://see.xidian.edu.cn/vipsl/database_Video.html
[55] F. Li, Y. Yang, and J. Wu, "Attack and flee: Game-theory-based analysis on interactions among nodes in MANETs," *IEEE Trans. Syst., Man, Cybern., B, Cybern.*, vol. 40, no. 3, pp. 612–622, Jun. 2010, doi: 10.1109/TSMCB.2009.2035929.
[56] H. Li, Y. Yang, Q. Z. X. Gao, and G. Ma, "Cooperative downloading in mobile ad hoc networks: A cost-energy perspective," *Int. J. Distrib. Sensor Netw.*, vol. 12, no. 3, 2016, Art. no. 3028642, doi: 10.1155/2016/3028642.
[57] N. Marchang, R. Datta, and S. K. Das, "A novel approach for efficient usage of intrusion detection system in mobile ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 1684–1695, Feb. 2017, doi: 10.1109/tvt.2016.2557808.
[58] H. Amraoui, A. Habbani, and A. Hajami, "A forwarding game approach for reducing topology control traffic in MANETs," *Arabian J. for Sci. Eng.*, vol. 43, no. 12, pp. 6945–6961, Dec. 2018, doi: 10.1007/s13369-017-2910-7.

BURHAN UL ISLAM KHAN received the Ph.D. degree in engineering from International Islamic University Malaysia, Kuala Lumpur, in 2021. Before commencing his Ph.D., he has been involved in varying roles as that of a Software Engineer, a Research Analyst, and an Assistant Professor. He has published over 60 refereed articles in a wide range of highly recognized international journals and conferences (Springer, IEEE, ACM, and so on.). 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 (IIUM), 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 F. OLANREWAJU (Senior Member, IEEE) 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 the 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, International Islamic University Malaysia, where she is leading the Software Engineering Research Group (SERG). She represents her University, IIUM, at Malaysian Society for Cryptology Research. Her current in hand projects revolve around MapReduce Optimization Techniques, Compromising Secure Authentication and Authorization Mechanisms, Secure Routing for ad-hoc networks, Formulating Bio-Inspired Optimization Techniques. She is an Executive Committee Member of technical associations like IEEE Women in Engineering, Arab Research Institute of Science and Engineers, and so on.

MISS LAIHA BINTI MAT KIAH (Senior Member, IEEE) received the Ph.D. degree in information security from Royal Holloway, University of London, U.K., in 2007. Since then, she has been an Active Researcher in computer science particularly in security with the Faculty of Computer Science and Information Technology, University of Malaya (UM). She was promoted to a professorship, in 2015. This is evidenced by her publications and research projects in which she is/was the Principal Investigator (PI) and Co-PIs. As a Professional Technologist (Ts.), keeping up with the current trend and demand of ever evolving computing technology field is crucial to ensure the quality and the impact of her research work. Her main research interests include the security aspect of computing and technology fields with variation of applications in multi and/or trans disciplinary projects. Her current research interests include cyber security, blockchain technology, the IoT, and health information exchange. She is an active member of the EC Council, the Malaysian Society for Cryptology Research (MSCR), and the Malaysia Board of Technologists (Ts.).

ROOHIE N. 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 Bangaluru, India, in 1990, and the Ph.D. degree from the University of Kashmir, in 2005. She is currently a Professor and the HOD with the Department of Computer Science and Engineering, NIT Srinagar, India. She has authored 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.