information

Article

SGM: Strategic Game Model for Resisting Node Misbehaviour in IoT-Cloud Ecosystem

Burhan Ul Islam Khan [1,*], Farhat Anwar [1], Farah Diyana Bt. Abdul Rahman [1], Rashidah Funke Olanrewaju [1], Khang Wen Goh [2,*], Zuriati Janin [3,*] and Md Arafatur Rahman [4]

[1] Department of Electrical and Computer Engineering, Kulliyyah of Engineering, International Islamic University Malaysia (IIUM), Kuala Lumpur 53100, Malaysia
[2] Faculty of Data Science and Information Technology, INTI International University, Nilai 71800, Malaysia
[3] Faculty of Electrical Engineering, Universiti Teknologi MARA (UiTM), Shah Alam 40450, Malaysia
[4] Faculty of Computing, Universiti Malaysia Pahang (UMP), Pekan 26600, Malaysia
* Correspondence: burhan.iium@gmail.com or burhankhan@iium.edu.my (B.U.I.K.); khangwen.goh@newinti.edu.my (K.W.G.); zuriaty@uitm.edu.my (Z.J.)

Abstract: This paper introduces a computational strategic game model capable of mitigating the adversarial impact of node misbehaviour in large-scale Internet of Things (IoT) deployments. This security model's central concept is to preclude the participation of misbehaving nodes during the routing process within the ad hoc environment of mobile IoT nodes. The core of the design is a simplified mathematical algorithm that can strategically compute payoff embrace moves to maximise gain. At the same time, a unique role is given to a node for restoring resources during communication or security operations. Adopting an analytical research methodology, the proposed model uses public and private cloud systems for integrating quality service delivery with secure agreements using a Global Trust Controller and core node selection controller to select an intermediate node for data propagation. The initiation of the game model is carried out by identifying mobile node role followed by choosing an optimal payoff for a normal IoT node. Finally, the model leads to an increment of gain for selecting the regular IoT node for routing. The findings of the evaluation indicate that the proposed scheme offers 36% greater accuracy, 25% less energy, 11% faster response time, and 27% lower cost than the prevalent game-based models currently used to solve security issues. The value added by the proposed study is the simplified game model which balances both security demands and communication demands.

Keywords: game theory; node misbehaviour; IoT-Cloud Ecosystem; strategic modelling; secure agreement; trust controller

Citation: Khan, B.U.I.; Anwar, F.; Rahman, F.D.B.A.; Olanrewaju, R.F.; Goh, K.W.; Janin, Z.; Rahman, M.A. SGM: Strategic Game Model for Resisting Node Misbehaviour in IoT-Cloud Ecosystem. *Information* **2022**, *13*, 544. https://doi.org/10.3390/info13110544

Academic Editor: Valentina Casola

Received: 18 September 2022
Accepted: 28 October 2022
Published: 17 November 2022

1. Introduction

Mobile ad hoc network has witnessed significant attention for more than a decade owing to its cost-effective, non-infrastructure-based communication system [1]. Owing to the decentralised version of the network and topology, such a form of ad hoc network always has a higher security concern, irrespective of massive archives to state security solutions [2–6]. With changing time and demand for communication, cloud computing and the Internet of Things (IoT) have evolved [7]. The domain of IoT involves encapsulating multiple forms of wireless communication technologies, where a mobile ad hoc network is one of them [8]. However, a closer look into the majority of the existing studies shows that the concept implementation of IoT considers an independent node governed by its security and communication protocol [9,10]. The actual concept demands the presence of a mobile node with ad hoc features to be deployed under IoT and cloud environments. This is a challenging scenario owing to a different set of communication protocols in mobile ad hoc networks and IoT, where there is no generalised algorithm yet. It will eventually mean that security protocols for mobile ad hoc networks will not be completely functional

when subjected to an IoT environment [11,12]. Hence, there is a need for a study that calls for constructing a generalised secure routing scheme when a mobile ad hoc network is deployed in an IoT scenario. Apart from this, the threats studied in mobile ad hoc networks differ from those of exponentially challenging threats in IoT [13]. Existing security protocols in mobile ad hoc networks cannot mitigate such threats in the IoT environment.

Various studies have introduced the mobility concept in IoT, emphasising mitigating security threats [14–17]. However, such studies are mainly encryption-based or use artificial intelligence [18–20]. Such a research contribution is beneficial only if the attacks are well-defined and not a challenging form of attack, e.g., node misbehaviour [21]. The most challenging aspect of node misbehaviour is that it is quite a computationally resource-consuming matter to identify the presence of a threat. At present, various studies are being carried out in the context of security for mobile ad hoc networks [22], node misbehaviour [23], cloud-based threats [24], and IoT-based threats [25]; however, they have not been studied together. At the same time, game theory is found to be one of the better and more evolving security alternatives compared to the more frequently adopted cryptographic scheme [26,27]. There are studies to prove that the application of game theory to wireless networks offers more promising results when it comes to modelling [28]. Adopting game theory provides better control of user behaviour, which also yields better cooperation among the wireless nodes in the network. This process can be reflected in the improved performance of the network. Various game-based models address security and non-security demands in a wireless network. There is a broader scope for developing better security models using game models. Therefore, the proposed scheme contributes a novel strategic game model capable of identifying and resisting the participation of misbehaved nodes.

The contribution of the proposed model is as follows:

- The proposed scheme introduces a matrix of transactional records to access distributed storage systems and retain encoded sensitive information related to trust.
- A novel dual controller scheme is introduced, viz. Global Trust Controller and Core node Selection Controller, to formulate a secure agreement system for validating the global trust of all nodes.
- A unique payoff management scheme is introduced, which mainly performs speedy calculations, allocations, and updates, resulting in faster processing during routing operations.
- The proposed scheme deploys IoT-based mobile nodes in an ad hoc manner considering the usage of both private and public clouds for role identification, payoff selection, and gain maximisation.
- The results of the study are compared to existing game models with respect to accuracy, response time, energy, and cost, unlike any current security scheme in IoT.

The paper's organisation is as follows: Section 2 presents a discussion on existing schemes, followed by highlighting identified problems in Section 3. Section 4 discusses the adopted research methodology, while Section 5 discusses system design implementation. Section 6 highlights the outcomes, while Section 7 summarises the conclusion with respect to the inclusion of the novel features presented by the proposed scheme.

2. Existing Approaches

Presently, there are various security strategies for resisting possible intrusion in a wireless network, especially concerning the ad hoc mode of connectivity. This section discusses some of the significant contributions in this regard.

2.1. Studies on Misbehaviour

At present, there are different security mechanisms for resisting node misbehaviour problems. When a specific node starts to exhibit misbehaviour, it drastically decreases the communication performance of the wireless network. During node misbehaviour, the node usually violates the assigned routing scheme and adopts an unprogrammed ruleset, which could be detrimental to the entire communication system. The recent work by Paul et al. shows the adoption of vulnerable conditions in mobile ad hoc networks [28].

The study introduced an authentication mechanism to mitigate node misbehaviour using a collaborative approach of diffusing information about the local selfish node. Behfarnia and Eslami [29] developed a voting game-based scheme to identify node misbehaviour. The technique implements a single-stage Bayesian game for capturing information related to node uncertainties. Abhishekh et al. [30] presented a solution for relay node misbehaviour in the IoT environment. This model discusses an intrusion detection system to securely uplink and downlink communication between relay nodes and IoT networks. A study on misbehaviour detection was also carried out by Sharma and Liu et al. [31] using a supervised machine-learning scheme in the IoT context. A similar line of work was also carried out using prototyping by Astillo et al. [32], where a ruleset of behaviour is formulated for IoT, followed up by using the Kalman filter for data estimation. Zhang et al. [33] presented a significant detection model for secure communication among mobile nodes in a vehicular network. The model evaluates the weight of dynamic trust for time-varying misbehaviour while the trusted vehicle is selected along with the differential allocation of resources. A similar direction of work toward vehicular networks was formulated by Nguyen et al. [34]. The integrated usage of reputation and learning schemes is also reported to be used for misbehaviour detection as per the work of Gyawali et al. [35]. The model implements evidence-based theory using reputation value to ascertain secure communication among the vehicles. Studies on misbehaviour detection found insecure communication can be mitigated using the detect-before-decoding principle, as noted in the work of Ding and Wang [36].

2.2. Game-Based Security Studies

There are a number of works of literature where game theory concept is harnessed specifically to secure the wireless network. Game theory is used to build a strategic mathematical model to understand the interaction among players involved in the communication process. This involves implementing game theory to identify and resist vulnerable conditions during communication [37–40]. There has been some interesting research using game theory which offers potential insight into its capability to model intrusive interactions among communicating nodes [41]. The work done by Subba et al. [42] developed a game model of multiple layers on intrusion determination in ad hoc networks, which they claimed was capable of identifying various forms of attacks. Sun et al. [43] developed a tree-based security model that considers communication and security as two essential attributes of the Bayesian Nash Equilibrium game. The work of Liu et al. [44] presents a game-based mechanism to resist byzantine attacks, which takes into consideration the uncertainty of identifying the attackers. The implementation of the Stackelberg game model to fight jamming attacks is seen in the work of Li et al. [45]. Their model offers a distinctive role for standard transmitters and attackers, while it also implements a genetic algorithm for the optimal usage of resources. Qi et al. [46] present a sophisticated game model using Bayesian and Stackelberg games to resist intelligence jammers. This strategy also determines the rate of decline of transmission and eavesdropping. A unique adoption of the Stackelberg game and learning mechanism is seen in the work of Qi et al. [47]. The model accomplishes an equilibrium stage using a log-linear learning scheme to define its access policies. Furthermore, they experimented with using game theory to resist denial-of-service attacks in vehicular networks [48], combating network layer attacks [49], and improving trust in IoT [50].

2.3. Evolving Studies on Ad Hoc Security

An ad hoc network is an integral part of cloud computing and IoT, which will eventually mean that it is now exposed to a higher range of security threats. The conventional security protocols for ad hoc networks are restricted in their capability when integrated with IoT, which is a massive-scale deployment compared to conventional ad hoc networks. Fog computing, another revised version of cloud computing, is increasingly used, also has security concerns associated with it. Feng et al. [51] developed a secure game model for

resisting lethal threats in fog computing. A dynamic Stackelberg model was developed to improve the interaction among the actors in order to resist threats. A study on securing IoT was carried out by Wang et al. [52] using a collaborative game model: the stochastic Petri-net model. There are also other studies that have depicted the ongoing issues despite various existing IoT security schemes [53,54].

Hence, there is a need for a study to address the problems associated with different forms of security in the present state of challenging wireless networks. The following section highlights the problems identified.

3. Research Problems

Existing literature has some studies on resisting potential threats in a wireless network. However, specific open-ended issues are explored, which must be solved to mitigate the rising security concerns. The identified research problems are as follows:

- Gap between IoT and ad hoc network security: The current state of security solutions in ad hoc networks is not applicable when integrated with cloud or IoT systems. Due to the progress of technologies, the necessary revision has not been carried out considering the practical deployment environment. For example, when a mobile ad hoc network (MANET) node is deployed in IoT, the security protocol for it [13] differs from the security protocol of IoT [50]. Moreover, the ad hoc network concept is not considered much while all nodes are deployed in the IoT scenario; they are considered in terms of individual nodes and not in the form of a network. Currently, there are more IoT security schemes than conventional ad hoc security.
- Sophisticated Game Modelling: Studies prove that the game concept is one of the most rapidly evolving security solutions in the network [51,52]. However, most game concepts deployed to date associated the model with developing interactive game stages, including multiple steps. Although it was quite possible to use this multi-stage gaming model to address various traits of security, in the case of a complex environment, sophisticated measures had to be taken and there was less assurance of model sustainability. Hence, there is a need for a simplified and straightforward game model to perform better decision-making. Furthermore, it is notable that most of the existing game models have extensive payoff matrix computation, which also demands resources. Therefore, when applied to a sizeable practical network, such a sophisticated game model will call for a delay and higher response time. Thus, a lightweight game model is needed to secure a challenging communication environment.
- Computational Burden not emphasised: There are two forms of threats in the network; one form is when the attacker's identity is well-known based on their attack patterns, while the second form is unknown. Hence, security modelling confirming the presence of misbehaved nodes calls for an extensive set of observations to be carried out. Such threat monitoring calls for deploying a method with a lesser dependence on resources and the inclusion of smart operational processes geared towards identifying the attacker's intention in the least amount of time possible.

Therefore, existing studies do not emphasise balancing the computational demand with security on dynamic networks.

4. Proposed Methodology

The main purpose of the proposed scheme is to develop a framework capable of resisting the participation of misbehaved nodes, as well as strategies that can identify any form of nodes with an unauthorised presence in the data-forwarding process other than regular nodes. The work is an extension of our previous research [55–58] in which game theory on MANET is incorporated in addressing security vulnerabilities due to the presence of misbehaving nodes in a much larger scenario involving mobile IoT systems and cloud environments. The framework architecture for this purpose is shown in Figure 1.

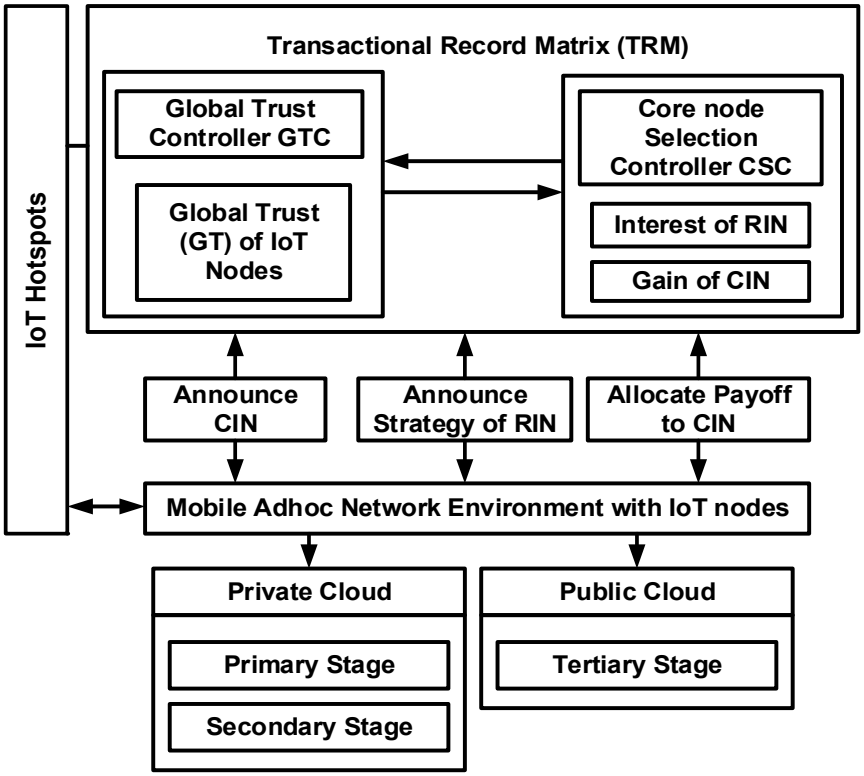


Figure 1. Proposed strategic game model for resisting malicious node participation formatting.

According to Figure 1, the study model contributes mainly to developing a transactional record matrix, which is essentially meant to retain all the essential transactional details for secure and simpler accessibility. The proposed scheme also develops a novel controller scheme which is completely based on trust evaluation over various roles of nodes. On the basis of resources as well as evaluated trust score, the scheme selects Core IoT Nodes (CIN), as well as defines the strategy of operation for RIN with its allocated payoff. The complete implementation cycle considers mobile nodes deployed in an IoT environment with an ad hoc network. The environment is also supported by private and public cloud ecosystems for rendering service availability. The core contribution of proposed scheme is to deploy a novel game mechanism in order to secure data transmission in an IoT environment with mobile nodes. The work adopts an analytical research methodology to develop a series of operations where the details are as follows:

- Environment: The presence of both regular mobile IoT nodes and malicious nodes is regarded as misbehaving nodes by the environment. Nodes are assumed to adhere to any conventional on-demand routing scheme, which adds security to the existing routing scheme, and no mobile IoT nodes forward data on their own. Instead, a core IoT node is used to perform the task during the propagation process and thus save the most resources.
- Core Actors: There are two types of core actors in the proposed system, which are Core IoT Nodes (CIN) and Regular IoT Nodes (RIN). An RIN collects all the data and forwards them to a destination node in an ad hoc manner if it is located within its communication range. Otherwise, the RIN takes the assistance of the CIN by sending a request control message to the latter as a part of the interaction between CIN and RIN. CIN does not participate in data aggregation or typical forwarding processes, unlike the intermediate nodes in conventional ad hoc networks. Instead, CIN are selected based on potential connectivity with a higher probability of linking to the destination node. Hence, any node with a high number of connected links (apart from RIN) and better residual energy is selected as a CIN. The proposed scheme entails the

process of CIN selection by RIN based on newly formulated quality metrics and global trust. Therefore, from a security viewpoint, any node with a higher value of computed trust in a proposed scheme is finalised to be selected as a CIN. Upon receiving the information of the destination node from the CIN, the RIN forwards the data.

- Transactional Record Matrix (TRM): Unlike existing schemes, the proposed method does not retain or process the transactional routing data in one area of storage units. Instead, it creates a distributed database system where all of the transactional information is split and stored. The majority of the essential security-based processed information (global trust, Quality metric, roles, payoff, gains) evaluated by the controller system is managed in distributed order to restrict any form of direct accessibility by any unauthorised node.
- Cloud-Based Enabling Technologies: The proposed scheme makes use of both private and public clouds to improve privacy control and cost-effectiveness. Private cloud systems store information about the actors' identified roles (primary level) and payments for RIN (secondary level), whereas public cloud systems store data on profit maximisation when it comes to selecting CIN (tertiary level). It should be noted that the cloud ecosystem is the underlying technology of the IoT environment, where the matrix of transaction records is explicitly maintained. Because of the discrete location, it becomes computationally extensive, making it impossible for any unauthorised node to intrude on both clouds at the same time.
- Modelling Game Concept: The development of the proposed scheme's security condition is based on a strategic game model considering the selection of CIN using a Core node Selection Controller (CSC) and Global Trust Controller (GTC). The value of GTC is obtained from CSC to find the potential CIN. The main idea is to confirm the legitimacy of the CIN by encouraging the participation of a good number of RIN. The allocation of payoff and gain computation is based on trust, quality, and roles observed over a limited channel capacity. Unlike any conventional game model, the operation involved in this model is relatively straightforward and does not involve any conditional logic, which could cause contradictions in discovering node misbehaviour.

The following section further illustrates an extended discussion of all the essential security processes to resist the participation of node misbehaviour.

5. System Design

The first part of developing the proposed scheme is constructing a matrix to store the transactional records, which will act as a shared database system. The novelty of this initial step is that the proposed model keeps the transactional records of data being exchanged by mobile nodes in an encoded form in a distributed yet highly connected database system. The proposed scheme implements a strategic game model to control node misbehaviour, which deploys an on-demand ad hoc protocol. The proposed concept of the strategic game model allocates two discrete roles of a mobile node in IoT, the CIN and RIN. The complete implementation of the proposed security model is carried out in three stages, viz. primary, secondary, and tertiary. The primary stage is responsible for determining the role played by each TRM, while the secondary stage performs the selection of the payoff for the RCN. The tertiary stage enhances the gain for the RCN. It should be noted that the operation carried out for the primary and secondary stages is carried out over the private cloud, which is not accessible to all nodes, while the tertiary stage is carried out in the public cloud, which is accessible to every IoT node in the environment. The scheme ensures that TRM is introduced in mobile IoT systems to perform various operation sequences, viz. (i) consistent validation of GTC scores exchanged by any mobile IoT nodes, (ii) efficient selection of CIN, and (iii) reliable allocation of payoffs for the CIN. The implementation is carried out using both public and private cloud ecosystems to retain better cost-effectiveness of the proposed strategic game model.

The study considers the deployment of TRM within an IoT hotspot, a type of an access point mounted within the environment with a coverage range slightly more than that of

mobile IoT nodes. The realisation of the proposed model is carried out by developing a unique agreement system responsible for automating the predefined execution of programs within TRM. The two essential actors in this process are the GTC and CSC. The GTC is responsible for storing and updating the global trust value of all the mobile IoT nodes publicly. It will eventually mean that the proposed scheme assists in validating the shared value of global trust through any communicating IoT nodes. The CSC is responsible for aggregating the game strategies adopted by RIN and CIN, in order to select the upcoming CIN, thereby keeping the network updated. Furthermore, CSC also performs the aggregation and dispatching of the computed payoff from normal IoT nodes to their respective CIN to permit cooperation with each other. Further operation is discussed as follows.

5.1. Private Cloud IoT System

The proposed scheme assumes that any prevalent routing scheme, such as AODV and OLSR, is implemented, so that selecting the respective CIN can be carried out on the mobile IoT nodes, which ultimately assists in forwarding the routing information. The scheme also assumes that all the mobile IoT nodes maintain TRM to formulate its encoded address, which further enables communication with the agreement system. Additionally, the proposed scheme considers *global trust* (*GT*) and *quality metric* (*QM*) parameters for identifying mobile IoT nodes. The quality of service is computed by obtaining the information from the control message for route discovery by mobile IoT nodes working in an ad hoc environment. The mathematical expression for computed quality metric α is as shown in Equation (1):

$$\alpha_i = C_i \cdot A_i \cdot P_i \tag{1}$$

As shown in Equation (1), the computed quality metric of ith node α_i depends upon residual channel capacity C_i, adjacent nodes of ith node A_i, and weight of specific mobility path of ith node P_i. Apart from this, it should be noted that computation of global trust is a representation of reliability factor based on previously exhibited behaviour of mobile IoT nodes. This is an essential security enhancement, as in case of node misbehaviour, the value of the quality metric will either rise or decline significantly. Hence, an abnormality of quality metric will be the primary indicator of misbehaved nodes in an ad hoc environment. Furthermore, it should also be noted that the value of the computed global trust fluctuates in different contexts. An attacker node can misuse this by sharing any random *GT* value (within the observed fluctuation) to get an illegitimate entry into the IoT ecosystem. This problem is addressed by using TRM, which assists in validating all the shared values of global trust.

The proposed strategic game framework amends the on-demand routing by incorporating only two forms of control message, viz. (i) the first control message C_{msg1}, which is required for preliminary route discovery by sharing node-based local information, and (ii) the second control message C_{msg2}, which is required for forwarding a command that is exchanged in the private cloud among RIN. This control message retains the information of the selected node in order to play the role of CIN and the payoff recommended by the RIN of each node. The RIN further processes this information to confirm the node's intention towards a similar CIN. The size of both control messages is 31 bits. Figure 2a highlights the format of C_{msg1}, where *QM* is a quality metric field while the *GT* field retains a global trust score. The CIN field exhibits the current role of a mobile IoT node to be a CIN. Figure 2b has fields of respective payoffs for the current CIN. As the complete operation is carried out over a private cloud system, there is no way such information could be easier to access by an attacker node. Even if the node misbehaves for this purpose, the value of each field in the control message will change, which will fail the validation process of shared information of global trust.

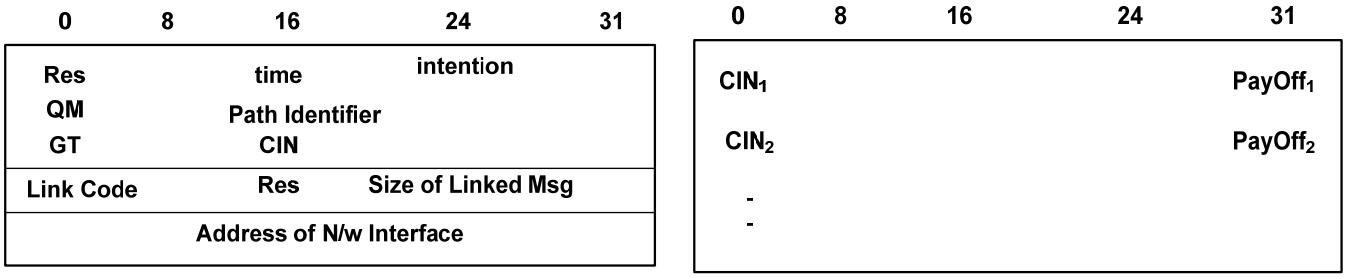


Figure 2. Format of newly formulated control message: (**a**) format for $C_{msg}1$; (**b**) format for $C_{msg}2$.

5.2. Public Cloud IoT System

This work employs game theory to deploy its security scheme based on global trust and the selection of CIN. To accomplish this, a simplified dual controller design, namely GTC and CSC, is used in the development of an agreement system. The following is an explanation of how these two controllers work:

- Global Trust Controller (GTC): This controller system is responsible for managing all the updates for legitimate IoT nodes. The process is carried out over the public cloud system, making the operation in adherence to the agreement system as illustrated in Figure 3. A reliable source is provided to all nodes to perform the validation for the obtained controlled message.
- The classification of dependable parameters, as shown in Figure 3, demonstrates that the entire validation process carried out by GTC is done using the address of the mobile IoT node and a list of all connected nodes maintained in TRM. To access the legitimate IoT node, obtain its global trust, and update its value, an explicit set of functions is built. The first function, 'index legitimate IoT node,' is in charge of indexing the legitimate mobile IoT node while also determining whether the target node is present in the list of node addresses in TRM. In the case of a new mobile IoT node, it configures the address of the mobile IoT node with the address of the destination mobile IoT node, along with initialising the default value of global trust. This information is then added to the list. The second function, 'obtain global trust', is responsible for validating the global trust score that finally returns the score of global trust stored in the public cloud system. The new value of the global trust is configured using this function's agreement system, which is the prime operation of the third function, 'update global trust score'.
- Core node Selection Controller (CSC): This controller aggregates all the possible strategies of both the players, i.e., CIN and RIN, along with the constructs of the core structure that retain information about the RIN, CIN and local information of mobile IoT nodes. As shown in Figure 4, the core structure associated with the CIN maintains information about their respective identity and residual channel capacity. At the same time, the RIN holds information about the address of TRM and payoff. Furthermore, the dependent entities of CSC will consist of an object of CIN, as well as its respective address, as shown in Figure 4. The first function, 'define CIN,' is used to self-declare a mobile IoT node as a CIN in the public cloud. This function generates a CIN object by extracting the global trust score from GTC, while the second function, 'obtain CIN,' returns a list of all of the defined CIN. The third function, 'Strategy,' is used to build RIN.

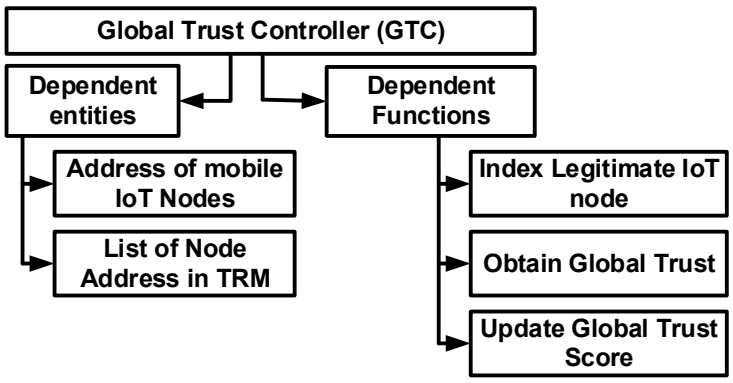


Figure 3. Dependent entities and function of GTC.

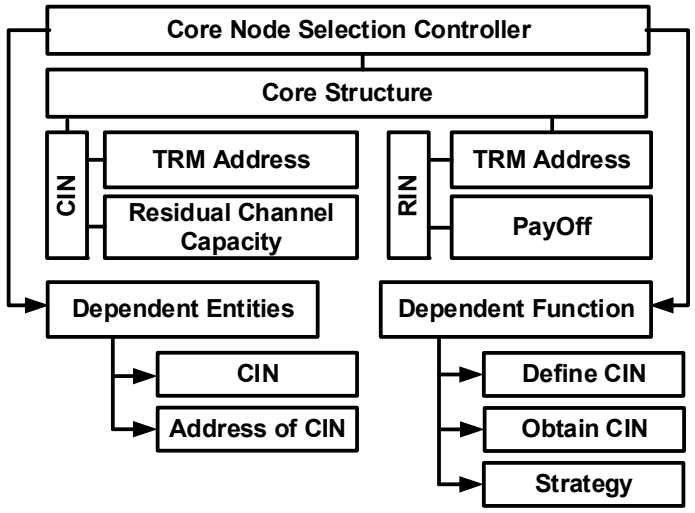


Figure 4. Core structures, dependent entities, and function of CSC.

5.3. Strategic Game Model

The incorporation of this strategic game model (SGM) optimises the selection process of CIN. The proposed SGM uses both public and private cloud ecosystems to select legitimate nodes cost-effectively and reliably. For any given adjacent nodes, each node in a distributed ad hoc environment of IoT is required to define its CIN and RIN along with its explicit roles. In contrast to all possible adjacent nodes, a specific *i*th node is needed to announce itself as a CIN, based on quality metric QM and global trust GT attributes. For this purpose, a set of adjacent nodes $A(i)$ is considered by the *i*th mobile node with an input of QM and GT. A matrix is constructed for adjacent nodes consisting of GT, QM, and their respective identity information. An *i*th node announces itself as a CIN if its QM score is found to be more than a cut-off value of the same as its adjacent nodes. A similar selection operation is carried out for a higher value of GT if both are found to be less than the cut-off, then the *i*th node announces itself as a RIN. All RIN must compare their features with respect to QM and GT to make them deployable for RINs. Using this operation, a definite payoff is allocated to the RIN when it plays the role of CIN. This is one of the essential processes from a security and privacy perspective, as misbehaved nodes will never be able to announce themselves owing to the discrepancies in their QM and GT scores. The empirical expression used for representing the degree of fluctuation between the CIN and RIN, i.e., $QM_{RIN-CIN}$ perspective, is as shown in Equation (2):

$$QM_{RIN-CIN} = (1 - \Delta QM) \times 100 \quad (2)$$

Equation (2) shows that the variable ΔQM represents the ratio of QM for RIN to QM for CIN. A similar mathematical strategy, shown in Equation (3), is applied for the expression fluctuation of GT for CIN and RIN as follows:

$$GT_{RIN-CIN} = (1 - \Delta GT) \times 100 \tag{3}$$

As shown in Equation (3), the variable ΔGT represents the ratio of GT for RIN to QM for CIN. The above two expressions are used to overcome the possible evolution of fluctuation and hence assist in normalising it. It should be noted that selection of CIN is carried out if an ith node consists of higher values than either of the above expressions in the least case or both expressions in the best case. The search and selection of the feasible CIN among the adjacent nodes in IoT are carried out by the ith node that announces itself as RIN. The RIN allocates an optimal payoff to the selected CIN based on their services. The value of the payoff to be assigned to the CIN is entirely equivalent to the legitimacy of the CIN, based on the QM and GT scores stated in both Equations (2) and (3). The mathematical computation of the payoff for the RIN is expressed as in Equation (4).

$$P_{RIN-CIN} = mean(QM_{RIN-CIN}, GT_{RIN-CIN}) \tag{4}$$

There is also a possibility that the value of the payoff is to witness multiple acceptances by multiple numbers of RIN within the communication range of CIN. In such conditions, the RIN is required to compute the gain, G, for selecting the CIN, which is mathematically expressed as in Equation (5),

$$G_{RIN-CIN} = [\theta(P_{RIN-CIN}).\, QM] - P_{RIN-CIN} \tag{5}$$

Equation (5) shows that the first component $\theta(P_{RIN-CIN})$ is equivalent to the individual payoff $P_{RIN-CIN}$ divided by the total value of the payoffs $P_{RIN-CIN}$ for all the adjacent nodes. The second component, QM, is the summation of ΔQM and ΔGT obtained from Equations (2) and (3). The actor, RIN, is the one that initiates the game by exploring the feasibility of CIN in the vicinity of their communication range, i.e., CIN(RIN). At the same time, it uses a private cloud to do so using its on-demand routing scheme for propagation. A misbehaved node cannot mimic this mechanism, as the complete operation is carried out over private networks of the IoT-cloud system. The method uses the function of obtaining CIN information from the CSC module to extract information from a group of all of the nodes with higher values of QM and GT to be elected as a CIN. The system performs the computation of payoff $P_{RIN-CIN}$ based on its respective attributes (i.e., $QM_{RIN-CIN}$, $GT_{RIN-CIN}$), considering all the CIN present in the set obtained from this function of CSC. Using a direct propagation of control message among the mobile IoT nodes in an ad hoc network, the system shares computed payoff $P_{CIN-RIN}$ among its adjacent mobile nodes. For better cost control, this operation is carried out in the private cloud; however, the final calculated value of the adjusted payoff is stored in a public cloud system where this information is appended to the CSC module using a discrete function of '*strategy*' shown in Figure 4.

After executing the above-mentioned step, the proposed system aggregates the RIN interested in cooperation. At the same time, their recommended computed individual payoff values are used for maximising the gain of the selected CIN. In this part of the implementation, the core target is to confirm that the RIN is capable of increasing the payoff of the CIN in adherence to the allocated channel capacity value in the IoT-cloud system. Under these conditions, the presence of any misbehaved nodes demands the usage of more channel capacity, which the system instantly identifies due to contraction of the logical condition formed for selecting CIN. Apart from this operation, the scheme assists in directly propagating computed payoff to the accepted CIN by the RIN. Applying the concept of game theory, the proposed system mathematically defines the motivation of the CIN in

the form of utility, based on their interest/motivation with respect to QM, GT, and P. The expression for the utility of CIN is as written in Equation (6):

$$\rho_{CIN-RIN} = \sum_{i=1}^{R} \left[P_{(RIN-CIN)i} + QM_{(RIN-CIN)i} + GT_{(RIN-CIN)i} \right] \quad (6)$$

Using the list consisting of game strategy (as a dependent function of CSC), the system represents the node's interest with respect to their optimal payoff P, GT, and QM. The initiation of the game is carried out by computing utility $\rho_{CIN-RIN}$, $QM_{CIN-RIN}$, and $GT_{CIN-RIN}$. The system then computes the proportion of utility with respect to the demanded channel capacity followed up by evaluating the summation of all of the required channel capacity from the interested RIN. In the preliminary stage of this process, it accepts the whole list of selected RIN, which is reduced down by the filtering process. In this filtering process, the system checks if the total demanded channel capacity of the interested RIN is found to be more than the residual channel capacity at the CIN. Finally, the system filters out the RIN with a reduced value of utility ρ. At the same time, the ultimate set of RIN is deployed by the selected CIN in the CSC module to confirm the final RIN.

In the proposed SGM, the CIN announce its new role in the CSC module, which then computes the GT score in the GTC module. The identified role of the CIN is shared with the route-discovery control message that is exchanged with its adjacent mobile IoT nodes. All of the RIN validate the request message received from the CSC module using a function of obtaining CIN. The determination of the payoff is carried out by selecting CIN using the RIN after it gets a list of feasible CIN. The sharing of this payoff takes place in a private cloud among all of the RIN, which can further assist in fine-tuning their recommended payoffs and confirming the finally selected CIN. The announcement of the final CIN is carried out by the RIN, which updates all the nodes.

Hence, by adopting the SGM, the scheme ensures that no misbehaved nodes present in an ad hoc network environment will ever be able to distort or manipulate any form of routing information (both control message and data). Without using any form of conventional encryption mechanism, this system develops the first line of defense system restricting any form of participation of any illegitimate or unauthorised node.

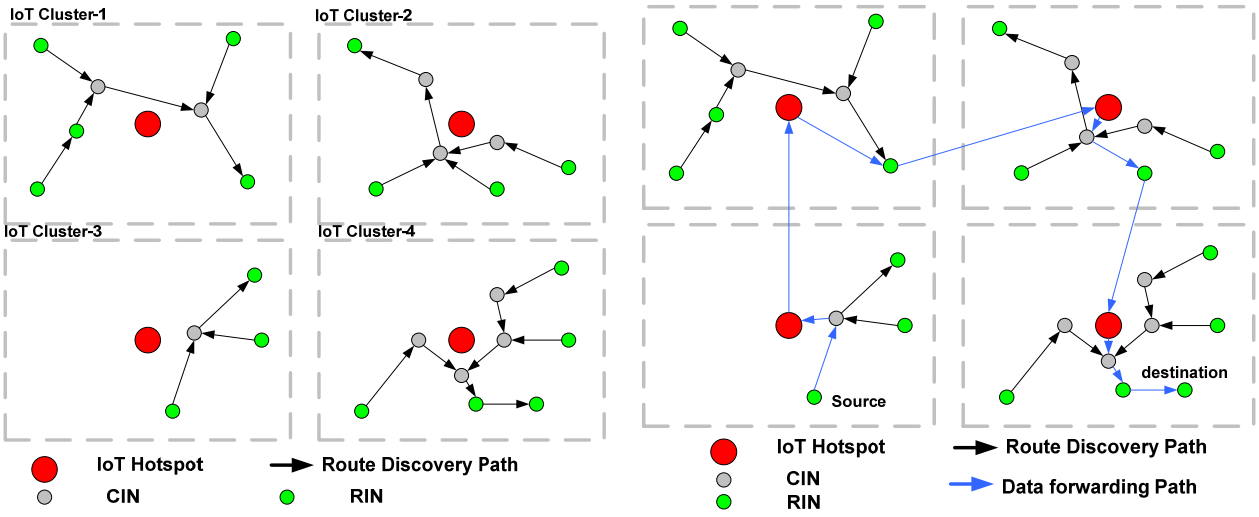
6. Result Discussion

Whereas the preceding section posits the scheme as employing a novel game model, with the primary goal of identifying misbehaving mobile IoT nodes and then resisting their participation in the data-forwarding process, this section discusses the simulation environment and analysis strategy used, followed by a discussion of the results obtained.

6.1. Simulation Environment

The first step in developing a simulation strategy is to create a comprehensive IoT environment in a clustered form, as shown in Figure 5a, which depicts a sample of four IoT clustered zones. As shown in Figure 5, the RIN communicates with other nodes via single-hop communication, if it is closer to their transmission range, or it requires the assistance of CIN, whose selection process was discussed in the previous section. It should be noted that depending on the density of nodes in each cluster, there may be multiple IoT access points. However, the absence of a CIN will cause the RIN to communicate with the IoT hotspot, which will then search for the nearest CIN. The address of the new CIN is shared with RIN. An IoT hotspot is assumed to offer sufficient coverage for all types of nodes within each cluster. Figure 5a highlights the intra-cluster operation where the control message is propagated to look for the destination node. If the destination node is located within the cluster, the target mobile node follows the path (shared by CIN) to share the data with its destination node. Figure 5b highlights the inter-clustering operation where the source and destination node are located in different clusters. In such cases, the IoT hotspots assist in sharing the address of the next relay node located in different clusters and finally assist in offering proper path information. The proposed study considers Optimized Link

Source Routing for this process owing to its lesser delay performance and suitability for dynamic change in ad hoc networks [59].



(**a**) (**b**)

Figure 5. Simulation environment of the proposed scheme: (**a**) IoT cluster formation and routing initiation; (**b**) Inter-cluster data forwarding.

Table 1 highlights the simulation parameters considered for the analysis. It should be noted that the values of the simulation parameters were configured from observation carried out on the frequently implemented research work in the existing system.

Table 1. Simulation parameters.

#	Parameters	Values
1	Number of Nodes	500–1000
2	Node deployment	Random
3	Initialised Energy	10 J
4	Iteration	1000
5	Sensing Range of Node	10 m
6	Sensing range of IoT access point	100 m
7	Dimension of one unit of IoT Cluster	100×100 m^2

All the values tabulated in Table 1 can be amended to suit any application demands in IoT. While analysed with a different range of values, the variation in numerical outcomes was found to be only a mere 5.27%, which exhibits the consistency of the proposed model implementation.

6.2. Analysis Strategy

The first strategy of analysing the results of the study is to compare it with existing game models, which are Nash equilibrium, Bayesian Nash Equilibrium, and Stackelberg Game. The main justification behind the selection of these three existing game models mentioned above is as follows:

- Adoption of Nash equilibrium assists in accurately detecting the best payoff for a player based on the decision of the player and other players. Hence, when it comes to estimating global trust in ad hoc environments, Nash equilibrium offers an unbiased estimation of all the individual trust scores that can be applied for the cause of both routing and security in large IoT scenarios.

- Adoption of Bayesian Nash Equilibrium depends on retaining a belief in target players aligned with the adopted strategies of remnant players. This is a better option than Nash equilibrium as the latter does not offer the players' belief score specifications. Eventually, it means that Bayesian Nash Equilibrium leads the nodes to converge into perfect strategically formulated beliefs with better consistency when exposed to vulnerable conditions. Hence, any deviation in trust score and belief will directly indicate the presence of malicious/misbehaved nodes.
- Stackelberg game is the most frequently implemented game model compared to other game models. According to this game mode, a sequential decision is prioritised over a simultaneous one. This model offers better decision making to the second mover, who can adopt a strategy based on action undertaken by the first mover. Apart from this, the best part of this model is the optimal acquisition of operational cost by the follower node. This eventually implies better decision making with higher clarity by the regular node, in order to perform secure routing upon detecting unknown/uncertainly behaved nodes in large-scale dynamic networks.

The secondary strategy for analysis is to incorporate 5–10% of total nodes as misbehaving nodes whose identities are not predefined or shared with adjacent nodes in each IoT cluster. This setting allows deploying an unknown attacker node in the simulation area, which must be identified and isolated from active routing operations. The tertiary strategy of the proposed scheme is to carry out the analysis using standard performance metrics of identification accuracy, energy consumption, cost, and response time. The rationale behind adopting these metrics is stated in the following subsection.

6.3. Result Accomplished

The complete implementation was carried out in a MATLAB environment on a standard 64-bit windows machine with an i7 processor. Observation of the results was carried out for 1000 iterations, and its numerical scores are represented in graphical analysis for better analytical representation. Each analysis was carried out in a similar test environment, considering four performance metrics and compared with three frequently adopted game models. The discussion of these outcomes is as follows:

6.3.1. Identification Accuracy

This parameter highlights the actual score of correctly identifying the proportion of misbehaved nodes after implementing the proposed scheme. Mathematically, the computation of accuracy was carried out using Equation (7):

$$Accuracy = \frac{I_n}{T} \times 100 \tag{7}$$

As shown in Equation (7), the computation of *Accuracy* was achieved considering positively identified misbehaved nodes, I_n, with respect to total nodes, T. The outcome of this analysis is shown in Figure 6, which shows that the proposed system offers significantly higher accuracy in contrast to the existing game model.

The justification behind this outcome is that though adopting the Nash equilibrium model offers better detection of the payoff, the identified payoff does not remain the same during the attack, especially if the attackers employ a dynamic strategy. This problem is somewhat addressed using Bayesian Nash Equilibrium, where a better convergence rate is obtained due to better consistency in its belief-system formulation. However, the formulated belief and its respective consistency do not cope with the dynamic strategies adopted by the misbehaving nodes over time, which is one downfall of this approach. Nonetheless, this is one of the best approaches if the attacker's behaviour is known, assuming it will not change until the allocation of payoff. A similar problem also exists in the Stackelberg game model.

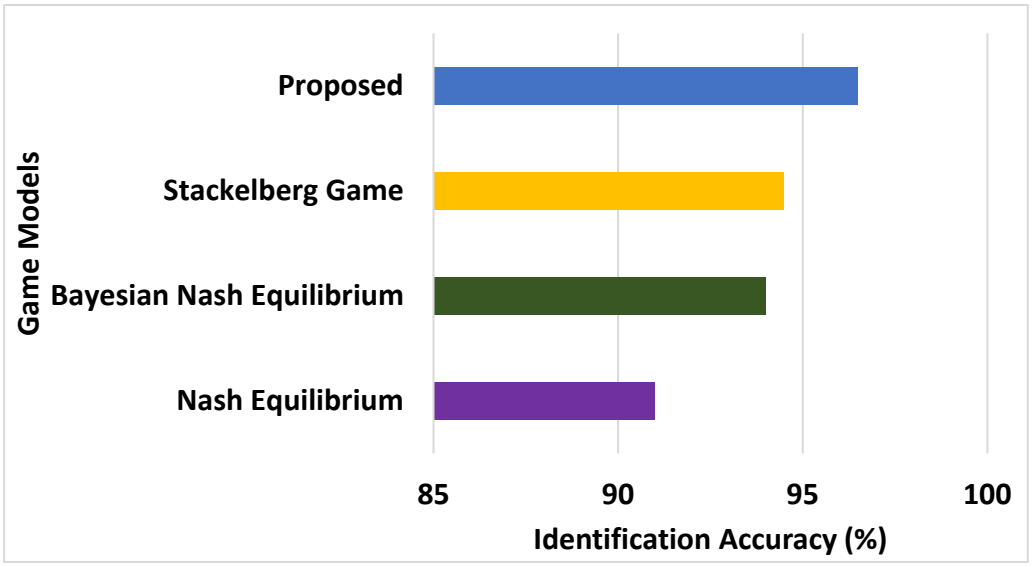


Figure 6. Comparative analysis of identification accuracy.

On the other hand, the proposed scheme, by adopting the concept of distributed TRM, allows a faster progression towards the payoff computation upon finding any deviation in computed GT or QM. Hence, the proposed scheme's accuracy in identifying misbehaved nodes in large-scale deployment is relatively higher. Therefore, this scheme offers a reliable outcome when the mobile IoT nodes are deployed in an ad hoc manner in a large-scale deployment area.

6.3.2. Analysis of Energy Consumption

Energy is one of the essential resources while performing any form of node operation, be it routing or security implementation. Higher energy retention is always a necessary demand in the computation of game models to this end, owing to the mathematical computation involved. Apart from this, the proposed system performs three stages of operation, synchronised with private and public clouds, including multiple sequences of computing-updated GT and QM based on the dual roles of nodes (CIN and RIN). For this purpose, the mobile nodes are assigned with an initial energy of 10 J, while they will consume 50 nJ for forwarding 1 bit of data. This condition is based on the first-order radio energy model [60]. The mathematical expression used for computing total energy, E_T, consumption is written in Equation (8):

$$E_T = E_{TX} + E_{RX} + E_{agg} + E_{amp} \tag{8}$$

In Equation (8), the dependable variables for the computation of energy are transmittance energy, E_{TX}, receiving energy, E_{RX}, aggregation energy, E_{agg}, and amplification energy, E_{amp} [60]. Figure 7 showcases that this scheme offers reduced energy consumption compared to other models observed over the entire iteration.

The prime reason for the consumption of energy during data propagation of nodes is mainly due to more retransmission attempts of control messages, C_{msg}, in the case of non-availability of adjacent nodes, more usage of amplified energy, E_{amp}, during the condition of signal attenuation, or higher fluctuation of mobility of IoT nodes. Considering the possibility of any of these circumstances, or all of them, the proposed system introduces a concept where IoT hotspots and CIN reduce the extensive load on route discovery and data propagation. Apart from this, the allocation and updating of payoffs are carried out via TRM, which is highly distributed, reducing the effort of either confirming the presence of misbehaved nodes or performing data delivery. Hence, there is less fluctuation from an identified path of propagation by mobile IoT nodes in the proposed system,

resulting in higher retention of residual energy. On the other hand, all of the existing game models include highly sophisticated logical conditions for evolving with a secured strategy, resulting in extensive energy depletion.

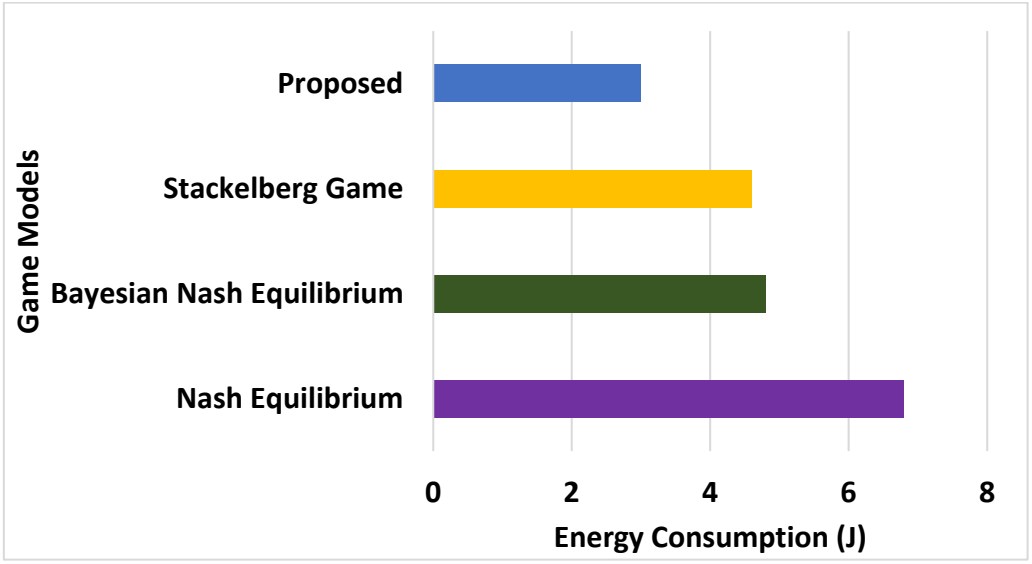


Figure 7. Comparative analysis of energy consumption.

6.3.3. Analysis of Cost

To assess the practicality of the proposed system, it is sufficient to understand the overall cost involved in the implementation. The proposed system defines the term *cost* as overall resources and operations involved in executing the proposed strategic game model in order to resist malicious node participation. The mathematical expression used for this purpose is as in Equation (9):

$$C = \frac{C_{TRM} + C_{stages} + C_{pay} + C_{Cloud}}{n} \quad (9)$$

Equation (9) shows that the evaluation of cost, C, depends upon the cost of maintaining TRM, C_{TRM}, the cost of three stages of operation, C_{stages}, the cost of payoff computation, allocation, and updating, C_{pay}, and the cost of dual-cloud-based game modelling, C_{Cloud}, with respect to the total number of deployed nodes, n. The proposed system uniformly allocates the hypothetical and dimensionless numerical value of one unit of consumed cost for each of the four operations. With each operation observed in 1000 simulation rounds, the analysis arrived at the outcome shown in Figure 8, which exhibits a lower cost for the proposed system.

From the observation in Figure 8, it can be noted that Nash equilibrium is not significantly different from Bayesian Nash Equilibrium. The prime reason for the higher cost involved in this existing system is that the Nash equilibrium strategy depends on all the known and correct strategies of other nodes. Such computation can never be carried out, especially if the intrusion type is highly dynamic, where a node could alter their strategy of attack even if they announce a different strategy during game interaction (to increase their payoff). Furthermore, a similar problem exists in Bayesian Nash Equilibrium. Still, other forms include extensive operation steps to compute payoffs usually maintained in a multi-dimensional matrix. Hence, the system takes more effort to compute the payoff and visit and re-visit the payoff matrix every time, increasing the value of the C_{pay} parameter. Stackelberg's game has an obvious advantage in this regard. However, the payoff still significantly reduces for the second mover. Hence, it has to carry out more operations to get an appropriate payoff, increasing the value of C_{pay} and C_{stages}, incurring more costs to complete the entire security operation.

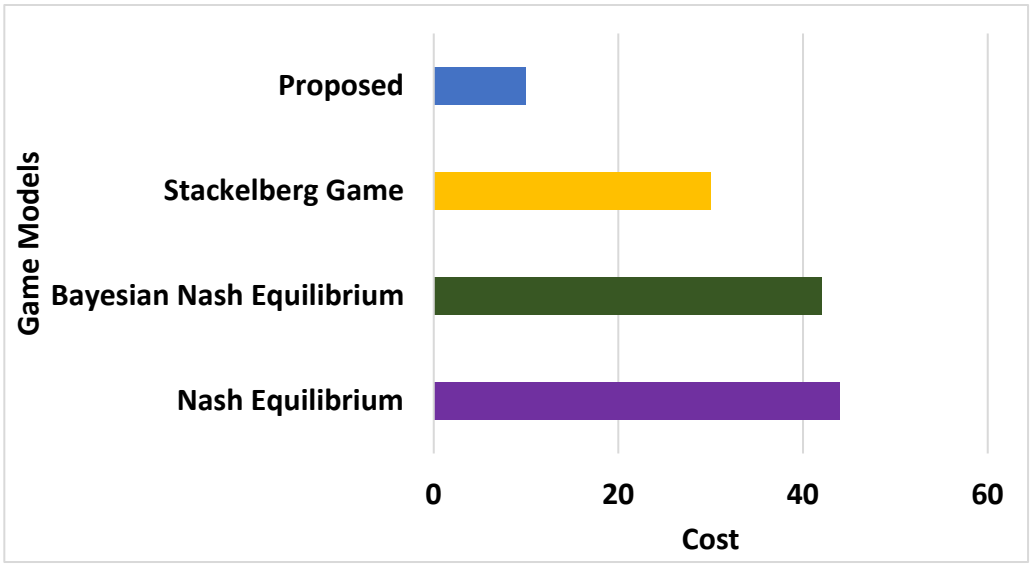


Figure 8. Comparative analysis of cost.

6.3.4. Analysis of Response Time

Response time is a critical parameter to consider, especially for security systems; higher response time is detrimental for any form of the network where a malicious node will have an opportunity to reframe its attack strategy further. The computation of response time is programmatically carried out as the time between the start point of the first request of the source node to propagate data (to the neighbouring node, or CIN or IoT access point) until the data are successfully forwarded to the destination node. Figure 9 highlights that the proposed system offers a superior performance of highly reduced response time compared to the existing scheme.

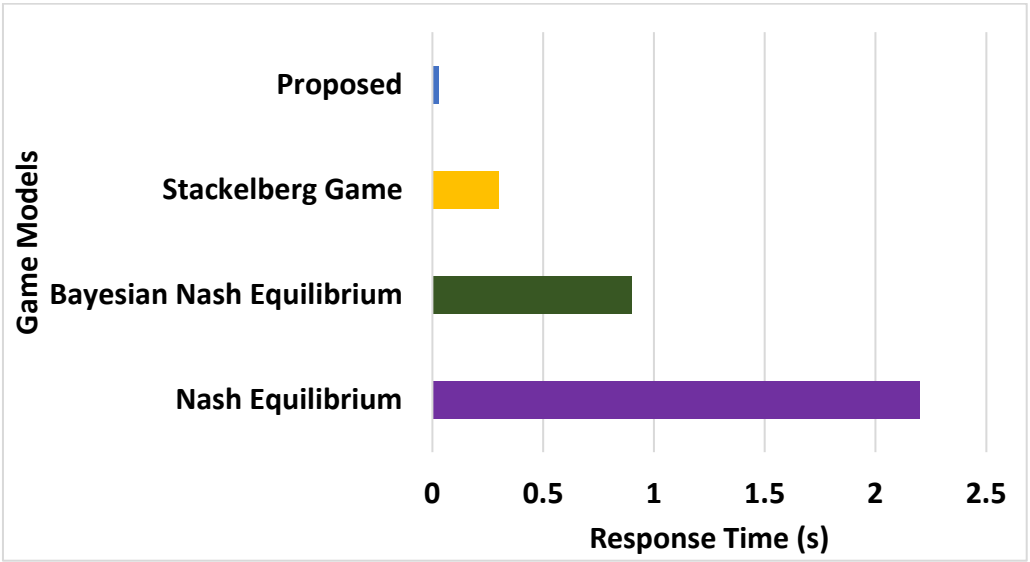


Figure 9. Comparative analysis of response time.

The outcome exhibited in Figure 9 shows that TRM's contribution was more about incorporating the distributed scheme in order to maintain sensitive transactional information in distributed cloud storage in encoded form. However, a deeper insight into TRM shows that it offers faster availability of its service to store the sensitive payoff information, or to generate the information based on the request of RIN or CIN. It eventually means that the confirmation of security facts for any target node during data transmission is almost

instantaneous because of TRM. Apart from this, both modules of GTC and CSC exchange information upon any event, which causes speedy delivery of services related to *GT*, *QM*, roles, the path of propagation, and optimally selected CIN. This operation to distribute service availability is quite challenging for any existing game model resulting in increased response time.

7. Conclusions

The proposed study model introduces a novel mechanism to thwart node misbehaviour in the ad hoc environment of the mobile IoT ecosystem. The scheme mainly focuses on better quality management the for secure deployment of on-demand routing protocol. Integrating public and private cloud modelling is carried out to manage cost-effective agreement systems, i.e., GTC and CSC. Interestingly, the scheme maintains a distributed security scheme to resist dynamic node misbehaviour. The novelty introduced by the proposed scheme is that: (i) it differs from any existing game modelling scheme, in that the proposed system allows the selection of CIN with more comprehensive ranges of scores (*GT*, *QM*, roles, payoff, gain) with highly reduced time spent on updating them; (ii) the introduction of TRM permits the first layer of security as well as service availability simultaneously where the encoded payoff information is only forwarded to the legitimate nodes, preventing higher processing time and service delivery; (iii) the maximisation of gain in the selection of CIN is one essential security contribution which balances both security demands and computational burden-reduction demand at the same time; (iv) the quantified results obtained suggest that our proposed scheme offers approximately 36% higher identification accuracy, a 25% reduction in energy consumption, 11% faster response time, and a 27% reduction in cost incurred compared to existing game models.

Author Contributions: Conceptualisation, methodology: B.U.I.K.; validation, writing review and editing: B.U.I.K., F.A., K.W.G., R.F.O., F.D.B.A.R., M.A.R. and Z.J.; formal analysis, investigation, writing original draft preparation: B.U.I.K. and F.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research was partially supported by IIUM-UMP-UiTM Sustainable Research Collaboration Grant 2020 (SRCG) under Grant ID: SRCG20-013-0013.

Data Availability Statement: Not applicable.

Acknowledgments: The authors express their personal appreciation for the effort of Binyamin Adeniyi Ajayi, Manasha Saqib and Gousia Nissar in proofreading, editing, and formatting the paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kanellopoulos, D.; Cuomo, F. Recent developments on mobile ad-hoc networks and vehicular ad-hoc networks. *Electronics* **2021**, *10*, 364. [CrossRef]
2. Das, S.; Samanta, S.; Dey, N.; Patel, B.; Hassanien, A. *Architectural Wireless Networks Solutions and Security Issues*, 1st ed.; Springer: Singapore, 2021; p. 323.
3. Srilakshmi, R.; Bhaskar, M. Prevention of attacks in mobile ad hoc network using African buffalo monitoring zone protocol. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*, 184–192. [CrossRef]
4. Prasad, M.; Tripathi, S.; Dahal, K. An enhanced detection system against routing attacks in mobile ad-hoc network. *Wirel. Netw.* **2022**, *28*, 1411–1428. [CrossRef]
5. Chiejina, E.; Xiao, H.; Christianson, B.; Mylonas, A.; Chiejina, C. A robust Dirichlet reputation and trust evaluation of nodes in mobile ad hoc networks. *Sensors* **2022**, *22*, 571. [CrossRef]
6. Dai, J.; Xu, X. A Analysis Of Attack And Defense Mobile Ad Hoc Network Based On OPNET. *IOP Conf. Ser. Mater. Sci. Eng.* **2019**, *611*, 012081. [CrossRef]
7. Mangla, M.; Satpathy, S.; Nayak, B.; Mohanty, S. *Integration of Cloud Computing with Internet of Things-Foundations, Analytics and Applications*; John Wiley & Sons: Hoboken, NJ, USA, 2021; p. 384.
8. Bruzgiene, R.; Narbutaite, L.; Adomkus, T. MANET Network in Internet of Things System. In *Ad Hoc Networks*; Ortiz, J., Pachon De La Cruz, A., Eds.; BoD–Books on Demand: Norderstedt, Germany, 2017; pp. 89–114.
9. Tournier, J.; Lesueur, F.; Mouël, F.; Guyon, L.; Ben-Hassine, H. A survey of IoT protocols and their security issues through the lens of a generic IoT stack. *Internet Things* **2021**, *16*, 100264. [CrossRef]

10. Sobin, C. A Survey on architecture, protocols and challenges in IoT. *Wirel. Pers. Commun.* **2020**, *112*, 1383–1429. [CrossRef]
11. Apparao, M.; Sambana, B.; Srinivasa Rao, D. Secure routing in MANETS and IoT. *Sci. Technol. Dev.* **2019**, *VIII*, 325–333.
12. Swain, J.; Pattanayak, B.; Pati, B. A Systematic Study and Analysis of Security Issues in Mobile Ad-Hoc Networks. In *Research Anthology on Securing Mobile Technologies and Applications*; Information Resources Management Association, Ed.; IGI Global: Hershey, PA, USA, 2022; pp. 144–150. [CrossRef]
13. Simpson, S.; Nagarajan, G. Security Challenges and Attacks in MANET-IoT Systems. In *Enterprise Digital Transformation*; Auerbach Publications: New York, NY, USA, 2022; pp. 159–201.
14. Sha, K.; Yang, T.; Wei, W.; Davari, S. A survey of edge computing-based designs for IoT security. *Digit. Commun. Netw.* **2020**, *6*, 195–202. [CrossRef]
15. Chanal, P.; Kakkasageri, M. Security and privacy in IoT: A survey. *Wirel. Pers. Commun.* **2020**, *115*, 1667–1693. [CrossRef]
16. Mrabet, H.; Belguith, S.; Alhomoud, A.; Jemai, A. A survey of IoT security based on a layered architecture of sensing and data analysis. *Sensors* **2020**, *20*, 3625. [CrossRef] [PubMed]
17. Anh, V.; Cuong, P.; Vinh, P. Context-aware mobility in Internet of Thing: A survey. *EAI Endorsed Trans. Context-Aware Syst. Appl.* **2019**, *6*, 158875. [CrossRef]
18. Rana, M.; Mamun, Q.; Islam, R. Lightweight cryptography in IoT networks: A survey. *Future Gener. Comput. Syst.* **2022**, *129*, 77–89. [CrossRef]
19. Ahanger, T.; Aljumah, A.; Atiquzzaman, M. State-of-the-art survey of artificial intelligent techniques for IoT security. *Comput. Netw.* **2022**, *206*, 108771. [CrossRef]
20. Thanh, C. A Survey of Machine Learning Techniques for IoT Security. In *International Conference on Future Data and Security Engineering, Proceedings of the 8th International Conference, FDSE 2021, Virtual Event, 24–26 November 2021*; Springer: Singapore, 2021; pp. 139–157. [CrossRef]
21. Sadek, F.; Belkadi, K.; Abouaissa, A.; Lorenz, P. Identifying misbehaving greedy nodes in IoT networks. *Sensors* **2021**, *21*, 5127. [CrossRef]
22. Banerjee, B.; Neogy, S. A Brief Overview of Security Attacks and Protocols In MANET. In Proceedings of the 2021 IEEE 18th India Council International Conference (INDICON), Guwahati, India, 19–21 December 2021; pp. 1–6. [CrossRef]
23. Khan, U.; Agrawal, S.; Silakari, S. A Detailed Survey on Misbehavior Node Detection Techniques in Vehicular Ad Hoc Networks. In *Information Systems Design and Intelligent Applications. Advances in Intelligent Systems and Computing*; Mandal, J., Satapathy, S., Kumar Sanyal, M., Sarkar, P., Mukhopadhyay, A., Eds.; Springer: New Delhi, India, 2015. [CrossRef]
24. Khoda Parast, F.; Sindhav, C.; Nikam, S.; Izadi Yekta, H.; Kent, K.; Hakak, S. Cloud Computing Security: A Survey of Service-Based Models. *Comput. Secur.* **2022**, *114*, 102580. [CrossRef]
25. Williams, P.; Dutta, I.; Daoud, H.; Bayoumi, M. A Survey on Security in Internet of Things with A Focus on The Impact of Emerging Technologies. *Internet Things* **2022**, *19*, 100564. [CrossRef]
26. Maschler, M.; Zamir, S.; Solan, E. *Game Theory*; Cambridge University Press: New York, NY, USA, 2020.
27. Lin, D.; Wang, Q.; Yang, P. The Game Theory: Applications in The Wireless Networks. In *Game Theory—Applications in Logistics and Economy*; Tuljak-Suban, D., Ed.; IntechOpen: London, UK, 2018. [CrossRef]
28. Paul, C.; Bhanu, D.; Dhanapal, R.; Jebakumar Immanuel, D. An Efficient Authentication Using Monitoring Scheme for Node Misbehaviour Detection In MANET. In *International Conference on Computing, Communication, Electrical and Biomedical Systems*; Springer: Cham, Switzerland, 2022; pp. 627–633. [CrossRef]
29. Behfarnia, A.; Eslami, A. Misbehavior Detection in Ephemeral Networks: A Local Voting Game in Presence of Uncertainty. *IEEE Access* **2019**, *7*, 184629–184642. [CrossRef]
30. Abhishek, N.; Tandon, A.; Lim, T.; Sikdar, B. A GLRT-Based Mechanism for Detecting Relay Misbehavior in Clustered IoT Networks. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 435–446. [CrossRef]
31. Sharma, P.; Liu, H. A Machine-Learning-Based Data-Centric Misbehavior Detection Model for Internet of Vehicles. *IEEE Internet Things J.* **2021**, *8*, 4991–4999. [CrossRef]
32. Astillo, P.; Kim, J.; Sharma, V.; You, I. SGF-MD: Behavior Rule Specification-Based Distributed Misbehavior Detection of Embedded IoT Devices in A Closed-Loop Smart Greenhouse Farming System. *IEEE Access* **2020**, *8*, 196235–196252. [CrossRef]
33. Zhang, X.; Lyu, C.; Shi, Z.; Li, D.; Xiong, N.; Chi, C. Reliable multiservice delivery in fog-enabled VANETs: Integrated misbehavior detection and tolerance. *IEEE Access* **2019**, *7*, 95762–95778. [CrossRef]
34. Nguyen, V.; Lin, P.; Hwang, R. Enhancing misbehavior detection in 5G vehicle-to-vehicle communications. *IEEE Trans. Veh. Technol.* **2020**, *69*, 9417–9430. [CrossRef]
35. Gyawali, S.; Qian, Y.; Hu, R. Machine learning and reputation based misbehavior detection in vehicular communication networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 8871–8885. [CrossRef]
36. Ding, X.; Wang, Y. Misbehavior detection and optimal threshold analysis in DF cooperative relay networks. *IEEE Wirel. Commun. Lett.* **2021**, *10*, 2718–2721. [CrossRef]
37. Shah, H.; Kakkad, V.; Patel, R.; Doshi, N. A survey on game theoretic approaches for privacy preservation in data mining and network security. *Procedia Comput. Sci.* **2019**, *155*, 686–691. [CrossRef]
38. Jing, J. Applications of game theory and advanced machine learning methods for adaptive cyberdefense strategies in the digital music industry. *Comput. Intell. Neurosci.* **2022**, *2022*, 2266171. [CrossRef]

39. Kiennert, C.; Ismail, Z.; Debar, H.; Leneutre, J. A survey on game-theoretic approaches for intrusion detection and response optimization. *ACM Comput. Surv.* **2019**, *51*, 1–31. [CrossRef]
40. Kumar, R.; Singh, S.; Kela, R. Analyzing advanced persistent threats using game theory: A critical literature review. In *International Conference on Critical Infrastructure Protection*; Springer: Cham, Switzerland, 2021; pp. 45–69. [CrossRef]
41. Jan, S.; Amin, N.; Shuja, J.; Abbas, A.; Maray, M.; Ali, M. SELWAK: A secure and efficient lightweight and anonymous authentication and key establishment scheme for IoT based vehicular ad hoc networks. *Sensors* **2022**, *22*, 4019. [CrossRef]
42. Subba, B.; Biswas, S.; Karmakar, S. A game theory based multi layered intrusion detection framework for VANET. *Future Gener. Comput. Syst.* **2018**, *82*, 12–28. [CrossRef]
43. Sun, Z.; Liu, Y.; Wang, J.; Mei, F.; Deng, W.; Ge, Y. Non-Cooperative game of throughput and hash length for adaptive Merkle tree in mobile wireless networks. *IEEE Trans. Veh. Technol.* **2019**, *68*, 4625–4650. [CrossRef]
44. Liu, X.; Lim, T.; Huang, J. Optimal Byzantine attacker identification based on game theory in network coding enabled wireless ad hoc networks. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 2570–2583. [CrossRef]
45. Li, Y.; Bai, S.; Gao, Z. A multi-domain anti-jamming strategy using Stackelberg game in wireless relay networks. *IEEE Access* **2020**, *8*, 173609–173617. [CrossRef]
46. Qi, N.; Wang, W.; Zhou, F.; Jia, L.; Wu, Q.; Jin, S.; Xiao, M. Two birds with one stone: Simultaneous jamming and eavesdropping with the Bayesian-Stackelberg game. *IEEE Trans. Commun.* **2021**, *69*, 8013–8027. [CrossRef]
47. Qi, N.; Wang, W.; Xiao, M.; Jia, L.; Jin, S.; Zhu, Q.; Tsiftsis, T. A Learning-based spectrum access Stackelberg game: Friendly jammer-assisted communication confrontation. *IEEE Trans. Veh. Technol.* **2021**, *70*, 700–713. [CrossRef]
48. Ilavendhan, A.; Saruladha, K. Stackelberg security game to mitigate the DoS attack in vehicular ad-hoc networks. *J. Ambient. Intell. Humaniz. Comput.* **2021**, *12*, 1–8. [CrossRef]
49. Ilavendhan, A.; Saruladha, K. Comparative study of game theoretic approaches to mitigate network layer attacks in VANETs. *ICT Express* **2018**, *4*, 46–50. [CrossRef]
50. Abdalzaher, M.; Samy, L.; Muta, O. Non-zero-sum game-based trust model to enhance wireless sensor networks security for IoT applications. *IET Wirel. Sens. Syst.* **2019**, *9*, 218–226. [CrossRef]
51. Feng, S.; Xiong, Z.; Niyato, D.; Wang, P. Dynamic resource management to defend against advanced persistent threats in fog computing: A game theoretic approach. *IEEE Trans. Cloud Comput.* **2021**, *9*, 995–1007. [CrossRef]
52. Wang, D.; Chen, I.; Al-Hamadi, H. Reliability of autonomous Internet of Things systems with intrusion detection attack-defense game design. *IEEE Trans. Reliab.* **2021**, *70*, 188–199. [CrossRef]
53. Mehta, M.; Patel, K. A survey on IoT authentication security service. *Int. J. Syst. Softw. Secur. Prot.* **2022**, *13*, 13. [CrossRef]
54. Chi, C.; Wang, Y.; Tong, X.; Siddula, M.; Cai, Z. Game theory in internet of things: A survey. *IEEE Internet Things J.* **2022**, *9*, 12125–12146. [CrossRef]
55. Khan, B.; Olanrewaju, R.; Hadi Habaebi, M. Malicious behaviour of node and its significant security techniques in MANET-A review. *Aust. J. Basic Appl. Sci.* **2013**, *7*, 286–293.
56. Khan, B.; Anwar, F.; Olanrewaju, R.; Pampori, B.; Mir, R. A game theory-based strategic approach to ensure reliable data transmission with optimized network operations in futuristic mobile adhoc networks. *IEEE Access* **2020**, *8*, 124097–124109. [CrossRef]
57. Khan, B.; Anwar, F.; Olanrewaju, R.; Kiah, M.; Mir, R. Game theory analysis and modeling of sophisticated multi-collusion attack in MANETs. *IEEE Access* **2021**, *9*, 61778–61792. [CrossRef]
58. Khan, B.; Olanrewaju, R.; Mir, R.; Baba, A.; Adebayo, B. Strategic profiling for behaviour visualization of malicious node in MANETs using game theory. *J. Theor. Appl. Inf. Technol.* **2015**, *77*, 25–43.
59. Dafalla, M.E.M.; Mokhtar, R.; Saeed, R.; Alhumyani, H.; Abdel-Khalek, S.; Khayyat, M. An optimized link state routing protocol for real-time application over vehicular ad-hoc network. *Alex. Eng. J.* **2022**, *61*, 4541–4556. [CrossRef]
60. Du, X.; Zhou, Z.; Zhang, Y. Energy-efficient data aggregation through the collaboration of cloud and edge computing in Internet of Thing's networks. *Procedia Comput. Sci.* **2020**, *174*, 269–275. [CrossRef]