ECM-GT: Design of Efficient Computational Modelling based on Game Theoretical Approach Towards Enhancing the Security Solutions in MANET

Burhan Ul Islam Khan, Rashidah Funke Olanrewaju, Farhat Anwar, Roohie Naaz Mir

Abstract*: Game Theory is a useful tool for exploring the issues concerning Mobile Ad-Hoc Network (or MANET) security. In MANETs, coordination among the portable nodes is more significant, which encompasses their vulnerability challenges to several security assaults and the inability to run securely, when storing its resources and manage secure routing between the nodes. Hence, it is imperative to design an efficient routing protocol to secure all nodes from unknown behaviors. In the current research study, the game-theory approach is utilized for analytical purpose and addresses the security problems in MANETs. The game-theoretic approach is mainly adopted to find the malicious activities in the networks. In the proposed work, a Bayesian-Signaling game model is proposed which analyses the behavior of both regular/normal and malicious nodes. The game model proposed also provides the finest actions of autonomous tactics for every node. A Bayesian-Equilibrium (BE) offers the best solution for games to resolve the incomplete information by joining strategies and players payoff which form an equilibrium. By exploiting the BE mechanism, the system can detect the behavior of regular as well as malicious nodes. Therefore, Efficient Computational Modelling based on Game Theory or ECM-GT methodology will reduce the utility of malicious nodes and increase the utility of regular nodes. Also, it stimulates the best co-operation among the nodes by exploiting the reputation system. On comparing our results with the existing systems, it was found that the proposed algorithm performed better in the detection of malicious nodes, throughput, false positive rate and detection of attacks.

***Index Terms*: Bayesian-Equilibrium, Game-Theory, Bayesian signaling model, MANETs, Secure routing protocol.**

I. INTRODUCTION

Nowadays, security is becoming the main contesting issue in the research field of mobile wireless networks viz.MANETs. In a mobile ad-hoc network, mobile devices can organize autonomously and collaborate with each other on bandwidth-constrained wireless connections. The mobile nodes in a MANET can behave like network routers as well as network hosts; a network router is responsible for packet routing whereas network host is meant for sending and receiving packets [1]. The mobile ad-hoc network topology changes dynamically. Many researchers have proposed different distributed algorithms which determine the network routing, link-scheduling, and network organization. Conversely, the unique features of wireless mobile networks present several security-related challenges. Before narrowing down to the prominent security issues that are the primary point of concern in the proposed study, the general problems that are inherent with MANETs are illustrated in brief:

A. Insecure Wireless Environment

One of the critical issues of using wireless network starts with the ubiquitous access as well as the pervasive nature of performing computation [2]. Along with the various set of services rendered in a wireless environment, different types of proximity services are also frequently used, making users depend on multiple forms of identities to access such services. Due to this phenomenon, the wireless environment possesses maximum dimensionality of security vulnerability especially from the networking devices that they are using [3]. Similar features are also applicable in MANET, thus making it very hard to authenticate and authorize any user who happens to be existing in the wireless environment predominantly.

B. Absence of Central Points

In MANET, there does not exist any concept of Entry and Exit points such as routers, gateways, etc. [4]. The lack of such a centralized facility makes the detection of assaults on the network a very challenging task especially when considering a MANET environment which is highly dynamic and primarily scaled [5].

C. Constrained Resources

The mobile nodes existing in the MANET system are typically small devices powered by batteries, usually having a low computational capability. This limited power resource is one of the prime reasons which makes a node to behave selfishly especially when it finds its available power has depleted below some threshold [6]. Moreover, channel capacity is highly limited for the data transfer in a MANET system [7].

Revised Manuscript Received on May 10, 2019

Burhan Ul Islam Khan, Department of Electrical & Computer Engineering, Kulliyyah of Engineering IIUM, Kuala Lumpur Malaysia.
Rashidah Funke Olanrewaju, Department of Electrical & Computer Engineering, Kulliyyah of Engineering IIUM, Kuala Lumpur Malaysia.
Farhat Anwar, Department of Electrical & Computer Engineering, Kulliyyah of Engineering IIUM, Kuala Lumpur Malaysia.
Roohie Naaz Mir, Department of Computer Science & Engineering, National Institute of Technology, Srinagar, Kashmir.

D. Node Mobility

As the word mobile in networking brings about sophistication trends, it also brings with itself the associated complications. In MANET, nodes are mobile and can thus move in every direction at any time and can independently leave as well as join the network; consequently, the network topology can change quickly, hence termed as dynamic. Node mobility leads to frequent link breakages; furthermore, traditional Intrusion Detection System (IDS) techniques turn ineffective to cope with highly dynamic topologies [8].

E. Scalability

In traditional wired networks, the scale is more or less predefined before actual deployment and rarely changes during its use, but the same does not hold true for MANETs where the scale keeps on changing with time or instead can be understood to be unpredictable. Thus, one can hardly predict the status (topology and number of nodes in a network) of the network in future due to which related protocols and services must be well-matched with its dynamically varying scale.

F. Nature of Unpredictability

Mobile ad hoc networking system can be used in any geographic location on the earth if multiple nodes with routing capability exist. Hence, visualizing this scenario in real time applications will mean that there exist a multiple number of nodes where it is almost hard and sometimes nearly impossible to understand which node is legitimate [9]. Dynamically changing links, the random mobility of nodes and varying scale of the network all contribute to the unpredictable asset.

Unfortunately, the feasibility to detect the intruders in a MANET is decidedly less owing to its decentralized topology, and thus malicious activities are performed by intruders to exploit the vulnerable characteristics of MANETs. The current improvement in MANETs that assists in the brisk construction of the network and interacting without predefined setup also presents itself in relevance for various IoT-based presentation domains in smart towns [10] [11]. Multiple attacks have been recorded almost at every layer within the MANET, i.e., application, transport, physical, MAC or data link, and network. Such networks are susceptible to various attacks which disrupt the reputation and trust among the mobile nodes [12] [13] [14]. The reliable mobile nodes have to pay the cost of the intrusion and other attacks where their communication is severely affected thereby leaving an adverse impact on overall application performance, massive intrusion, eavesdropping, and loss of data. The cost of an attack scenario is much worse when the MANET system is considered with large scales such as IoT urban scenarios. It could be observed from the review of related works that the routing protocol-based solutions are comparatively more in number than the other security-based mechanisms employed in MANETs. Nevertheless, it should be realized that the malicious behavior can be overlooked in large-scale MANET applications if only routing-based approaches are emphasized. This is because several factors such as node behavior and the dynamics of strategies implemented on various kinds of nodes are somewhat complicated to solve when mechanizing the routing approach. Though numerous issues have been identified in MANETs in the recent past such as power issues [15], [16], routing effects [17], QoS issues [18] [19], the security-related problems are still unsolved [20] [21]. There are several security assaults present in MANETs like Denial-of-Service (DoS), black-hole, wormhole, resource depletion, interference and so on [22]. Some of the significant researchers have done a massive volume of research, but an efficient system that ensures failproof and proper security is yet to be seen and normalized for the security protocols in future. That is, presently the network security is becoming the emerging topic for researchers to resolve several adversary attacks.

GameTheory mechanism has been introduced to improve the rate of network security. Game-Theory is an essential tool which gives a mathematical framework for model design and can analyze the decision-based problemsbecause it addresses the issues where multiple users with incentives compete. In this mechanism, a single user's outcomes depend on his decisions as well as on others' choices. Likewise, the security mechanism in MANETs also depends on the actual defense schemes as well as on the decision taken by attackers. Game theory modelling is intended for explaining the reason humans behave in some particular way and for guessing the action they would perform based on their behavior. In the security domain, game theory can be employed as an aid to select an optimal strategy for attacking and defending as per the probability of actions that shall be performed by the defender or attacker. Considering the criteria of the game, game theory defines a utility function for every player. Utility functions are utilized for showing the results of the actions performed by the players. Suppose a strategy A is selected by a player that maximises his/her outcome based on the strategy B of the other player or group; strategy A becomes the best response [23].

Traditionally, game theory has been utilized as a modelling tool to describe and influence behavior in social systems. In recent times, game theory has evolved as an essential tool for prescribing or controlling behaviours in a dispersed engineered system [24]. The underlying principle for such a prospect stems from the similarities between the decision-making frameworks in distributed engineered systems and social systems [25]. Game theory deals with the decision making logic in societal situations where the results rely on the decisions of the independent agents (two or more) involved. An essential trait in those situations is that every decision maker has only limited control over the result [26]. The main goal in game theory is to retrieve a proper strategy for the resolution of conflicts arising or to acquire the optimal series of decisions leading to the highest payoff value [27].

While exploring some latest techniques on the security systems in MANET and Mobile Wireless Sensor Network (MWSN), it was revealed that there exists prominent involvement of game theory due to the computational efficiency and prospective accuracy in its probabilistic approach. However, as of now, there are no standardized frameworks developed for studying security problems while dealing withthree or

more player's interactions with anemphasis on including severaltypes of defenders and offenders. In the proposed work, a Bayesian Signaling (BS) approach has been used for securing MANET systems, i.e., ECM-GT. The primary aim is to detect malicious activities and behaviors. Also, this approach can find the solution and gets the threshold value which can be utilized for designing a secure routing protocol for MANETs. Additionally, the proposed strategy reduces the malicious node utility and stimulates better collaboration among the nodes by exploiting the reputation system.

The content following has been divided into various sections with Section-II reviewing about related work which discusses the prior study and security challenges in MANETs. Section-III illustrates the framework design of the proposed system followed by result analysis in section-IV. The paper culminates in a conclusion of the proposed work.

II. BAYESIAN SIGNALLING GAME MODEL

In general, the games can be either cooperative or non-cooperative. In the non-cooperative scheme, two or multi-players compete, while in the cooperative plan, number of players team up to reach the highest possible benefits. Cooperative games are those in which there is cooperation among the players which scrutinize optimal strategies for the group of players whereas non-cooperative games analyse the environment in which players exist, and the autonomous decision of nodes determines the node payoff. One of the non-cooperative game models is a Bayesian game model where the player performs an action even without complete information of the competent [28] [29].

A game contains a group of players, payoffs, and some moves/strategies. Each player has a strategy for the action of the probable state in the game. Players' payoffs give an incentive scheme where the player loses or wins in a specific state in the game. Since all the nodes are portable, they can travel arbitrarily. Payoff scheme supports the players to forward the packets to one another. Security guarantee is inefficient in resource consumption. Therefore, to overcome this problem, the MANETs are divided into a set of distinct clusters. In every cluster, the nodes select a head-node which serves as IDS for the whole cluster. In this system, a single node is motivated by providing a reputation model. In other game models, 'Bayesian interaction' games offer a solution for distributing the endogenous interaction model, which defines some asymptotic statistics for co-operating with other players [30]. Therefore, this approach can solve various critical issues in which there is a delay among private information and player reaction. The present study provides a 'Bayesian Signaling' model to solve the security issues in MANETs.

III. RELATED WORK

According to researchers, there are two corresponding methods which guard MANETs: 1) Prevention based (e.g., authentication) and 2) Detection based approach (e.g., intrusion detection system). In [31][32], authors have introduced general requirements for an intrusion detection system (IDS) that works in MANET systems and presented a primary intrusion detection mechanism for MANETs. In this, authors showed that every IDS agent is independently involved in the task of intrusion detection. On the other hand, authentication is an essential mechanism that is initiated by the IDS. After the process of authentication, only authorized user can proceed for further process.

When the literature related to security in MANETs was studied, it was found that game-theory-based solutions were increasingly being used to various problems related to MANETs like that of topology control [33], [34], [35], [36], [37], dynamic spectrum sharing [38], [39], [40], etc. The research works studied have been briefed below:

In [41], a multi-level noncooperative game theory approach was introduced where each network node with IDS was able to detect the attack, whereas in [42] researchers have proposed an integrated ad-hoc routing protocol for MANETs with Game-Theory strategy. An advantage was that every node could transmit their data packets via the route with low power utilizationof host IDS and the lesser prospect of attack as per the finest decision.

Authors in [43] have tried to design an IDS based cooperative method to find the intrusions in the ad-hoc networks. In [44], authors have applied the 'Bayesian' approach to the study of intrusion detection between legitimate and malicious nodes. The malicious node will be responsible for deceiving the legitimate nodes by cooperating with each other and obtaining high payoffs, whereas legitimate nodes select a probability to work together with malicious nodes and make the misbehaviors report to their updated beliefs. However, some researchers have found few excellent routing protocols which address the security-related issues in MANETs by applying Game-Theory approach. Almost the entire existing research has considered only a security game system with dual-players in the security game approach, i.e., defender and attacker. In the situation with multiple defenders and attackers, the security game model is designed as a dual-player game where the defender behaves like a single player and single attacker. Hence, this assumption is not realistic for MANETs; i.e., it is valid only for the centralized network system. As a result, each node in a MANET should be treated as an individual node in the security game system.

In [45], the authors utilized Bayesian watchdogs for proposing a collaborative approach to detect selfish nodes and black holes in MANETs. The idea behind watchdogs involves Bayesian filtering and sharing of reputation among collaborative nodes. The watchdog performance is improved by reducing the percentage of false positives and false negatives.

The author in [46] put forth the Bayesian game model to thwart gray hole attacks in wireless ad hoc networks. The authors have defined an extensive form of game in the proposed defense approach that can be evaluated by interim equilibrium. The author examined this interim equilibrium after converting the Bayesian normal form game.

A Bayesian game for wireless sensor networks was formulated by authors in [47] for identifying the malicious nodes.

There are two Bayesian Nash equilibria in this game that can be used as a defense strategy, but it could not be modeled as a dynamic Bayesian game since the adversary could update beliefs only at the termination of every game-stage.

In [48], authors have presented a model involving network-centric as well as node-centric perception of node interactions participating in MANETs by employing cooperative game theory. The use of cooperative game theory helps in seizing the large player group dynamics; the strategy selected by any player relies on the self-interested game perception as well as the group-wide policy of the alliance that the player forms a part of. Alternatively, the non-cooperative approach characterizes CORE in a better way as compared to other mechanisms in real-life scenarios. However, multiple players have not been considered in their approach.

In [49], the intrusion detection process has been modeled employing game theory. The IDS models based on game theory are supposed to model intrusion detection as a non-cooperative game between a defender and an attacker where the defender attempts to raise its payoff value to the maximum by raising its probability of effective intrusion detection whereas the attacker attempts to reduce its likelihood of being sensed by the IDS to the minimum.

In [33], authors have proposed a solution to topology control in MANETs centred on the game theory by exploring the Nash Equilibria concept which is meant for the normal games and controls the overall topology by the selection of proper power level by each node in a MANET. The works [50], [34] also exploit the power level as potential games for deciding the underlying topology in case of networks that are power efficient. In [35], researchers have proposed a distributed approach for solving the problem of connectivity in MANETs. Authors in [36] have examined the congestion control game by regulating a contention window and a time interval. The same problem has been solved by authors in [37] by employing pricing models**.**

Connectivity games have been proposed in [33] for wireless networks as a part of game-theory applications to topology control. In a strong connectivity game, there is the requirement that every network node should be linked (not compulsorily directly) to every other network node. Each node in a strongly k-connected game can accessall other nodes through k internally disjoint paths. All games progress among the players in synchronized steps with just one player active at a particular instant. The radio propagation power is reduced by the player to a level which upholds the desired network objectives. However, such approaches are not applicable to realistic situations because strict synchronization and global network coverage are needed. The potential games that reduce power [50] preserve desired topologies with the least power consumption and less transmission power for discrete devices. Such games also presume comprehensive knowledge of the current state of the overall network for every user at every computational step.

In [51], a model has been constructed that allows the formation of clusters with individual trusted nodes functioning as the Certificate Authority (CA). The main intention of the system proposed is the stimulation of non-confident community nodes to participate by the allocation of trust-based incentives for their participation. These incentives are later employed by these nodes for availing various cluster services. The results obtained reveal the preservation of the security of the certificate authority which prolongs the cluster lifetime. Furthermore, the cluster-size can be shrunk by the model that hints at an increase in the formation of clusters. This brings about efficiency and network stability in serving the nodes in clusters. Nevertheless, the malicious behavior of cluster nodes has not been considered, and the security analysis of the model has also not been performed.

The authors in [52] have addressed the intrusion problem in MANETs and a fewof its solutions grounded on game theory. Four game-theory based approaches have been evaluated in their study claiming to increase the performance of the IDS by the utilization of Energy efficiencies, Number of nodes with IDS capability, Clustering and Competence in detecting misbehaving selfish nodes as the performance metrics. The authors have also presented the pros and cons of the proposed system.

A unique credit-based cooperation system was proposed in [53] that defends against cheating done by malicious nodes by utilizing hash chains on the messages. The authors showed that this system imposed a lower workload on nodes as compared to the methods that employ digital signatures. Besides, it has been demonstrated by game-theoretic analysis that a node can attain any cooperation level if appropriate payments are made by the mechanism. But the authors have not discussed the scalability of the system; the coordination among the malicious nodes has not beentaken into account, and the malicious nodes have been exhibited as fragile. Also, hash chains are susceptible to rainbow attacks. Therefore, there is a scope for enhancing the employed strategies.

In [42], authors have proposed a security add-on known as “AODV-GT” based on game theory for the reactive Ad-hoc On-Demand Distance Vector (AODV) protocol. This add-on is meant for safeguarding MANETs from blackhole attack. The proposed system is based on non-cooperative non-zero games and dramatically reduces the packet drop ratio on integration with AODV. This contrasts with the utilization of unaided AODV when blackhole nodes are present in the network. Nevertheless, authors have assumed the presence of HIDS sensors in the MANET environment which are responsible for the elimination and detection of malicious nodes, therefore, leaving the malicious behavior untouched. Also, this add-on fails to run on top of other existing MANET routing protocols and cannot be applied for other routing attacks.

Authors in [54] have proposed a global punishment scheme based repeated game forwarding model for enforcing node cooperation as well as mitigation of selfish behavior. The conditions leading to the acquirement of Nash Equilibrium for the MANET's cooperative state have also been emphasized upon by the authors. This model is stable than the existing approaches in the sense that it takes into account the reasonability of misbehaving nodes (i.e., selfish nodes here).

Nevertheless, selfish nodes have not been modeled fragile in this study. The simulation performed in this paper reveals that cooperation can be enforced by this system among the selfish nodes. But no effort can be seen about mitigation or examination of malicious behavior. Also, this model cannot be applied to ward off newcomer attack, Sybil attack, bad-mouthing attack, etc.

Another game-theoretic framework has been proposed in [44] for analyzing the strategy profiles of malicious and regular nodes. In the highly empirical work conducted by authors, every node on the opposite side is modeled as rational concerning the playing of the game with the rest of the nodes. The authors have exhibited the tussling between malicious and regular nodes as Multistage Bayesian Signaling Game. Nonetheless, authors challenge that quite a lot of regular nodes could begin to show selfish behavior eventually as the game proceeds. The node rationality has not been taken into account when the decision-making model for the malicious-regular node game was designed with the sole intent to discourage selfish behavior shown by regular nodes.

In [41], a host-based IDS has been designed by employing a non-cooperative dynamic game with insufficient information. The interactions among the MANET nodes have been modelled as a simple signalling game that falls into the category of a multistage non-cooperative dynamic game with inadequate information. An optimal strategy has been presented for both host-based IDS and the intruders. The IDS and the attacker play the intrusion detection game. The attacker aims to attack the target node by the transmission of a malicious message from an attack node. When the target node receives the malicious message without being exposed by host IDS, the intrusion is considered to be successful. However, when the message transmitted by the alleged intruder is interrupted and blocked after being assumed as an intrusion, the host IDS is confident that the nature of the message is malicious. An undetected intrusion costs the user more severely than the false alarms in this model. In the game model proposed, the sender is a node, and the receiver is a host-based IDS to which messages are directed. The sender node can be a malicious node/attacker or a regular node. The strategy adopted by the IDS is the selection of an optimal scheme from the available set for responding to a message coming from a sending node. The tactic chosen depends on the preceding beliefs of the receiver so that the effective payoff can be maximized after reducing the costs associated with missed attacks and false alarms to the least. This model is considered to be theoretically consistent, and this modelling technique is believed to model intrusion detection more realistically in comparison to existing approaches.

A game theory framework was proposed in [55] using Bayesian formulation for analysing interactions between pairs of attacker nodes and defending nodes. Though they took into account the energy and resource constraints in MANET, they studied the Nash equilibrium for host-based IDS/attacker game in static as well as dynamic scenarios. The dynamic Bayesian game model has been found to be more realistic because the IDS can revise its belief consistently on the maliciousness of the adversary as the game proceeds. The authors suggest a novel hybrid Bayesian detection approach for the IDS where the opponent's actions are estimated using a lightweight monitoring system and the last resort of defence is a heavyweight monitoring system. They have discovered that this dynamic game model results in monitoring schemes for the defender which are energy-efficient and enhancing the total hybrid detection power at the same time. Furthermore, it has also been shown that even though the equilibrium in this model is determined by the knowledge of malicious node on the utility of defender for various actions and what is thought about the updated belief of the defender, it is robust enough to the imperfect knowledge of the malicious node regarding the lightweight monitoring system of the defender.

In [56], a game theory model has been presented by the researchers for efficiently deploying IDSs in MANETs. They have asserted that there is a detection system on each node running continually in the majority of the previous IDSs. Thus, it leads to a costly overhead for the resource-constrained mobile device. Game theory has been employed for modelling the interactions between the attacker and the IDS to establish if it is necessary to keep the intrusion detection system running without negotiating its effectiveness. In the proposed model, an intrusion from the attacker is detected by an IDS; thus, this model works as a game among the players, the attacker and the IDS. The main aim of the attacker is attacking the MANET without being detected while that of the IDS is the detection of the attack by the attacker. Therefore, the proposed model has been constructed for non-cooperative two-player no-zero sum game. The assumptions considered by the authors include: an intrusion detection system is present on each node which scrutinises the data for intrusion detection and needs not run continually on the node during the time the network is up. There are two strategies for both players in the strategy profile. The pure strategy space thus comprises of no monitor, monitor t% time and that of the attacker consists of no attack, attack s% time. The authors have taken into account perfect as well as imperfect IDS, and thus two-game models have been established by them – between the attacker and perfect IDS, and the other between the attacker and imperfect IDS. For both the models, the solution is a mixed policy pair of Nash equilibrium where none of the players has autonomous motivation for altering its tactic. The details of the players' payoffs and game models have been tabulated in [56] which show that there is no need of keeping the IDS running continually while maintaining its efficacy. They believe that this analysis plays a role in establishing optimal defence strategies that must be deployed by the network administrator.

In [44], authors have designed a 'Game-Theory' framework which analyzed the profile strategies for regular as well as malicious nodes. The author applied a BS game model and examined a relation between nodes by a combination of action and cost, a gain of each strategy. They proposed a decision-based approach for regular nodes which report and make malicious nodes to escape. Finally, they presented some countermeasures to control the flee-strategy.

In [57] a 'Game-Theory' approach was adopted which analyzed the co-operation incentive strategies offered by two different systems and by a method with non-cooperation incentive mechanism. The authors proposed a plan of exploiting threshold values which determines the node trustworthiness in the reputation model and of returning co-operative nodes in the price-based system which can be influenced by wealthy nodes. The resulting analysis carried out by simulation experimentation shows the priority of the unified framework on a separate reputation system.

In [58], researchers have studied the co-operation enforcement for independent MANETs in noisy observation and mainly focused on basic networking features like packet forwarding. Additionally, the authors have proposed a strategy with a belief model which can manage the co-operation system as well as measured its performance parameters. Finally, the simulation outcomes showed that the proposed model could perform efficiently as compared to unconditional co-operative results when noisy observation exists.

Authors in [59] have proposed a probabilistic model which involves two players, and they act as dynamic variables. In this approach, two players' coordinate with each other and call for a co-evolutionary process of network and play, this has been taken from [59] which shares the games. Moreover, they have considered the statistical model by adopting the Bayesian interaction model. In this, each player utility function contains two conditions: 1) Reward of the player in the interaction process which shares the structure and 2) A payoff element interpreted as a part of the player.

TABLE I. MITIGATION OF NODE MISBEHAVIOR IN MANETS

AUTHOR	CONTRIBUTION	RESULT OBTAINED	LIMITATIONS
(Wang, 2014) [40]	Presented Mean Field Game Theoretic method for enhancing security in cognitive radio MANETs	- Significantly improves the MANET lifetime and decreases the probability of compromising - Empowers a separate node in MANET to decide for shared-out security defense	- Scenario of multiple defenders and multiple attackers not considered
(Hamdi and Abie, 2014) [63]	Emphasized on e-Health applications by presenting a game theory based model for IoT adaptive security	- Increases the lifespanof smart-things by 47% as compared to the current models - Balances the security-effectiveness and energy-efficiency	- Only some threat scenarios considered in the simulation
(Abegunde et al., 2016) [64]	Proposed a dynamic game for IoT and IEEE 802.15.4 in which nodes can choose and acclimate their game tactics consistent with their energy level and the 'state of the game'	- Improved security and performance in comparison to IEEE 802.15.4 access method - Enhancement in fairness and utility in channel sharing in addition to energy usage efficiency	- Reality of load-level variation not taken into account

In [60] a solution was introduced for managing the consumption of resources of the intrusion detection system in between every node during the prevention of nodes from the selfish action. To address selfish action, the author designed an incentive model regarding reputation which encourages the nodes to take part in the node selection scheme by considering the cost analysis. The cost analysis was devised to prevent the nodes' information and guarantee every node's contribution to the selection process. Authors showed that the proposed node selection approach is suitable to solve the IDS issues in MANETs.

In [61], a survey was presented on different approaches to network security and privacy. The prime motive was to address various research approaches for adopting Game-Theory to network security. From this study, the authors showed that game theory is an essential tool which is exploited as a solution for current and emerging security issues in the networking system.

In [62] a game-theory approach was adopted for the detection of malicious users/attackers in the MANETs. Each user is designed as payoff swelling strategic agent. A "Fictitious play" is utilized for genuine user action, but no bounds are forced on malicious attacker strategies. The author found the worst-case equilibrium and acknowledged the efficiency of network topology. In addition to these approaches, the previous record of studies concerned with the mitigation of misbehavior problem of nodes in a MANET environment together with their pros and cons has beentabulated in Table I.

(La and Cavalli, 2016) [65]	Put forward an algorithm for node misbehavior detection by using weighted-link in hierarchical 6LoWPAN sensor networks	- Defendedby several experiments in the real platform showing favorable results without false negatives and lesser false positives	- No consideration of node mobility - Exposed to some intricate intrusions/ attacks in the network and application layer
(Das et al., 2015) [66]	Presented a novel game-theoretic model to detect selfish nodes in MANETs	- Assures low-cost, secure data transfer the minimum idle time	- Existence of malicious nodes has not been cared about
(Taheri et al., 2016) [67]	Put forward an approach for malicious node detection employing Game Theory	- Improvement in malicious node detection efficiency and lesser false positives than former algorithms	- Multiple attacker-defender settings have not been taken into consideration
(Rajkumar and Narsimha, 2016) [68]	Presented a threshold revocation mechanism based on Trust and CA distribution for improving MANET security	- Exterminates misbehaving nodes - Simulation showed improvement in delivery ratio, packet drop and resilience	- Various issues like slow revocation, network overhead and inaccuracy
(Sengathir and Manoharan, 2013) [69]	Proposed a security add-on for Multicast Ad-hoc On-Demand Distance Vector protocol	- Efficiently detects misbehaving nodes	- No clear distinction between Malicious and Selfish nodes. - Malicious nodes have been modeled as fragile.

			- Cannot be applied to other routing protocols

The next section illustrates the proposed framework design.

IV. FRAMEWORK DESIGN

The framework presented in this paper considers a dynamic multi-stage Bayesian Signaling game. Every mobile node in a Bayesian game is set with some classified information which has a considerable effect on the game evolution whereas the remaining mobile nodes are assumed to hold information about the classified data of the belief system. Those belief values are denoted by a probability distribution and updated by the application of Bayes rules if novice information is available. The mobile nodes choose the most optimum action in the course of the game based on the classified data as well as the existing belief information. The proposed framework adopts Perfect Bayesian Equilibrium ensuring belief formation for a particular node type about its competing mobile node type, updating the belief information at the termination of each stage and approving the actions performed with the help of the belief system in the present stage.

In the framework, a cluster is formed in which mobile nodes associate or depart autonomously owing to their mobility in the collective simulation environment. The identity of mobile nodes is regulated by the physical features of the nodes that are permanently static. When there is a new incoming node that desires to add to the cluster, other nodes existing in the cluster allot their initial beliefs to that node. In case a malicious node enters a cluster that has not been visited previously, other nodes of that cluster consider the malicious node as the newcomer and allot their initial beliefs to it. Every node in that cluster receives the reporting information broadcast from the regular mobile node. If the information reported is positive, the malicious node shall be reprimanded. Nevertheless, if the information reported about malicious node identification is false, the regular node liability shall be affected severely. The proposed approach evaluates results by considering the expected failure of false alarm (F) and expected gain of genuine reporting action (G_{rep})

Mobile nodes monitor the outgoing data of the neighbour by utilizing the uninhibited environment ofMANET, but the origin of communication disruption cannot be comprehended by them. Such a process is called Neighbour Monitoring in MANETs [70]. Thus, parameters like φ, ψ and δ are used for distinguishing the actions of neighbour nodes in a better way, and such a phenomenon is referred to as Neighbour Surveillance.

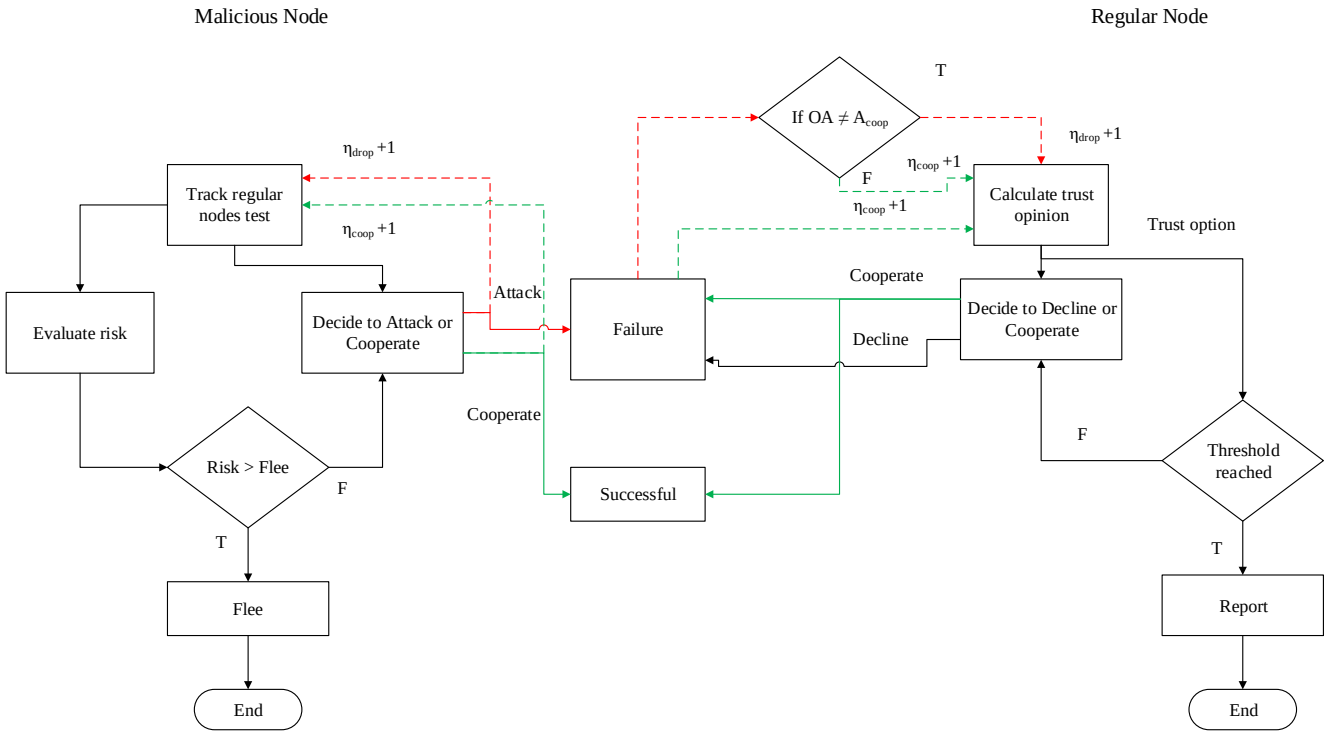

Fig.1. Regular vs malicious node decision-making model.

The proposed framework employs a decision-making model that is a cognitive process resulting in the determination of actions to be performed among the variety of available options. The decision-making model of regular vs malicious nodes in the proposed system has been shown in Fig. 1. The regular node examines the belief option (Op_{belief}) and evidence adequacy (Op_{uncer}) continuously for the competing nodes from feedback received from neighbour monitoring. After each successful communication, the regular nodes raise the η_{coop} by one and the opponents' strategy is checked on communication failure. In case the opponent chose A_{dec} / A_{att}, then η_{drop} would be raised by one else η_{coop} is increased by one. The regular nodes follow a threshold policy for taking the reported decision against the competent node. If the regular nodes fail to reach the threshold, the current belief held by the regular nodes for opponents and the selfishness characteristic for itself determines the cooperate or decline action. Malicious

nodes can also be modelled as rational and as such shall assess its trust factor with regular nodes continuously. A decision rule for fleeing is also followed by the malicious node to avoid being reported. Malicious nodes shall develop attacking frequency so that it becomes tough for regular nodes to determine their type.

In comparison to the existing works, the proposed work involves factors to depict selfishness and collaboration while formulating the node strategies in the game. Table II holds the essential parameters considered in the proposed system.

TABLE II. PARAMETERS INVOLVED IN THE PROPOSED SYSTEM

Actions to be taken by Regular/Malicious nodes	
A_{att}	Attack
A_{cop}	Cooperate
A_{dec}	Decline
A_{flee}	Flee
A_{rep}	Report
Gain and Cost of Actions Adopted	
G_{att}	Gain associated with A_{att}
G_{coop}	Gain associated with A_{coop}
G_{rep}	Gain associated with A_{rep}
C_{att}	Cost associated with A_{att}
C_{coop}	Cost associated with A_{coop}
C_{flee}	Cost associated with A_{flee}
C_{rep}	Cost associated with A_{rep}
List of Opinion Formulation	
Op_{uncer}	Opinion of Uncertainty
$Op_{disbelief}$	Opinion of Disbelief
Op_{belief}	Opinion of Belief
Other Parameters	
F	Failure caused by false alarm
δ	Probability of the node being malicious.
φ	Probability of attack by malicious node
η_{coop}	Quantity of identified A_{cop}
η_{drop}	Quantity of identified A_{att} or A_{dec}
Ψ	Probability of cooperating by regular node

In mobile ad-hoc networks, a node is malicious if it reveals anomalous action which reduces the network performance. In this study, "Bayesian-signaling" (BS) game model is adopted to exhibit the finest actions of selfish strategy and to control the malicious nodes' behavior. This game model can provide secure and reliable communication between the nodes. The scenario is contemplated in this way to deal with the limitations in security in large-scale MANETstaking into account the multi-stage game theory.

This scheme considers the two-player strategy, i.e., sender and receiver, both are involved in the BS game model. Node behavior provides the sender type. The receiver will not observe the nature of the sender. The sender elects to forward the data from a set of possible messages $\{I \rightarrow [i_1, i_2,\ldots i_n]\}$ depending on its behavior type and the receiver notices the message from the sender without realizing the sender type. Then, the receiver selects the possible actions in the set of actions A = {C, D} where C indicates 'cooperate' and D indicates 'decline'. Two players collect the payoff values which depend on sender type; here sender selects the data (message) whereas the receiver chooses the action.

Bayesian-Equilibrium (BE) is a game plan under the BS model which illustrates the following deliberations; like as the sender type (S_t) forward a message $[i^*(S_t)]$ in the set of probability distribution on I. The nodes probability, S_t considersany message 'i' from the set of I while the receiver performs an action from the action sets (i.e., C or D).

Furthermore, the payoff evaluation and belief system update mechanism decide the node strategy. The node strategy can be a BE, mixed, or pure strategy. In pure strategy, node behavior will not be altered whatever the situation, whereas, in mixed strategy, node type can be reformed randomly. The Bayesian equilibrium gives a strategy profile and updates the belief based on the nodes' type. Pure strategy selects an action on the basis of payoff value, whereas mixed strategy revises the belief system for the rest of the nodes. In this approach, relay and sender nodes are considered as malicious nodes. The algorithm that follows reveals the strategy of optimal action for game players.

Algorithm

Input: Sender node (S_n) and Receiver node (R_n)
Output: Find the malicious action
Start.
Init Sender node and Receiver node
Define a profile strategy for S_n and R_n.
Decide the Node type {Regular or Malicious}.
Revisethe S_n and R_n beliefs by applying Bayes rule.
Find optimal payoff value for S_n and $R_n$revised beliefs
Realize the reasonable action {C,D}.
if action not reasonable then
Report to the corresponding nodes as malicious node
else
Determine action C and D
end if
End

A. Multi-Attacker Node Collusion Model

The proposed framework is designed considering the system has incomplete information about the node types, meaning that the user has no control over the behaviour of the attack, the user distributes merely the malicious nodes created within the simulation area. Nevertheless, understanding the working of collusion attacks appears discerning, but the main point is if collusion can be targeted for colossal collateral network damage. Thus, for supporting the huge network damage, innovation has been introduced in the proposed attacker module in the form of auto-coordination among the attacker nodes within the simulation area.

The example given in Fig. 2 shows a malicious node at cluster position CP1 having limited time for performing the coordination after the initiation of the attack and before decamping. Another significant fact involves that the existence of similar belief for two sets of nodes does not imply those nodes are regular.

The regular nodes dominantly cooperate when it comes to communication thus raising the belief. Nevertheless, the cooperation shown by the malicious node is targeted to breach the regular node belief system. Therefore, the temporal analysis of simulation is performed by the system for extracting three crucial parameters – belief, uncertainty and malicious node probability

Evaluating these three terms shall feature the distinction between malicious and regular nodes. Thus, it is highly reasonable to set up a dedicated channel for the communication of malicious nodes under the condition that the three parameters as mentioned above are computed parallelly by another task. From Fig. 2(i), it can be observed that the malicious node at cluster position CP1 can probably communicate with the surrounding attacker nodes CP7, CP6 and CP2. Likewise, after establishing the communication, any of them might extend to the particular neighboring attacker nodes. This phenomenon continues while the cluster ID is stored for avoiding C_{info} redundancy among them. To sum up, it means that the whole communication channel encapsulating every attacker node (with no repetition) shall be compromised as shown in Fig. 2(ii).

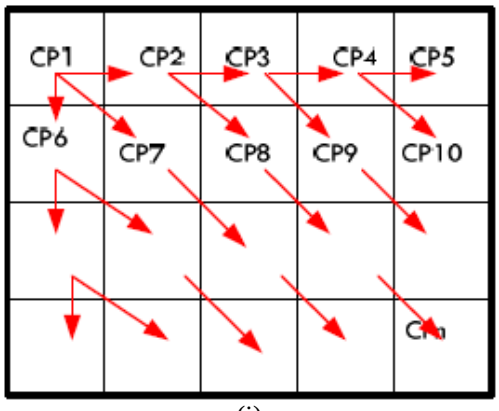

Fig. 2. Example depicting malicious node coordination.

B. Dependencies and Assumptions

The core assumptions of the proposed framework are given below:

i. Malicious nodes can be rational regarding their targets.

ii. Malicious nodes are correctly modeled, i.e., they do not show any indications of selfishness in any game-stage.

iii. Nodes may trace the outgoing packets of their neighbors (network monitoring mechanism) at a one-hop distance through passive observation.

iv. Observation error may arise but with decidedly less probability.

v. An authentication scheme is assumed to exist, and that the identity is confined to the physical node that cannot be faked or changed in the time the node stays in the cluster.

vi. Malicious node is assumed to deport from the cluster where it carried out the attack; it shall also obliterate the entire history of transactions in that cluster with it thereby making the detection process really challenging.

vii. The trust of the mobile nodes cannot be monitored external to the cluster.

viii. Since the proposed study has been performed considering a multi-stage game, thus the time factor is supposed to be classified into slots, and every slot represents the present game stage progress.

ix. Malicious nodes do not perform an attack in the initial game stages for maximizing their utility by decamping the regular node trust factor.

C. Payoff Formulation

For payoffs, the result of the players is presented in the numeric form. It evaluates the performance or utility of the player. The comprehensive procedure for the formulation of payoff is given below:

1. For a regular stranger node, the target shall acquire ‘a’ payoff value when it trusts, where a > 1.
2. For a malicious stranger node attacking the target successfully, it shall result in damage to the target equivalent to ‘a’.
3. If the stranger is suspected by the target node, it shall cost 1.
4. If there is a genuine doubt, the target node shall attain ‘b’ amount of the feedback message, where b lies between 0 and 1.
5. If the trust is not valuable, the target shall lose ‘b’ amount of payoff.
6. If the stranger node is malicious but feigns to be normal as the game proceeds.
7. The stranger node is deemed as the sender, and the target node is considered as the receiver.

The payoffs measure the strategy of players in subsection-A. In the BS game model, C is dominated by a stranger's strategy D because if the end node selects the trust, then the payoff value is 3 while selecting D and 2 when selecting C. If the end node selects doubt, the node receives-1 for D as opposite to 0 for C. Therefore, D is the better result. Likewise, end nodes elect the strategy of doubt dominating trust.

D. Evaluating the Payoffs

In the BS approach, payoffs stimulate the specific players who are performing misbehavior actions that search for the better result of the game.

It can represent cardinal or ordinal payoffs, and payoffs are calculated using a payoff matrix. The decision maker estimates the best outcomes. Dual players are performed in this game model, including S_n and R_n. The sender node selects an action from the set of action space for forwarding the information 'i' to the receiver.

The receiver notices this message 'i' and replies to it by selecting an action from the action set. The receiver does not contain any private message, so it contains a solo type node information. The receiver has a certain previous belief about the type of the sender. Later, the receiver acts; every player is assigned payoffs based on the type of message from the S_n. The receiver acts and chooses a node type for replying the sender. The anticipated payoff integrates the attitude of the player towards a possible danger. Every player obtains a payoff depending on its action as well as its neighbors' actions.

Table III overviews the payoffs of regular as well as malicious nodes. Here, SM stands for 'signaling malicious,' and PS stands for'prefers to send' The predictable payoff is measured as a product probability of the type of node and the payoff of every action selected. If the estimated payoff is high, the matching action is elected as a receiver-action and a sender-action. The sender's predictable utility is a mixture of its payoffs to pure strategy by the receiver.

TABLE III. PAYOFFS FOR REGULAR AND MALICIOUS NODES

Node Type		R Action	
Normal Node	**Malicious Node**	**Co-operate**	**Decline**
SM	SM	0, 0	0, 0
SM	PS	P, 0	p-1, p-1
PS	SM	P, p	P, 0
PS	PS	1, p	-1, p-1

The sender selects only one action - to cooperate (C) or decline (D), depending on the type of the receiver. Since the receiver is considered as a regular node, the actions involve C, D, and report. The decline implies that a node discards participation whereas co-operating in the sense a node makes itself accessible for communication. The sender may conduct a simple dropping packet attack, that is similar to the regular nodes' decline strategy. The sender nodes generate the payoff value from the malicious node, while regular nodes receive no results from D. If the receiver selects a report, it gives the gain SM and if the sender is malicious, regular nodes grow PS from an effective C, where PS and SM are growing for the cooperate and report, respectively. Such nodes may also select (D) decline, that acquires no-cost and zero-gain, even when the opponent opts to attack. The receiver, though, discards the message coming from the sender and also notifies the surrounding nodes if the information from the sender is malicious or regular. The receiver selects the decline action on the basis of the BE strategy.

The sender proposes to suggest sending the message to the receiver. Then, the receiver selects action C or D for the offered message of the sender. Nonetheless, the best response of the receiver is to agree to take a message regardless of the category providing it. This message is not seized in the strategy profile (C, D) since the message set of the receiver is never grasped along that route.

TABLE IV. PERFORMANCE PARAMETERS

Performance Parameters	Values
Simulation Area	(900 x 900) m
Simulation period	1000 sec
Total number of Nodes	50, 85,100, 150
Rate of Transmission	200 m
T_v (Threshold Value)	(0,1)

V. PERFORMANCE ANALYSIS

In this section, the system presents the analysis of the performance of malicious nodes behavior and evaluates both nodes strategies (i.e., regular and malicious) like pure strategy, a mixed strategy, and BE strategy. Table IV represents the parameters list. During this simulation process, almost 40 per cent of nodes are taken as misbehaving. The outcomes of the simulation showed the results of varying level games by comparing with different strategies of regular nodes.

A. Average of Node Utility

The utility of nodes will show the actual value of the payoff of nodes. The average payoff is evaluated by referring to the values of anticipated payoff, that is considered from the payoff matrix. The predictable payoff that integrates the player behavior towards the risk will assess the type of product probability, and each payoff action is selected. If the estimated payoff is high, the neighboring player action is chosen as receiver action and sender action.

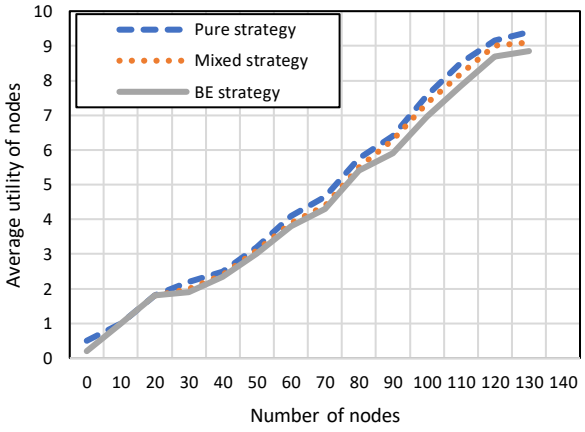

Fig. 3. Assessment of regular node utility under malicious node strategy.

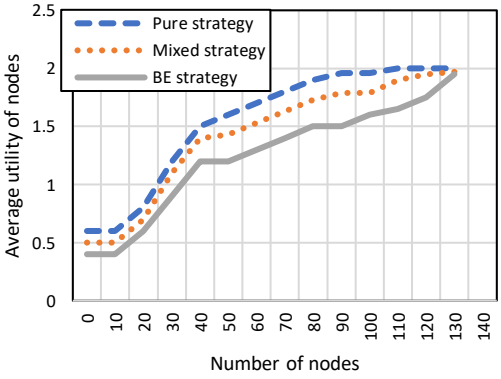

Fig. 4. Assessment of malicious node utility under malicious node strategy.

B. Nodes Strategies

In this study, the system includes three different strategies; such as 1) Pure Strategy, 2) Mixed Strategy and 3) Bayesian Equilibrium (BE) strategy, where nodes select to offer all the players actions. The pure strategy evaluates the player action in every possible achievable situation in the game. While in mixed strategy, such action appears from the distribution. A BE strategy performs with a belief system wherein all the information strategy is an optimum given belief. The selected strategies evaluate the node utility. Fig. 3 and Fig. 4 represent the comparisons of three strategies with nodes utility. In the first comparison, the utility of the regular nodes is maximum when it follows the BE strategy. This is owing to regular nodes, that contains all the possibilities to co-operate with all regular nodes and with a lesser percentage of malicious nodes. While in Fig. 4, it can be observed that the malicious node utility is high. Here, regular nodes can select either pure or mixed strategy; the system decreases the malicious node payoff and drops their utility considerably. In Fig. 4, it is seen that the BE performs efficiently as compared to others when malicious nodes utilize a mixed or pure strategy. Fig. 3 shows the variation of strategies in case of normal nodes. The overall utility of the malicious node is low since it can choose a path to send the packets to the remaining nodes. In the proposed strategy, the normal node can report on malicious node type to other nodes. Finally, the simulation results conclude that the proposed system (BE strategy) is suitable for normal nodes which diminish the utility of malicious nodes.

C. False Positive Rate and Detection Rate of Malicious Nodes

The misdetection rate of normal nodes and the detection rate of malicious nodes of the proposed system were evaluated by comparing it with algorithms in [67] and [71] by running them in various conditions. The results obtained have been illustrated in Fig. 5 and 6.

Fig. 5 depicts the false positive rate of normal nodes and the detection rate of the malicious nodes has been shown in Fig. 6 where the malicious node percentage varies between 10 and 40 per cent. The results depict that the proposed system proved effective in detecting malicious nodes as compared to the algorithms in [67] and [71]. It can be perceivedfrom the figures that the detection rate shows a declining trend with the increase in the malicious node percentage. Nevertheless, the slope in these figures is less steep than the other two algorithms. Furthermore, the detection rate is considerably improved by a better scale than the rest two algorithms.

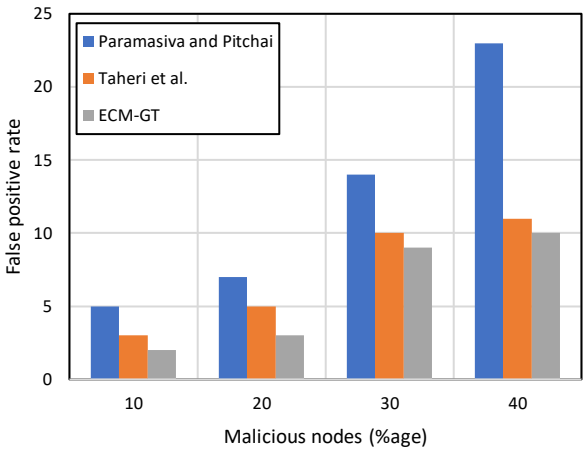

Fig. 5. False positive rate vs percentage of malicious nodes.

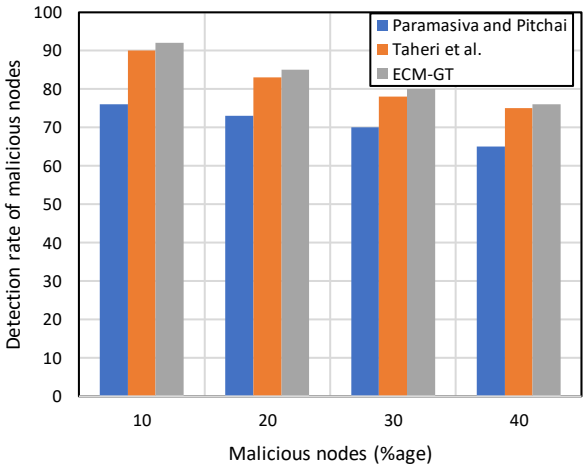

Fig. 6. Detection rate of malicious nodes vs malicious nodepercentage.

D. Throughput and Attack Detection

Other parameters like throughput and percentage of attacks detected, were also measured in every simulation round with the growing percentage of malicious nodes and the results were compared with that of the algorithm in [71].

Fig. 7 displays that the throughput decreased as the malicious node percentage in the network went up. Initially, maximum throughput is attained by the network that is reduced to the lowest level when half of the nodes in the network are malicious. Furthermore, it shows that the proposed system has comparatively better throughput than the system in [71].

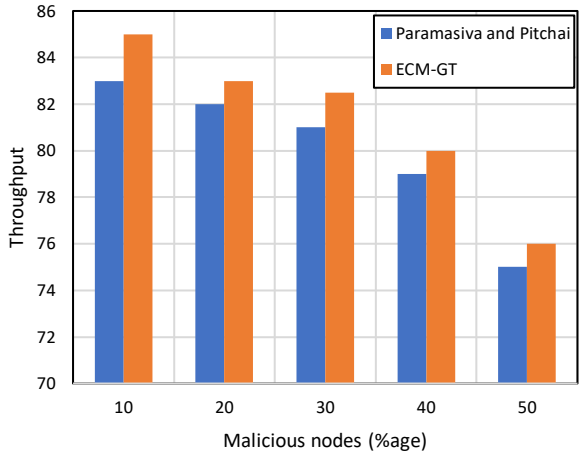

Fig. 7. Throughput vs percentage of malicious nodes.

From Fig. 8, it can be discernedthat the number of attacks detected a decline with the growing number of malicious nodes. When the percentage of malicious nodes is less in the network, all attacks can be sensed by the proposed system unfailingly, but the percentage of attacks detected reduce when half of the network nodes are malicious.

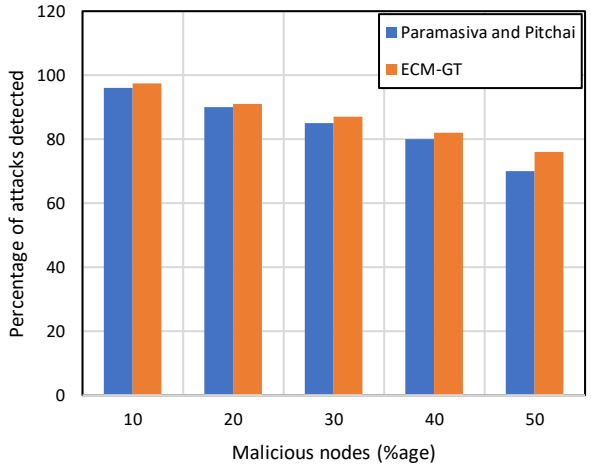

Fig. 8. Percentage of attacks detected vs malicious nodepercentage.

VI. CONCLUSION

This study provides a Bayesian-Signaling (BS) game approach which finds out the malicious actions and behaviors in MANETs. It also provides a solution of the model and generates the threshold values which will be further considered for the designing of a secure routing protocol for MANETs. The BS game model is a type of sub-game which subsequently plays and is regarded as an optimum solution for the detection of malicious attacks. This system considered both regular and malicious nodes for the experimental analysis. If it is a malicious node, the co-operation among the nodes is quite less, and it can worsen the network's performance. Hence, the BS game model was adopted to protect the packet dropping attacks. The regular/normal node in the MANET continuously follows the belief revision process for self-information, then selects the probability to co-operate with its corresponding nodes and considers the BS decision rule to convey the nature of node. The proposed ECM-GT model also examined the strategies of nodes (regular and malicious nodes), and the motive was to diminish the malicious node utility and maximize the utility of regular node by applying Bayesian signaling approach. This system proved better than the existing system and can thus be applied for a safer and more reliable operation in micropayments in the ad-hoc wireless network.

ACKNOWLEDGMENT

This work was partially supported by the Ministry of Higher Education Malaysia (Kementerian Pendidikan Tinggi) under the Fundamental Research Grant Scheme (FRGS) number FRGS19-137-0746 (Ministry Project ID: FRGS/1/2019/ICT03/UIAM/01/2) and Research Initiative Grant Scheme (RIGS) number P-RIGS19-020-0020.

REFERENCES

1. B. U. I. Khan, R. F. Olanrewaju, F. Anwar and A. Shah, "Manifestation and mitigation of node misbehavior in adhoc networks",*Wulfenia Journal*, vol. 21, no. 3, pp. 462-470, 2014.
2. Y. Zhang, J. Zheng and M. Ma eds., *Handbook of research on wireless security*. IGI Global, 2008.
3. Venkataram, *Wireless & Mobile N/W Security*, Tata McGraw-Hill Education, 2010.
4. 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", *Journal of Theoretical & Applied Information Technology*, vol. 77, no. 1, pp. 25-43, 2015.
5. B. U. I. Khan, R. F. Olanrewaju, R. N. Mir, S. H. Yusoff and M. L. Sanni, "Trust and resource oriented communication scheme in mobile ad hoc networks",in *Proceedings of SAI Intelligent Systems Conference*, Springer, Cham, 2016, pp. 414-430.
6. B. U. I. Khan, R. F. Olanrewaju and M. H. Habaebi, "Malicious behaviour of node and its significant security techniques in MANET-a review",*Australian Journal of Basic and Applied Sciences*, vol. 7, no. 12, pp. 286-293, 2013.
7. V. Das et al., *Information Processing and Management*. Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg, 2010.
8. S. Muthumariammal and S. Muthumariappan, "Optimal combined intrusion detection and continuous authentication in high security mobile adhoc network," *Digital Image Processing*, vol. 2, no. 4, 2010.
9. J. Loo, J.L. Mauri and J.H. Ortiz, *Mobile Ad hoc networks: current status and future trends*. CRC Press, 2016.
10. M. Rath and C. R. Panigrahi, "Prioritization of security measures at the junction of MANET and IoT," in *Information and Communication Technology for Competitive Strategies, Proceedings of the Second International Conference on*, ACM, 2016, p. 127.
11. P. Bellavista, G. Cardone, A. Corradi and L. Foschini, "Convergence of MANET and WSN in IoT urban scenarios", *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3558-3567, 2013.
12. R. F. Olanrewaju, B. U. I. Khan, R. N. Mir and A. Shah, "Behaviour visualization for malicious-attacker node collusion in MANET based on probabilistic approach," *American Journal of Computer Science and Engineering*, vol. 2, no. 3, pp. 10-19, 2015.
13. B. U. I. Khan, R. F. Olanrewaju, F. Anwar, A. Najeeb and M. Yaacob, "A Survey on MANETs: Architecture, Evolution, Applications, Security Issues and Solutions", *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 12, no. 2, pp. 832-842, 2018.
14. B. U. I. Khan, R. F. Olanrewaju, M. M. U. I. Mattoo, A. A. Aziz and S. A. Lone, "Modeling malicious multi-attacker node collusion in MANETs via game theory", *Middle-East Journal of Scientific Research*, vol. 25, no. 3, pp. 568-579, 2017.
15. N. Tantubay, D. R. Gautam and M. K. Dhariwal, "A review of power conservation in wireless mobile adhoc network (MANET)," *International Journal of Computer Science Issues*, vol. 8, no. 4, pp. 378-383, 2011.
16. K. Arulanandam and B. Parthasarathy, "A new energy level efficiency issues in MANET," *International Journal of Reviews in Computing*, vol. 1, no. 5, pp.104-109, 2009.

17. G. Singh and J. Singh, "MANET: issues and behavior analysis of routing protocols", *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, no. 4, pp. 219-227, 2012.
18. J. Parvez and M. A. Peer, "A comparative analysis of performance and QoS issues in MANETs," *World Academy of Science, Engineering and Technology*, vol. 48, pp. 937-948, 2010.
19. B. U. I. Khan, R. F. Olanrewaju, N. A. Ali and A. Shah, "ElePSO: energy aware elephant swarm optimization for mobile adhoc network," *Pensee Journal*, vol. 76, no. 5, pp. 88-103, 2014.
20. B. U. I. Khan, R. F. Olanrewaju, A. M. Baba, R. N. Mir and S. A. Lone, "DTASR: dual threshold-based authentication for secure routing in mobile adhoc network," *World Engineering and Applied Sciences Journal*, vol. 7, no. 2, pp. 68-73, 2016.
21. B. U. I. Khan, N. F. Zulkurnain, R. F. Olanrewaju, G. Nissar, A. M. Baba and S. A. Lone, "JIR2TA: Joint Invocation of Resource-Based Thresholding and Trust-Oriented Authentication in Mobile Adhoc Network", in *Proceedings of SAI Intelligent Systems Conference*, Springer, Cham, 2016, pp. 689-701.
22. B. U. I. Khan, R. F. Olanrewaju, A. M. Baba, N. F. Zulkarnain and S. A. Lone, "STCM: secured trust-based communication method in vulnerable mobile adhoc network", in *Robotic, Vision, Signal Processing and Power Applications, 9th International Conference on*, Springer, Singapore, 2017, pp. 149-161.
23. E. Furuncu and I. Sogukpinar, "Scalable risk assessment method for cloud computing using game theory (CCRAM)," *Computer Standards & Interfaces*, vol. 38, pp. 44-50, 2016.
24. A. Talebpour, H.S. Mahmassani and S.H. Hamdar, "Modeling lane-changing behavior in a connected environment: A game theory approach," *Transportation Research Procedia*, vol. 7, pp. 420-440, 2015.
25. J.R. Marden and J.S. Shamma, "Game theory and distributed control,". In *Handbook of Game Theory with Economic Applications*, Elsevier, vol. 4, pp. 861-899, 2015.
26. A.M. Colman, *Game Theory and Experimental Games: The Study of Strategic Interaction*. Elsevier, 2016.
27. C. Adami, J. Schossau and A. Hintze, "Evolutionary game theory using agent-based methods," *Physics of Life Reviews*, vol. 19, pp. 1-26, 2016.
28. M.S. Abdalzaher, K. Seddik, M. Elsabrouty, O. Muta, H. Furukawa and A. Abdel-Rahman, "Game theory meets wireless sensor networks security requirements and threats mitigation: A Survey," *Sensors*, vol. 16, no. 7, p. 1003, 2016.
29. A. Ilavendhan and K. Saruladha, "Comparative study of game theoretic approaches to mitigate network layer attacks in VANETs," *ICT Express*, vol. 4, no. 1, pp. 46-50, 2018.
30. R. F. Olanrewaju, B. U. I. Khan, F. Anwar, R. N. Mir, M. Yaacob and T. Mehraj, "Bayesian Signaling Game Based Efficient Security Model for MANETs", in *Lecture Notes in Networks and Systems series*, K. Arai and R. Bhatia, Ed. Switzerland: Springer, Cham, 2019, pp. 1106-1122.
31. S. Bu, F. R. Yu, X. P. Liu, and H. Tang, "Structural results for combined continuous user authentication and intrusion detection in high security mobile ad-hoc networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 9, pp. 3064-3073, 2011.
32. Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, ACM, 2000, pp. 275-283.
33. S. Eidenbenz, V. S. A. Kumar, and S. Zust. "Equilibria in topology control games for ad hoc networks", *Mobile Networks and Applications*, vol. 11, no. 2, pp. 143–159, 2006.
34. R. S. Komali, A. B. MacKenzie, and R. P. Gilles. "Effect of selfish node behavior on efficient topology design", *IEEE Transactions on mobile computing*, vol. 7, no. 9, pp.1057-1070, 2008.
35. R. Ramanathan and R. Rosales-Hain. "Topology control of multihop wireless networks using transmit power adjustment", *NFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings*, vol. 2, pp. 404-413, 2000.
36. Z. Y. Fang and B. Bensaou. "A novel topology-blind fair medium access control for wireless LAN and ad hoc networks", *IEEE International Conference on Communications, 2003*, vol. 2, pp. 1129–1134, 2003.
37. T. Alpcan and T. Basar. "A game-theoretic framework for congestion control in general topology networks", in *Conference on Decision and control, Proceedings of the 41st IEEE*, vol. 2, 2002, pp. 1218-1224.
38. J. Huang, R. A. Berry, and M. L. Honig, "Auction-based spectrum sharing", *ACM/Springer Mobile Networks and Applications*, vol. 11, no. 3, pp. 405-418, 2006.
39. Z. Ji and K.R. Liu, "Belief-assisted pricing for dynamic spectrum allocation in wireless networks with selfish users," in *Sensor and Ad Hoc Communications and Networks, 2006. SECON'06. 2006 3rd Annual IEEE Communications Society on*, vol. 1, IEEE, 2006, pp. 119-127.
40. Y. Wang, 'A Mean Field Game Theoretic Approach for Security Enhancements in Mobile Ad-hoc Networks', Masters Dissertation. Carleton University, Ottawa, Ontario, Canada, 2014.
41. A. Patcha and J. M. Park, "A game theoretic formulation for intrusion detection in mobile ad hoc networks," *International Journal of Network Security*, vol. 2, no. 2, pp. 131–137, 2006.
42. E. A. Panaousis and C. Politis, "A game theoretic approach for securing AODV in emergency Mobile Ad Hoc Networks," in *Local Computer Networks, 2009. LCN 2009. IEEE 34th Conference on*. IEEE, 2009, pp. 985-992.
43. R.F. Olanrewaju, B.U.I. Khan, A.R. Najeeb, K.N.A.K. Zahir and S. Hussain, "Snort-Based Smart and Swift Intrusion Detection System", *Indian Journal of Science and Technology*, vol. 8, no. 1, pp. 1-9, 2018.
44. F. Li, Y. Yang and J. Wu, "Attack and flee: game-theory-based analysis on interactions among nodes in MANETs", IEEE *Transactions on Systems, Man, and Cybernetics*, Part B (Cybernetics), vol. 40, no. 3, pp. 612-622, 2010.
45. M.D. Serrat-Olmos, E. Hernández-Orallo, J.C. Cano, C.T. Calafate and P. Manzoni, "Accurate detection of black holes in MANETs using collaborative bayesian watchdogs," in *Wireless Days (WD), 2012 IFIP*. IEEE, 2012, pp. 1-6.
46. C.K. Doshi, S. Sankaranarayanan, V.B. Lakshman and K. Chandrasekaran, "Game theoretic modeling of gray hole attacks in wireless ad hoc networks," in *Proceedings of the International Conference on Signal, Networks, Computing, and Systems*, Springer, New Delhi, 2017, pp. 217-226.
47. H.Y. Shi, W.L. Wang, N.M. Kwok and S.Y. Chen, "Game theory for wireless sensor networks: a survey. Sensors," vol. 12, no. 7, pp. 9055-9097, 2012.
48. P. Michiardi and R. Molva, "Analysis of coalition formation and cooperation strategies in mobile ad hoc networks," *Ad Hoc Networks*, vol. 3, no. 2, pp. 193-219, 2005.
49. B. Subba, S. Biswas, and S. Karmakar, "Intrusion detection in Mobile Ad-hoc Networks: Bayesian game formulation," *Engineering Science and Technology, an International Journal*, vol. 19, no. 2, pp. 782-799, 2016.
50. R. S. Komali and A. B. MacKenzie, "Distributed topology control in ad-hoc networks: a game theoretic perspective", *Consumer Communications and Networking Conference, 2006. CCNC 2006. 3rd IEEE*, 2006, pp. 563-568.
51. A. Rachedi, A. Benslimane, H. Otrok, N. Mohammed and M. Debbabi, "A secure mechanism design-based and game theoretical model for manets," *Mobile Networks and Applications*, vol. 15, no. 2, pp. 191-204, 2010.
52. M. M Javidi and L. Aliahmadipour, "Game theory approaches for improving intrusion detection in MANETs," *Scientific Research and Essays*, vol. 6, no. 31, pp. 6535-6539, 2011.
53. H. Janzadeh, K. Fayazbakhsh, M. Dehghan and M. S. Fallah, "A secure credit-based cooperation stimulating mechanism for MANETs using hash chains," *Future Generation Computer Systems*, vol. 25, no. 8, pp. 926-934, 2009.
54. K. Wang and M. Wu, "Nash equilibrium of node cooperation based on metamodel for MANETs," *Journal of Information Science and Engineering*, vol. 28, no. 2, pp. 317-333, 2012.
55. Y. Liu, C. Comaniciu and H. Man, "A Bayesian game approach for intrusion detection in wireless ad hoc networks", in *Proceeding from the 2006 workshop on Game theory for communications and networks*, ACM, 2006, p.4.
56. N. Marchang and R. Tripathi, "A game theoretical approach for efficient deployment of intrusion detection system in mobile ad hoc networks", in *Advanced Computing and Communications, 2007. ADCOM 2007. International Conference on* (). IEEE, 2007, pp. 460-464.
57. Z. Li and H. Shen, "Game-theoretic analysis of cooperation incentive strategies in mobile ad hoc networks", *IEEE Transactions on Mobile Computing*, vol. 11, no. 8, pp. 1287-1303, 2012.
58. Z. Ji, W. Yu, and K. J. R. Liu, "A belief evaluation framework in autonomous MANETs under noisy and imperfect observation: Vulnerability analysis and cooperation enforcement," *IEEE Transactions on Mobile Computing*, vol. 9, pp. 1242-1254, 2010.
59. M. Staudigl, "Co-evolutionary dynamics and Bayesian interaction games," *International Journal Game Theory*, vol. 42, pp. 179-210, 2012.

60. N. Mohammed, H. Otrok, and L.Wang, "Mechanism design-based secure leader election model for intrusion detection in MANET," *IEEE Transactions on Dependable Secure Computing*, vol. 8, pp. 89-103, 2011.
61. M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bacşar and J. P. Hubaux, "Game theory meets network security and privacy", *ACM Computing Surveys (CSUR)*, vol. 45, no. 3, pp. 1-35, 2013.
62. G. Theodorakopoulos and J. S. Baras, "Malicious users in unstructured networks", in *INFOCOM 2007. 26th IEEE International Conference on Computer Communications*. 2007, pp. 884-891.
63. M. Hamdi and H. Abie, "Game-based adaptive security in the Internet of Things for eHealth", in *Communications (ICC), 2014 IEEE International Conference on*, 2014, pp. 920-925.
64. J. Abegunde, H. Xiao and J. Spring, "A dynamic game with adaptive strategies for IEEE 802.15. 4 and IoT", in *Trustcom/BigDataSE/I SPA*, 2016, pp. 473-480.
65. V. H. La and A. R. Cavalli, "A misbehavior node detection algorithm for 6LoWPAN Wireless Sensor Networks", in *Distributed Computing Systems Workshops (ICDCSW), 2016 IEEE 36th International Conference on*, 2016, pp. 49-54.
66. D. Das, K. Majumder and A. Dasgupta, "Selfish node detection and low cost data transmission in MANET using game theory", *Procedia Computer Science*, vol. 54, pp. 92-101, 2015.
67. Y. Taheri, H.G. Garakani and N. Mohammadzadeh, "A game theory approach for malicious node detection in MANETs", Journal of Information Science and Engineering, vol. 32, no. 3, pp. 559-573, 2016.
68. B. Rajkumar and G. Narsimha, "Trust based certificate revocation for secure routing in MANET", *Procedia Computer Science*, vol. 92, pp. 431-441, 2016.
69. J. Sengathir and R. Manoharan, "Security algorithms for mitigating selfish and shared root node attacks in MANETs", *International Journal of Computer Network and Information Security*, vol. 5, no. 10, pp. 1-10, 2013.
70. K.S. Win, "Analysis of detecting wormhole attack in wireless networks," in *Proceedings of World Academy of Science: Engineering & Technology*, 2008, p. 48.
71. B. Paramasiva and K. M. Pitchai, "Modeling intrusion detection in mobile ad hoc networks as a non cooperative game", in *Pattern Recognition, Informatics and Mobile Engineering (PRIME), 2013 International Conference on*, pp. 300-306.

AUTHORS PROFILE

Burhan Ul Islam Khan is a PhD Scholar and Teaching Assistant at the Department of Electrical & Computer Engineering, International Islamic University Malaysia. He received B.Tech. in CSE from IUST, Kashmir, and MS in CIE from IIUM, Kuala Lumpur during 2011 and 2014 respectively. Before commencing his Ph.D., he has been involved in varying roles as that of Software Engineer, Research Analyst and Assistant Professor. His current research interests include Formulation of Bio-Inspired optimization models in IOT, Designing One Time Password Schemes, Employing Mechanism Design, and Game theory to protect ad-hoc networks.

Rashidah Funke Olanrewajuis a Nigerian citizen, born in Kaduna, Nigeria. She received the BSc. Hons degree in Software Engineering from the University of Putra Malaysia, in 2002, and the MSc and PhD degrees in Computer & Information Engineering from the International Islamic University Malaysia (IIUM) Kuala Lumpur, in 2007 and 2011, respectively. She is currently an Associate Professor at the Department of Electrical and Computer Engineering, International Islamic University Malaysia where she is leading the Software Engineering Research Group (SERG). She is an executive committee member of technical associations like IEEE Women in Engineering, Arab Research Institute of Science and Engineers, etc. She represents her university, IIUM, at Malaysian Society for Cryptology Research. Her current in hand projects revolve around: MapReduce Optimization Techniques, Compromising Secure Authentication and Authorization Mechanisms, Secure Routing for ad-hoc networks, Formulating Bio-Inspired Optimization Techniques.

Dr. Farhat Anwar received a PhD degree in Electronic and Electrical Engineering from the University of Strathclyde UK in 1996. His research interest includes QoS in IP networks, routing in Ah-hoc and sensor networks, computer and network security, network simulation and performance analysis, IoT, and biometrics. He has published extensively in international journals and conferences. He has been with IIUM since 1999 and currently working as a Professor in the Department of Electrical and Computer Engineering.

Roohie Naaz Miris a Professor & HoD in the Department of Computer Science & Engineering at NIT Srinagar, India. She received B.E. (Hons) in Electrical Engineering from University of Kashmir (India) in 1985, M.E. in Computer Science & Engineering from IISc Bangalore (India) in 1990 and PhDfrom University of Kashmir, (India) in 2005. She is a Fellow of IEI and IETE India, senior member of IEEE and a member of IACSIT and IAENG. 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, security and routing in wireless ad-hoc and sensor networks.