IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 9, 2020, accepted May 21, 2020, date of publication May 26, 2020, date of current version June 5, 2020.

*Digital Object Identifier 10.1109/ACCESS.2020.2997711*

# A Novel Multi-Agent and Multilayered Game Formulation for Intrusion Detection in Internet of Things (IoT)

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

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

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

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

**ABSTRACT** The current era of smart computing and enabling technologies encompasses the Internet of Things (IoT) as a network of connected, intelligent objects where objects range from sensors to smartphones and wearables. Here, nodes or objects cooperate during communication scenarios to accomplish effective throughput performance. Despite the deployment of large-scale infrastructure-based communications with faster access technologies, IoT communication layers can still be affected with security vulnerabilities if nodes/objects do not cooperate and intend to take advantage of other nodes for fulfilling their malevolent interest. Therefore, it is essential to formulate an intrusion detection/prevention system that can effectively identify the malicious node and restrict it from further communication activities—thus, the throughput, and energy performance can be maximized to a significant extent. This study introduces a combined multi-agent and multilayered game formulation where it incorporates a trust model to assess each node/object, which is participating in IoT communications from a security perspective. The experimental test scenarios are numerically evaluated, where it is observed that the proposed approach attains significantly improves intrusion detection accuracy, delay, and throughput performance as compared to the existing baseline approaches.

**INDEX TERMS** Internet of Things, intrusion detection, multi-layer games, security measures.

## I. INTRODUCTION

The idea of the Internet of Things (IoT) had been envisioned in the last decade, where it was introduced as a global backbone to escalate the services of future generation wireless communications technologies such as 5G. It is considered as a promising area of research due to its potential capability to establish smarter and intelligent communication between multilayered physical and virtual nodes via cutting edge technologies [1], [2]. The conception of IoT enables things as nodes that are capable of sensing, processing, storing, and transmitting the data through the various layers of network components in a cooperative mode of communication. And the underlying definition of IoT also evolved with the convergence of multiple technologies and heterogeneous communication protocols which results in the formation of a de-facto network of all the smart and intelligence pervasive and ubiquitous applications. The eco-system contains IoT nodes in various sub-networks like WSN, MANET or VANET, etc. which gets connected to the gateways which push the data to the access point and further to the upper layers of edge server and finally to the cloud [3]–[6]. The prime purpose here lies in improvising the quality of lives through various applications, including smart transportation, smart city, smart industrial controls, and many others. Due to the future generation cellular network, the connectivity among IoT smart objects/devices is expected to be increased to a significant extent where the frequency band of millimeter-wave, mid-bands, and low-bands increases the data transfer rate through multi-hop communications [7], [8].

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

In the multi-hop communication paradigm, nodes cooperate to accomplish specific communication tasks. However, if nodes do not cooperate in communication and intend to use other nodes resources for passively gaining importance factor, then such nodes are often termed as 'Selfish nodes' [9]. These nodes do not impose malevolent intention to disrupt the communication process but act selfishly and only transmit their data-packets due to limited energy concern. In the long run, it affects the throughput, which is a crucial measure to ensure the overall network performance [10]. On the other hand, an IoT object/node can be malicious, which mostly intends to damage the facilities of the network with adversarial effects. If the probability of the presence of these types of node increases within an IoT network, then it negatively influences the network throughput, end-to-end delay, and energy consumption performance. The increasing complexity of IoT networks also magnifies various security vulnerabilities, and the presence of any types of malicious behavior of nodes can be identified through intrusion detection systems. Through such systems, the disruption of the network operations can be avoided to a significant extent [11], [12].

This paper explores various potential loop-holes in traditional approaches of intrusion detection. It introduces a robust multi-agent and multi-layer game-based approach to identify both the selfish ($S_{node}$) and malicious nodes ($M_{node}$) and minimizes the possibilities of attacks in IoT communication layers. The security model is constructed based on the combined paradigm of reputation-based strategy [13] and game theory modeling [14]. The prime reason behind adopting these strategies is that various research approaches in the IoT security domain directed their research approach with these strategies. Thus, considering the potential features of these approaches, the proposed strategic security modeling is formulated. The effectiveness of the proposed study is also assessed with a numerical analysis with strong hypothetical assumptions where throughput and end-to-end delay performance are tested along with intrusion detection accuracy. The numerical validation further exhibited the efficiency of the proposed approach.

The rest of the paper is organized as follows: Section II describes and outlines the most significant related works and also outlines the scope of those approaches in this current research study. Section III further illustrates the limitations of the existing approaches, and the consecutive section IV helps to formulate the proposed methodology. Section V illustrates the mathematical formulation of the multi-agent game with the combined approach followed by the result and discussion and performance validation i.e., an extensive comparative assessment in section VI. Finally, Section VII presents the contributory remarks of the formulated system.

## II. RELATED WORK

This section discusses the conventional literature, which talks about security in IoT, and also proposes different mechanisms to deal with it. The conventional research approaches in intrusion detection of IoT inclines towards identifying the non-cooperative nodes, such as selfish nodes and malicious nodes. However, the study of authors in [1] introduced a multilayered security modeling to strengthen the transmission of data packets between constituent IoT objects ($IoT_{obj}$) and another cellular-connected host object. The approach applies a set of inter-locking mechanism in a vital role to provide high-end and reliable, secure connectivity solution.

In [15], authors also directed their research work to represent IoT as a convergence of diverse technology, which has unprecedented business opportunities by means of improving the quality of lifestyle of humans. The study discusses the background of IoT security challenges and also discusses why it is a crucial requirement to reshape the future generation communication paradigm. The exploration of research approaches also shows that many research studies are concerned about cooperative and non-cooperative node identification using intrusion detection systems with the most cited approaches being: i) Reputation-based approaches, ii) Credit-based approaches, iii) Acknowledgment-based policies and most importantly, iv) Game theory-based policies.

The authors in [16] introduced a reputation-based security mechanism, where $IoT_{obj}$ having more reputation factors gain the attention of the system and considered as more cooperative nodes. Similarly, another approach by the authors in [17] also employs watch-dog reputation managers to maintain the accountability of cooperative and non-cooperative nodes in MANET which can be referred to as a subset of dynamic IoT. There exist other trust models that are referred by the authors in [18], [19], where the mathematical approach to isolate the non-cooperative nodes in dynamic clusters are introduced based on the reputation factor.

IoT has a wide range of application areas, where one of the key application areas include smart-healthcare systems. The IoT healthcare sensor devices generate vital information related to a patient's health condition; thereby, the essentiality of the suitability of IoT architecture is also concerned with identifying the security vulnerabilities. Another study [20] also presented a security model that includes customizable analysis language to improvise the IoT security to a significant extent.

The authors in [21] also introduced a credit-based security policy to identify the selfish $IoT_{obj}$ here; the underlying design principle shows that nodes trade data packets among themselves through cooperative communication. After buying the data packet, it sells that packet at a higher selling price. The presented approach combines a packet formulation model and its trading approach. Similar work has been found in the studies of [22], [23], where credit-based intrusion detection modeling formulation is mostly considered.

However, as compared to the approaches discussed above, the acknowledgment-based methodologies [24]–[26] are mostly referred to ensure a higher degree of reliability in packet transmission and malicious node authentication.

The most popular approach which is claimed to be suitable for securing IoT communication is - applied game theory-based modeling. The study of authors in [14] introduces the core principle of game formulation and also derives its adaptability into future generation dynamic ad-hoc networks such as IoT. The non-cooperative game theory is mathematically derived and evaluated in the study. Their research approach is further extended by the authors in [27] and [28], where the reliable packer transmission is mostly assessed through dynamic pricing-based game theory modeling.

A controlled identical mechanism of game and also another game theory modeling to detect and isolate malicious nodes are evaluated by the studies of [29] and [30], respectively. Both the studies concluded their research scope into futuristic dynamic IoT networks. The consecutive section further illustrates the problem findings to outline the research gap in this study.

## III. PROBLEM FINDINGS

### A. ABOUT TRUST-BASED SYSTEM

It is mostly observed by assessing the related works that despite having strength factors, most of the trust and reputation-based policies are computationally expensive and result in comparatively lower throughput and higher energy consumption. It can also be seen that these approaches do not impose a penalty on the nodes, which negatively influences the network activities and also do not encourage them with incentives. If incentives are given along with second chances, then $S_{node}$ and $M_{node}$ can cooperate with other nodes in communication and also, in the long run, assist in enhancing the network activities. In many cases, during the network operations, $S_{node}$ and $M_{node}$ can actively conspire with each other to gain other node resources unlawfully.

### B. ABOUT CREDIT-BASED SYSTEM

Another approach of intrusion detection is found in a credit-based approach where nodes pay a cost amount to the system to transmit its data packet. More likely, nodes also can trade their data packet and sell it for its profit. This approach is also not that efficient as it gets affected by a collision attack and also does not encourage the profitability of the security systems with punishment and incentive-based approach. Another weakness of this approach is that it does not ensure higher detection accuracy performance.

### C. ABOUT ACKNOWLEDGEMENT-BASED SYSTEM

The design principles of acknowledgment-based approaches also lack efficiency as it does not guarantee higher throughput performance and also cannot resist the network from a collision attack between selfish and malicious nodes. Another important aspect is that this approach is mostly found to generate communication overhead.

### D. ABOUT GAME THEORY MODELING-BASED SYSTEM

The underlying mathematical approach of game theory modeling also attained much attention from the researchers. It models the system based on applied mathematical theory; all node activities are analyzed and based on a collaborative assessment; the best possible solution is obtained. To date, game theory-based approaches are found most suitable to identify the malicious nodes and selfish nodes with a significantly lesser false positive rate. However, still, the research effort is active to improvise the system with time-cost efficient incentive mechanisms. If the performance scenario is concerned, then delay and throughput of the traditional approaches are still not satisfactory. The next section further discusses the formulated system, which is modeled to overcome the design limitations of the traditional intrusion detection approaches.

## IV. PROPOSED SYSTEM

The system incorporates a multi-agent game based modeling which takes the advantages of reputation-based mechanism and game theory modeling to identify the $S_{node}$ and $M_{node}$ in IoT effectively. The key design principle of this mechanism is analytically formulated with five different prime phases, viz. i) node/object ($IoT_{obj}$) initialization and deployment phase, ii) cluster formulation, iii) transmission of data packets with multi-agent and multilayered game modeling followed by iv) Updating the system database and v) Identification of $S_{node}$ and $M_{node}$ intrusion respectively. The joint-formulation of the reputation and game-based system is also assessed with a system representation where the possibility factor of node $i\epsilon IoT_{obj}$ for forwarding the message ($msg$) is calculated and also the possibility factor of node $i\epsilon IoT_{obj}$ for dropping the $msg$ is also calculated.

### A. NODE/OBJECT ($IoT_{obj}$) INITIALIZATION AND DEPLOYMENT PHASE

This phase of the research study deploys a set of $IoT_{obj} = \{I_1, I_2, I_3, \ldots .I_i\}$. Here, $i\epsilon Z^+$ and perform clustering to initialize and set-up the network parameters prior to triggering the networking events.

### B. CLUSTER FORMATION PHASE

In one particular cluster ($C_i$) of $n$ number of nodes, there will be a gateway node acting as a group header ($C_h$). These $IoT_{obj}$ collaboratively, and intelligently communicate with each other to accomplish a specific task. The $msg$ format in the cluster heads consist of 4-tuple attributes such as <node(id), hop(count), node(msg), status >. Here node(id) has to be 16-bit representation and hop(count) to $C_h$ should be of 8-bit representation.

### C. TRANSMISSION OF DATA PACKETS WITH MULTI-AGENT AND MULTILAYERED GAME MODELING

From the distributed computing viewpoint, the approach of multi-agent game algorithm runs in each $IoT_{obj}$, and depending upon the condition of execution, nodes are selected for route establishment and communication. During the communication scenario, nodes/$IoT_{obj}$ cooperate to transmit their own or other $IoT_{obj}$ data packet to $C_h$. For this purpose, each node belonging to $C_i$ runs their multi-agent game algorithm and calculates the reputation and trust factor of the nodes which are participating in routing activities in every subsequent round of communication. The other stage of execution involves updating of the system database.

### D. UPDATING THE SYSTEM DATABASE

During the communication activities when each node is assigned with a reputation factor, then a corresponding value is assigned to each node updated to the network system database. Simultaneously, other $IoT_{obj}$ within that particular $C_i$ also update their database structure with the reputation values corresponding to other nodes.

### E. IDENTIFICATION OF THE $S_{node}$ AND $M_{node}$

The system defines a cut-off value of reputation ($\mu$) in the initial stage of communication; and further it checks if node reputation is found lesser than $\mu$, the system identifies the $IoT_{obj}$ as $S_{node}$ and $M_{node}$ and also restricts their participation in further communication activities in IoT.

## V. MULTI-AGENT GAME FORMULATION

This study mostly focuses on designing a security approach that can be robust enough to deal with different types of $S_{node}$ and $M_{node}$ nodes. For this purpose, it is essential to effectively identify them without compromising much time so that the throughput and delay performance of the IoT network can be enhanced.

### A. ADOPTION OF REPUTATION AND TRUST-BASED APPROACH

There are various research studies that are directed to design and develop a reputation-based policy to assess different node activities in IoT. Here, based on the node trust factor, the system assigns reputation value ($rV$) to each node. Every node within the network assesses the trust factor. The nodes having more trust values and reputation are referred to as reliable nodes; on the other hand, nodes with lower trust factor and reputation values are referred to as $S_{node}$.

### B. SET OF STRONG ASSUMPTIONS TAKEN DURING SYSTEM MODELING

This study enforced a set of assumptions during the formulation of the mathematical modeling that corresponds to the security approach. Those are listed as follows:

- First of all, each $IoT_{obj}$ is aware of its adjacent neighbor nodes which come under its vicinity and also belong to the same $C_i$.
- Each $IoT_{obj}$ does not have any idea of whether its adjacent neighbors are $S_{node}$ or $M_{node}$.
- To formulate the best possible route, each node calculates its maximum available information about the other nodes and also computes the behavioral aspects of other nodes along with their expectation factor and intelligently computes the optimal strategy for route establishment.
- It is also assumed that nodes should cooperate in order as each $IoT_{obj}$ is mostly sensor-driven and operates with batteries and also having limited transmission frequency ($T_f$). During each round of communication activities, each node computes the information about its adjacent neighbors where it tries to objectify whether the trust factor of its adjacent neighbors is higher or not; that means whether that node is cooperating in most of the communication activities or the probability of dropping a packet is more for that particular $IoT_{obj}$.
- The prime intention of a genuine $IoT_{obj}$ is to gain maximum possible pay-off so that it can get many rewards in terms of communication resources. For this purpose, the node intends to help in forwarding the data packets and also interacts with other $IoT_{obj}$ in order to send its data packet with the successful transmission.

### C. GAME FORMULATION

In the context of formulating multi-agent game development, the game (g) is formulated as $g : g \to IoT_{obj} \bigcup A^j \bigcup u^j$ where $A$ refers to the set of actions associated with each $IoT_{obj}$ and $u$ corresponds to the functionality which is derived from the outcome of individual players in one round. Here, $j$ refers to the number of rounds, and $A^j$ is the set of node actions within the round $j$ for $i \to IoT_{obj}$ node. $A^j$ is defined in a way where for each node $i$, it corresponds to either 0 or $Pow_u(i)$. Here, $Pow_u(i)$ indicates the maximum power which is utilized by node $i$ to transmit the data packet. The set of actions is formulated for different games in each round of communication activities among $IoT_{obj}$. This study also assesses the node $p$ with respect to two different aspects during the game, whether it accepts the request and forwards the data with cooperation ($f_c$), or it declines the data reception of the data packet and also does not cooperate in the routing ($r_c$). The node $p$ can be a function of these two attributes such as $p \to f_c | r_c$. Each $IoT_{obj}$ should employ any of these strategies during route establishment and communication in each round of $j$. By means of these strategies, each player ($IoT_{obj}$) attains a value of profit, which is computed with the set of $u^j$. Here the $u^j$ for node $i$ is computed with the following eq. (1)

$$u^j\,(i) = c \times \sum [\left(nC_h\,(i)\,, nf_c\,(p \to i)^j\right] - b.n(i)^j \ldots . \quad (1)$$

In (1), $u^j\,(i)$ is computed where $c$ is a constant and $nC_h\,(i)$ refers to the number of $msg$ that has been received by node $i$ from $C_h$ of $C_i$. Also, $nf_c\,(p \to i)^j$ refers to the number of forwarded packets by $i$ for $p$ which also resides in $C_i$ for the specific communication round $j$. $n(i)^j$ also refers as $i$ nodes $msg$, which is sent to the destination during round $j$. Fig. 1 shows an overview of the mix-mode multi-agent game security modeling.

The system formulation refers to the mix-mode strategy of multi-agent game formulation based on both the i) reputation-based modeling and ii) game theory. If a node $p$ wants to transmit $msg$ to destination node $i$ and according to route establishment scenario as $(p \to i)^j$, the $msg$ gets

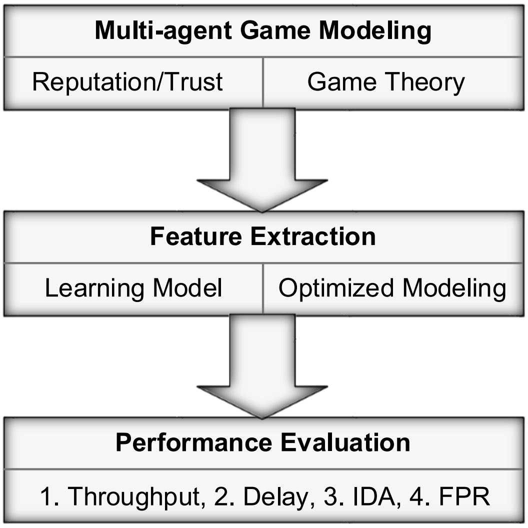

**FIGURE 1.** System design overview of the multi-agent game modeling.

transmitted to the recipient node $i$. Here comes a probabilistic scenario where it is uncertain whether $i$ will further forward the data packet or drop it. One important point to be noted here is that the destination node also can be a 1-hop neighbor or intermediate node when multi-hop communication is concerned. Therefore, the proposed system also computes the expectation values for $\exp(f_c)$ and also for $\exp(r_c)$ to ensure whether the intermediate node intends to send the data packets, or it intends to drop the msg by not cooperating in communication. Here, the strategy $s \rightarrow f_c | r_c$. According to the formulated theory, the intermediate node can take any actions $A^j$ with any strategy $s$ with a probability factor $\rho(s)$. In the context of the formulated approach, assessing cooperative and non-cooperative metric for each individual node is important. The multi-agent game modeling is designed from the perspective of making the $S_{node}$ cooperative in the communication requirement basis. After setting up the nodes in IoT scenario, the nodes are further clustered and here each node tries to find its reliable adjacent neighbor nodes. For this purpose, it broadcasts control message ($msg$). This study also incorporates IoT gateways to collect data from $C_h$. The system is also designed in a way where member nodes can transmit $msg$ to the $C_h$ through multi-hop communication. This study incorporates the multi-agent multilayered game for each active node. And through the game, nodes determine which is the best possible solution for forwarding their own respective $msg$ or forwarding other node data. While the system executes the game, each node will choose its adjacent neighbor as an intermediate node to forward the data to the destination. With the adjacent neighbor, the node will play the game and here it will learn the status from the neighbor node and update itself. This phase also includes selection of appropriate features from the neighbor nodes. If a node is found to be cooperating in the communication, then the system provides a higher trust factor with optimized probability to the node. In case of malicious node or selfish node, a cooperation procedure is evaluated to understand their intention in the game whether that node intentionally delays the routing, or it directly drops the data packet. Then the system assigns a lesser reputation factor to that particular node if appropriately identified. This way each node, through the cooperative game, understands and assess other nodes and update their reputation matrix $r[]$. For this purpose, the learning model is evaluated to understand the pattern of activities by each node about other nodes within the IoT network model. Through multilayered game, information regarding nodes is updated in every stage for the purpose of detecting the possibility of increasing non-cooperative nodes. The system here also incorporates penalty and reward factors. If intrusion takes place within the network through a particular $S_{node}$ or $M_{node}$ for $j$ round of communication, then the system imposes a penalty on them and minimizes the possibility of packet forwarding through that node, and nodes are restricted from transferring their data packets as well. On the other hand, if the non-cooperative $S_{node}$ or $M_{node}$ is identified through the learning model accurately, the system stimulates them to cooperate in authorized route establishment and packet forwarding as a penalty factor.

The system is also formulated in a way where it encourages $S_{node}$ to cooperate with other nodes during the communication scenario. The key idea of the game-theoretical approach is that each node closely monitors the activities of other nodes and also evaluates whether a node is forwarding the respective $msg$ of other nodes or it drops the packet within a specified time-slot ($T_{slot}$). The combined approach of game theory and reputation is applied here in a way where it clearly states that if a node is found not cooperating much in $msg$ forwarding and mostly deviates from the communication activities, then it means their reputation factor will go down. The respective $C_h$ collects all the information about its respective member nodes. For this purpose, it checks the reputation factor from the database of each member nodes. If the reputation factor is found below a threshold, then the system reports to $C_h$ about their intention and activities that means whether the nodes are $S_{node}$ or $M_{node}$. Here in this scenario, the $C_h$ will broadcast about the $S_{node}$ status to other member nodes so that they can make use of the selfish node during the routine activities. This is the way a non-cooperative node can be engaged in communication where it assists in packet forwarding to gain a higher reputation and reward. The following algorithm shows the execution steps of the formulated approach. The notation of important parameters that have been considered in the proposed algorithm formulation are highlighted in Table 1.

The algorithm is analytically designed and modeled in a way where the first stage includes the deployment of IoT objects within a network that can be patterned or random. Here, each IoT object is assigned with a unique RFID tag and assumed to get connected with the cloud without having a dependency on the internet protocols. This is the way the system also minimizes the possibility of energy consumption during the overall network operations. During the network set-up and connectivity and coverage estimation, each $IoT_{obj}$ broadcasts a control message to confirm their

**TABLE 1.** Notation table for proposed algorithm.

| Notation (Symbolic) | Description |
|---|---|
| $S_{node}$ | Selfish node |
| $M_{node}$ | Malicious node |
| $T_{slot}$ | Discrete Timeslot |
| $T_f$ | Transmission frequency |
| $IoT_{obj}$ | IoT objects |
| $'msg'$ | Control message |
| $C_h$ | Cluster head |
| $ACK$ | Acknowledge message |
| $C_i$ | $i^{th}$ –cluster |
| $f_c$ | Node's action of forward (Cooperating) |
| $r_c$ | Node's action of reject (Declining) |
| $u^j$ | Profit value attained by each IoT object |
| $S$ | Node strategy attained during communication scenario |
| $prob$ | Estimation of the willingness of node to participate in communication |

**Algorithm 1** Multi-Agent Game Assisted Intrusion Detection System Design for IoT

```
1. Begin
2. Input: $IoT_{obj} = \{I_1, I_2, I_3, \ldots .I_i\}, S_{node}, M_{node}$
3. Output: Report $\rightarrow C_h$ (status)
4. Node/object ($IoT_{obj}$) initialization and deployment phase
    a. <node(id), hop(count), node(msg), status >
    b. $IoT_{obj}$ (status): n bits array
    c. Exchange of 'control' msg
5. Perform clustering:
    a. Select $C_h$ and perform dynamic clustering
    b. for all $C_i$
        i. Enable multi-layered game
        ii. Perform connectivity
        iii. $IoT_{obj}$ (RFID) $\rightarrow C_h$
end
6. Execute multi-layered game during msg transmission
    a. for each $C_i$
        i. define $IoT_{obj}$ (source) and $IoT_{obj}$ (destination)
        ii. player(game): maximize(profit) $\uparrow$
        iii. player(game): minimize(losing profit) $\downarrow$
        iv. Initiate (Ack): $IoT_{obj}$(status)
        v. Compute: outcome(game)
        vi. Compute number of unsuccessful data reception and forwarding
        vii. Update reputation table (Evaluating stage)
end
    b. end of dynamic clustering
7. Effective feature selection <$IoT_{obj}$ (status), reputation, pay-off > and build (Learning-model)
    a. Alert: each member with $IoT_{obj}$(status) within specific clock-period
8. Update learning model and detect $< S_{node}, M_{node} >$
9. End
```

adjacent neighbors and also maintains its database with the information corresponding to the status of each neighbor. The clustering algorithm is designed to adopt the principle of the hierarchical dynamic clustering principle, which is found quite suitable for the dynamic IoT. After performing the clustering, each node transmits their respective *msg* bits, and also forwards the data packets between sources to destination considering the multi-agent game. The networking scenario is designed and formulated in a way that the possibility of communication among $IoT_{obj}$ tends to increase. The transmission of *msg* is considered between source and destination and also between the forwarding participants, which cooperate in communication. Each of the players take their individual decision during the multi-agent game and attempt to maximize their profit in terms of reputation and resources, subject to their probability of cooperating in communication activities as high as possible.

And similarly, each node will have the intention not to lose the profit or reputation. This approach applies to different use-cases of IoT. The multi-agent game is mainly multilayered; so, understanding the activities of each node within the IoT takes a progressive amount of time. Here the control packets basically consist of '*HELLO*' and '*ACK*' which are meant for establishing the communication in the initial round of execution work-flow model.

Here, the game is considered dynamic - the reason behind this is in the initial phase of the game; one player might cooperate in the first place, and other players can choose their actions depending upon the actions being taken by the first player. As in the initial stage, no node will have information about the $S_{node}$ or $M_{node}$, thus the game initially gets activated with incomplete information and with learning and cooperative way of communication corresponds to the updating of reputation factor and node status. One plays the game, and with the outcome of the game, the proper evaluation takes place which progressively updates the reputation table. This study designs a learning scenario that is modeled based on the individual node's experiences about other nodes, and the activity information, which includes the probabilistic factors corresponding to the successful and unsuccessful transmission and packet forwarding status. The game is also modeled in a way where depending upon the actions of the opponent node, the pay-off matrix is calculated, which assists another node in optimizing its action with the best possible strategy. The incorporation of established Nash Equilibrium theory assists in making each node to take the best possible actions against its opponent nodes. This game theoretic approach considers an infinite game which is repeated, and decisional analysis considers past behavioral aspects of each node for the assessment during the progressive intrusion detection modeling.

This way, the system identifies whether $S_{node}$, $M_{node}$ nodes are present in the network. If found, then the $C_h$ gets an alert *msg* about suspicious intrusion by that particular thing or object and makes that suspicious object cooperating in the communication activities. The proposed system utilizes the established theoretical principle of Nash Equilibrium modeling, the probability distribution of nodes are computed where it also assists in formulating the expectation metrics which indicates the possibility and willingness of a node in forwarding the data packet or not forwarding the data packet [31], [32].

The computation of the expectation metric to indicate the possibility of willingness of a node in forwarding the data packet is shown as follows:

$$E\,(prob \rightarrow f_c\,|\,S) = \sum p\,(S_i) = f_c \times Vu^j(i)\ldots.. \quad (2)$$

And also, willingness of a node in not forwarding the data packet as follows:

$$E\,(prob \rightarrow r_c\,|\,S) = \sum p\,(S_i) = r_c \times u^j(i)\ldots... \quad (3)$$

Here, S indicates the strategy the node is going to attain during the communication scenario and prob is the estimation of the possibility of the willingness of the node to participate in communication. Further, this way, the study intends to optimize the communication performance with higher throughput and a very lesser end to end delay performance, which is exhibited in the subsequent section.

## VI. COMPARATIVE PERFORMANCE ANALYSIS

The game theory has a significant contribution in the past few years as a new technique on the security systems in MANET and mobile wireless sensor network (MWSN) due to its potential accuracy and computational efficiency during threat computing and analysis [33], [34]. However, as of now, there are few analytical models developed for studying security problems with a focus on including multiple types of defenders and offenders (collaborative, erroneous/selfish and malicious nodes) simultaneously [19], [28]. This study considered the most significant and related existing works such as (Zhang *et al.*, 2018) [19] and (Sun *et al.*, 2013) [28] for benchmarking. The duo has also equivalently worked on a similar line of research, i.e. not limiting the regular nodes to absolutely cooperate. Furthermore, they have been extensively cited by the recent Intrusion Detection and Prevention approaches. Thereby it is quite imperative and logical to justify the importance of the baselines from the comparative assessment and validation viewpoint.

For experimental outcome, which is obtained after simulating the formulated intrusion detection and prevention mechanism in a numerical computing tool. The system evaluation with the experimental approach considers 500-800 number of nodes where the number of $S_{node} = 25$ or $M_{node} = 5$. For a different combination of scenarios, a more or less similar trend of outcome is obtained, as shown below.

Table 2 shows that with the increasing number of $S_{node}$ from 5 to 25, the proposed formulated system attains better intrusion detection accuracy, which is found to attain a maximum 99% as compared to the baseline approaches of [28] and [19].

**TABLE 2.** Analysis of intrusion detection accuracy (ID-A) with S = 25.

| Number of $S_{node}$ | ID-A (ProP) | ID-A [28] | ID-A [19] |
|---|---|---|---|
| 5 | 0.94 | 0.89 | 0.98 |
| 10 | 0.97 | 0.75 | 0.87 |
| 15 | 0.99 | 0.77 | 0.85 |
| 20 | 0.98 | 0.69 | 0.74 |
| 25 | 0.95 | 0.65 | 0.65 |

Another test scenario evaluation is performed where the impact of the increasing number of $M_{node}$ is observed on ID-A, as shown in Fig. 2.

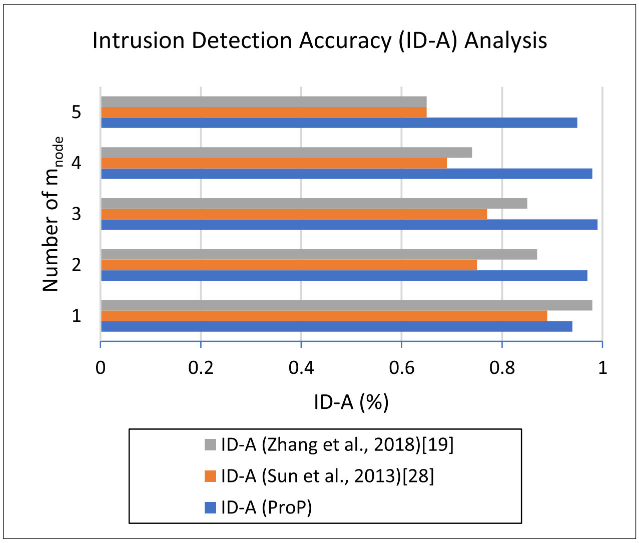

**FIGURE 2.** Analysis of IDA(%) for variable #$M_{node}$.

Here also, the interpretation shows that the ProP approach accomplishes better, and consistent performance as compared to the related baseline approaches.

Table 3 shows that in both the proposed and trust-based approach of [19], throughput outcome marginally differs, and the formulated approach attains superior throughput outcome where the maximum value is found 95 percent for 25 number of selfish nodes. The analysis also exhibited that as the formulated system also considers the notion of dynamic higher hierarchical clustering where $C_h$ gets selected dynamically and even as it evaluates suspicious intrusion level with

**TABLE 3.** Analysis of throughput with $S_{node}$ = 25.

| Number of $S_{node}$ | Throughput (ProP) | Throughput [28] | Throughput [19] |
|---|---|---|---|
| 5 | 87 | 56 | 86 |
| 10 | 81.4 | 50 | 85 |
| 15 | 88.92 | 42 | 78 |
| 20 | 89.34 | 41 | 81 |
| 25 | 95 | 36 | 84 |

the multi-agent game approach where the $S_{node}$ are bound to cooperate in message forwarding to gain reputation and $M_{node}$, will either forward the authorized data packet once it is trapped or it will leave the IoT zone, to save its resources. The outcome clearly shows that the throughput shows a significant increase despite the presence of $S_{node}$ and $M_{node}$, which means the occurrence of packet drops is significantly lesser as forwarding events are increased.

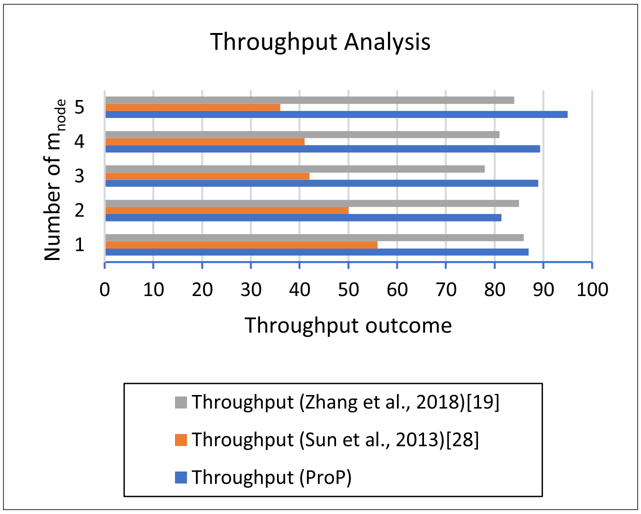

**FIGURE 3.** Analysis of throughput for variable $\#M_{node}$.

Fig. 3 also shows that despite the increasing number of $M_{node}$, the proposed system attains better throughput outcomes as compared to the baseline models.

From Table 4, it is observed that the proposed system also exhibits better delay performance, which is approximately 50% improvement over the delay performance of [28]. Out of all the approaches, the delay performance in [19] is found to be quite insignificant.

**TABLE 4.** Analysis of end-to-end delay with $S_{node}$ = 25.

| $\#S_{node}$ | Delay (ProP) | Delay [28] | Delay [19] |
|---|---|---|---|
| 5 | 17.34 | 42 | 80 |
| 10 | 16.54 | 50 | 85 |
| 15 | 20.3 | 42 | 78 |
| 20 | 21.4 | 41 | 81 |
| 25 | 22.7 | 36 | 84 |

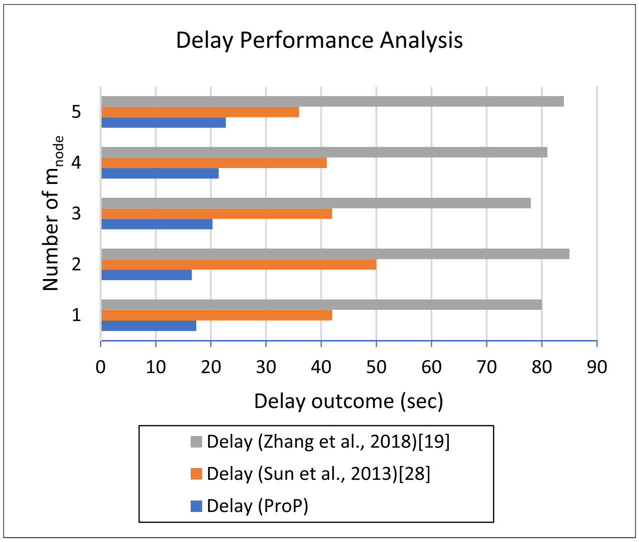

**FIGURE 4.** Analysis of delay for variable $\#M_{node}$.

Fig. 4 shows that with the increasing number of $M_{node}$, the proposed system delay performance does not get much affected if the number of $M_{node}$ and $S_{node}$ gets increased. And, the closer interpretation reveals the fact that the proposed system significantly outperforms the other two approaches.

The analysis of the false-positive rate in Table 5 also shows that the proposed system effectively identifies the selfish nodes with improvised learning strategies. In contrast, the performance of FPR is quite inferior in the other two cases. The prime reason for the proposed system to attain much reduced FPR is that it considered an infinite game model for n number of players where the game is simplified and modeled in a way where it converges towards the best possible outcome in each and every iterative step of execution. Whereas in the case of [19], a similar trend of FPR is followed which have got marginal difference with the proposed approach but FPR is quite higher in the case of [28]. The visual comparative outcome is illustrated in Fig. 5 where the interpretation can clearly show the significance of the proposed approach.

**TABLE 5.** Analysis of False Positive Rate (FPR) measure with $S_{node}$ = 25.

| $\#S_{node}$ | FPR (ProP) | FPR [28] | FPR [19] |
|---|---|---|---|
| 5 | 0 | 0.19 | 0 |
| 10 | 0 | 0.21 | 0 |
| 15 | 0 | 0.28 | 0.02 |
| 20 | 0.002 | 0.29 | 0.1 |
| 25 | 0.0127 | 0.27 | 0.14 |

From the analysis of FPR in Fig. 5, it is seen that the proposed system identifies the $M_{node}$ within the IoT with higher accuracy. In contrast, the outcome of the other two approaches reflects inferior FPR values as compared to the proposed system.

The analysis outcome clearly shows that the proposed approach not only poses efficiency in terms of security but also stimulates the nodes in cooperative packet forwarding which has a significant impact on increasing the throughput

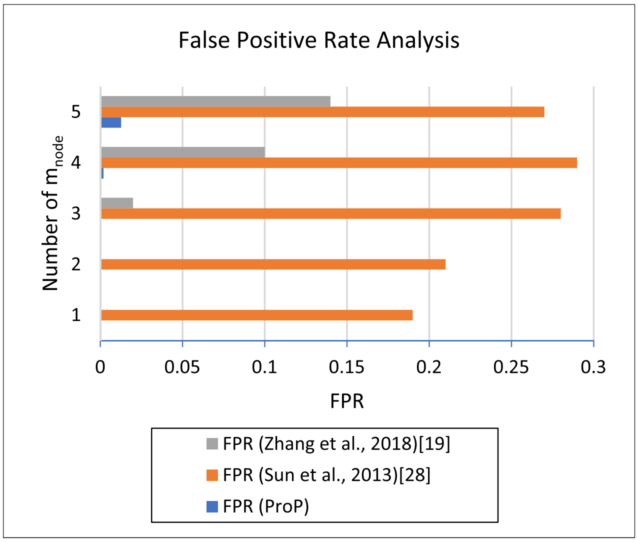

**FIGURE 5.** Analysis of FPR for variable #$M_{node}$.

and also the involvement of simplified computational steps makes it more computationally efficient which enhances the overall delay performance to a significant extent.

## VII. CONCLUSION

The study introduces a novel combined approach of intrusion detection techniques to strengthen information security in IoT layers. The novelty of the approach is that it is not only robust against different types of attacks but also does not compromise with the IoT communication performance in terms of both delay and throughput. Another contributory aspect includes that it not only identifies the $M_{node}$ and $S_{node}$ but stimulates them to cooperate in regular communication activities for a higher degree of packet forwarding. Eventually, the experimental outcome shows that the proposed approach is quite effective and significantly outperforms the conventional baseline modeling. However, the limitation of the proposed approach is that it adopted a complete theoretical study where the system design modeling is emphasized only for targeted use-cases in ad-hoc networks. Our future direction of research will investigate the data complexity management and dynamic traffic management in a secure environment for providing more reliable operation in cyber-physical systems and Industry 4.0.

## ACKNOWLEDGMENT

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

## REFERENCES

[1] C. Lee and A. Fumagalli, "Internet of Things security–multilayered method for end to end data communications over cellular networks," in *Proc. IEEE 5th World Forum Internet Things (WF-IoT)*, Limerick, Ireland, Apr. 2019, pp. 24–28.

[2] S. Ziegler, S. Nikoletsea, S. Krco, J. Rolim, and J. Fernandes, "Internet of Things and crowd sourcing—A paradigm change for the research on the Internet of Things," in *Proc. IEEE 2nd World Forum Internet Things (WF-IoT)*, Milan, Italy, Dec. 2015, pp. 395–399.

[3] M. Rouse. (2018). What is IoT Security (Internet of Things Security)?—Definition From WhatIs.com. IoT Agenda. Accessed: Aug. 31, 2019. [Online]. Available: https://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security

[4] Itu.int. *Internet of Things Global Standards Initiative*. Accessed: Dec. 31, 2019. [Online]. Available: https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx

[5] F. Mattern and C. Floerkemeier, "From the Internet of computers to the Internet of Things," in *From Active Data Management to Event-Based Systems and More*. Berlin, Germany: Springer, 2010, pp. 242–259.

[6] K. Ashton, "That 'Internet of Things' thing," *RFID J.*, vol. 22, no. 7, pp. 97–114, 2009.

[7] S. F. Abedin, M. G. R. Alam, N. H. Tran, and C. S. Hong, "A fog based system model for cooperative IoT node pairing using matching theory," in *Proc. 17th Asia–Pacific Netw. Oper. Manage. Symp. (APNOMS)*, Busan, South Korea, Aug. 2015, pp. 309–314.

[8] V. M. Rohokale, N. R. Prasad, and R. Prasad, "A cooperative Internet of Things (IoT) for rural healthcare monitoring and control," in *Proc. 2nd Int. Conf. Wireless Commun., Veh. Technol., Inf. Theory Aerosp. Electron. Syst. Technol. (Wireless VITAE)*, Chennai, India, Feb. 2011, pp. 1–6.

[9] B. U. I. Khan, R. F. Olanrewaju, R. N. Mir, A. Baba, and B. W. Adebayo, "Strategic profiling for behaviour visualization of malicious node in MANETs using game theory," *J. Theor. Appl. Inf. Technol.*, vol. 77, no. 1, pp. 25–43, 2015.

[10] A. A. Hadi, M. A. Zulkarnain, and Y. Aljeroudi, "Improved selfish node detection algorithm for mobile ad hoc network," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 4, pp. 103–108, 2017, doi: 10.14569/IJACSA.2017.080415.

[11] S. Hameed, F. I. Khan, and B. Hameed, "Understanding security requirements and challenges in Internet of Things (IoT): A review," *J. Comput. Netw. Commun.*, vol. 2019, pp. 1–14, Jan. 2019, doi: 10.1155/2019/9629381.

[12] A. Kanuparthi, R. Karri, and S. Addepalli, "Hardware and embedded security in the context of Internet of Things," in *Proc. ACM Workshop Secur., Privacy Dependability Cyber Vehicles*, Berlin, Germany, 2013, pp. 61–64.

[13] Z.-K. Chong, S.-W. Tan, B.-M. Goi, and B. C.-K. Ng, "Outwitting smart selfish nodes in wireless mesh networks," *Int. J. Commun. Syst.*, vol. 26, no. 9, pp. 1163–1175, Sep. 2013, doi: 10.1002/dac.1388.

[14] T. Basar and G. J. Olsder, *Dynamic Noncooperative Game Theory*, vol. 23. New York, NY, USA: SIAM, 1999.

[15] S. Singh and N. Singh, "Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce," in *Proc. Int. Conf. Green Comput. Internet Things (ICGCIoT), Noida, India*, vol. 2015, pp. 1577–1581.

[16] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. 6th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, Boston, MA, USA, 2000, pp. 255–265.

[17] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the CONFIDANT protocol," in *Proc. 3rd ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, Lausanne, Switzerland, 2002, pp. 226–236.

[18] A. Jesudoss, S. V. K. Raja, and A. Sulaiman, "Stimulating truth-telling and cooperation among nodes in VANETs through payment and punishment scheme," *Ad Hoc Netw.*, vol. 24, pp. 250–253, Jan. 2015, doi: 10.1016/j.adhoc.2014.08.018.

[19] W. Zhang, S. Zhu, J. Tang, and N. Xiong, "A novel trust management scheme based on Dempster–Shafer evidence theory for malicious nodes detection in wireless sensor networks," *J. Supercomput.*, vol. 74, no. 4, pp. 1779–1801, Apr. 2018, doi: 10.1007/s11227-017-2150-3.

[20] J. Rauscher and B. Bauer, "Safety and security architecture analyses framework for the Internet of Things of medical devices," in *Proc. IEEE 20th Int. Conf. e-Health Netw., Appl. Services (Healthcom)*, Ostrava, Czech Republic, Sep. 2018, pp. 1–3.

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

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

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

[24] K. Balakrishnan, J. Deng, and P. K. Varshney, "TWOAK: Preventing selfishness in mobile ad hoc networks," in *Proc. IEEE Wireless Commun. Netw. Conf.*, New Orleans, LA, USA, vol. 4, Mar. 2005, pp. 2137–2142.

[25] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, May 2007, doi: 10.1109/TMC.2007.1036.

[26] E. M. Shakshuki, S. Member, N. Kang, and T. R. Sheltami, "EAACK—A secure intrusion-detection system for MANETs," *IEEE Transactions on Industrial Electronics*, vol. 60, no. 3, pp. 1089–1098, 2013, doi: 10.1109/TIE.2012.2196010.

[27] Z. Ji, W. Yu, and K. J. R. Liu, "A game theoretical framework for dynamic pricingbased routing in self-organized MANETs," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 7, pp. 1204–1217, 2008, doi: 10.1109/JSAC.2008.080917.

[28] Y. Sun, Y. Guo, Y. Ge, S. Lu, and J. Zhou, "Improving the transmission efficiency by considering non-cooperation in ad hoc networks," *Comput. J.*, vol. 56, no. 8, pp. 1034–1042, 2013, doi: 10.1093/comjnl/bxt042.

[29] M. Touati, R. El-Azouzi, M. Coupechoux, E. Altman, and J. M. Kelif, "A controlled matching game for WLANs," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 3, pp. 707–720, Feb. 2017, doi: 10.1109/JSAC.2017.2672258.

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

[31] J. F. Nash, "Equilibrium points in n-person games," *Proc. Nat. Acad. Sci. USA*, vol. 36, no. 1, pp. 48–49, Jan. 1950.

[32] J. Nash, "Non-cooperative games," *Ann. Math.*, vol. 54, no. 2, pp. 286–295, 1951.

[33] F. Anwar, B. U. I. Khan, R. F. Olanrewaju, B. R. Pampori, and R. N. Mir, "A comprehensive insight into game theory in relevance to cyber security," *Indonesian J. Electr. Eng. Informat. (IJEEI)*, vol. 8, no. 1, pp. 189–203, 2020.

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

**BURHAN UL ISLAM KHAN** (Graduate Student Member, IEEE) received the B.Tech. degree in CSE from IUST, Kashmir, in 2011, and the M.S. degree in CIE from International Islamic University Malaysia (IIUM), Kuala Lumpur, in 2014, where he is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering. He is also a Graduate Teaching Assistant with the Department of Electrical and Computer Engineering, IIUM. Before commencing his Ph.D. degree, he has been involved in varying roles as that of a Software Engineer, a Research Analyst, and an Assistant Professor. His current research interests include designing one time password schemes, employing mechanism design, and game theory to protect ad-hoc networks.

**FARHAT ANWAR** (Member, IEEE) received the Ph.D. degree in electronic and electrical engineering from the University of Strathclyde, U.K., in 1996. Since 1999, he has been with 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 ad-hoc and sensor networks, computer and network security, network simulation and performance analysis, the IoT, and biometrics.

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

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

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