Project ID/Title: RIGS17-048-0623/STRATEGIC PROFILING & ANALYTIC MODELLING OF NODE MISBEHAVIOR IN MANET BASED IOT PARADIGM THEORY

Project Sponsor: Ministry of Higher Education Malaysia (Kementerian Pendidikan Tinggi) under Research Initiative Grant Scheme

Author Name(s): Asst. Prof. Dr. Athaur Rahman Bin Najeeb
Assoc. Prof. Dr. Rashidah Funke Olanrewaju

Department/Kulliyyah: Electrical & Computer Engineering/KOE

Abstract

Ubiquitous Computing and Internet of Things (IoT) are extremely popular in recent age and therefore imparting high level security mechanism is highly indispensable for such advanced technical systems. Game Theory acts as a suitable tool offering promising solutions to security-related concerns in Mobile Ad-Hoc Networks (i.e., MANETs). In MANETs, security forms a prominent concern as it includes nodes which are usually portable and require significant coordination between them. Further, the absence of physical organisation makes such networks susceptible to security breaches, hindering secure routing and execution among nodes. Coordination among nodes during communication and working without control of any central manager truly ensembles them to be applied in IoT. However, the identification and later mitigation of malicious nodes becomes an immensely difficult task especially when Selfish/Erroneous nodes exist along with normal Collaborative nodes in the Regular camp. Game Theory approach has been manipulated in the current study to achieve an analytical view while addressing the security concerns in MANETs. This study considers selfish nodes in the regular node camp while modelling the Regular versus Malicious node game and thereby enhancing the prior mathematical schema of strategical decision making to accommodate for the same. The proposed study performs statistical analysis and presents a mathematical model to mimic the multi-stage game between regular and malicious node using Game Theory. The simulation of the model has proved that the Perfect Bayesian Equilibrium outshines other approaches used in this study, specifically pure strategy and mixed strategy. The utility of both regular and malicious node has improved noticeably when nodes adopt PBE strategy. The framework tries to effectively represent the various unpredictable actions of node cooperation, node declination, node attacks as well as node reporting that can model the strategic profiling of various mobile nodes. Understanding the patterns and then deploying the algorithms in security products can reduce intrusion to a greater extent.

Key words

Internet of Things (IoT), Routing Security, Game Theory, MANET, Malicious attacker nodes

Table of Contents

1. Introduction 1
   1.1. Problem Statement 3
2. Background 4
3. Objectives 7
4. Methodology 7
5. Findings 10
   5.1. Average of Node Utility 10
   5.2. Nodes Strategies 10
   5.3. False Positive Rate and Detection Rate of Malicious Nodes 12
   5.4. Throughput and Attack Detection 13
6. Conclusion 14
7. Output 14
8. Future Plan of the Research 15
9. References 15

1. Introduction

In the modern era of networking and communication system, mobile adhoc network has increasingly attracted many researchers for its potential benefits in the line of infra-structure free communication system. A mobile adhoc network (MANET) consists of various independent wireless devices that can move at any direction. Each node is considered as a router and hence MANET is completely infrastructure-free networking system. MANET system can be considered as advanced version of wireless networking hence; it is also shrouded by all the issues that any wireless networking system may possess. Within a MANET, the entire communication system between the mobile nodes takes place in wireless environment thus extremely susceptible to vulnerabilities that are applicable in any wireless networking system. Mobile nodes are treated as routers so there doesn't exist any infrastructure, further they can move in any direction at any unpredictable time thereby mapping the topology of a MANET as of dynamic type [1]. The significance of the transmission happens in MANET system due to existing neighbouring nodes that play a pivotal role in forwarding data packets. Usually, the mobile nodes that come in transmission range of each other are termed as neighbour nodes [2]. When the mobile nodes are required to forward data packets to any of the non-neighbouring nodes, the MANET system takes the aid of series of multiple hops where the intermediate nodes behave as routers in it [3].

One of the biggest networking issues in MANET is that its transmission range as well as sensing range highly differs as the network consists of numerous. types of wireless nodes with various IEEE standards connected with each other. For this reason, the transmission boundaries are hard to be seen or defined. This is the gateway for entries of all the security breaches that may possibly occur in MANET as the wireless communication channel is highly unguarded from any types of external signals in less reliable wireless medium [2]. Moreover, as the nodes arbitrarily move hence, it often results in either portioned nodes or link breakage on the cost of communication channel established. Such issues not only give rise to QoS issues like bandwidth issues, energy issues, routing issues, but also such issues easily welcome all types of possible attacks on the MANET system. The security of the MANET system is shrouded with various security loopholes e.g. absence of infrastructure, resource limitation, restricted physical security, and more importantly the dynamic topology. It has already been seen in the

prior work [4-6] that cryptographic techniques are frequently considered and prioritized in majority of the security approaches in MANET. In sturdy association with mathematical theories, cryptographic techniques are quite challenging to design without enough researches and excavating the security analysis of MANET [5]. One of the easiest ways to find feasible solutions for accomplishing security in MANET is to explore the prior research work that claims cryptographic techniques as a solution for security. The prime aim of adopting such a step will be to accomplish a better security solution that is computationally efficient and can guarantee scalability, network performance, storage etc. As the schema of object-oriented programming can be preferably discussed using software engineering design patterns [5], similarly, cryptography is adopted very frequently in majority of the prior research to discuss secure framework that can address network breaches in MANET. Majority of the work illustrating cryptography as a solution was seen to address various attacks and mitigation techniques [7] and secure routing protocols in MANET [8]. However, it is quite challenging to decide whether cryptographic techniques should be encouraged much in next generation of research work in securing MANET system. The prime reason behind this is higher computational complexity associated with advanced cryptographic techniques.

Unfortunately, the presence of such vulnerable features of MANET permits intruders to perform malicious activity in the network where the feasibility of detection of the intruder is extremely less due to decentralization format of the network topology in MANET [9]. The cost of such attacks and intrusion has to be paid by the genuine mobile nodes where their communication system is sabotaged very badly affecting the final application performance, loss of data, eavesdropping, and massive intrusion. Further from review of literature, it can be established that solutions based on routing protocols are abundantly higher even as a part of security based techniques used in MANET, however, it should be clearly understood that purely emphasizing on the routing based approach can overlook the malicious behaviour in large scale MANET applications as various factors like node behaviour, dynamics of strategies adopted on different types of nodes are quite complex to be solved when routing approach is mechanized [10]. Although there are many ranges of issues that has been discovered in the past few decades in the area of MANET e.g., power issues [11,12] routing issues [13], QoS issues [14], but the issues pertaining to security are still unsolved [9,10]. While there is massive volume of research work that can be witnessed from some of the major publishers, but still one

efficient system ensuring proper and failproof security is yet to be seen and standardized for future security protocols.

1.1. Problem Statement

The uncertain scenario of selection by routing protocols for communication system in MANET gives rise to one of the peak security issue i.e. authenticating genuine or malicious nodes. This is due to the absence of integrated digital certificate-based node verification system between two mobile nodes in MANET. The presence of such malicious node is potentially harmful to any MANET application and has widespread damage of the computing resources connected in MANET. There are almost multiple numbers of attacks that have been recorded at almost every layer i.e. transport, application, network, data link or MAC, and physical [15]. This basically states that MANET is more vulnerable to different types of attacks that disrupt the trust and reputation system existing among the mobile nodes. The cost of attack scenario is much worse when the network is considered for larger dimension such as IoT environment.

While performing the preliminary study of the proposed system, it was known that large amount of previous study has emphasized on usage of cryptographic protocols to secure MANET, where implementation becomes a big question mark and challenges time and space complexity of those sophisticated algorithms [5]. Majority of the work done till date is focused on Intrusion Detection System (IDS) or more focused on detection of malicious node, however, the proposed study does not attempt to create any IDS or try to identify malicious because one or the other way, the attackers are smart enough to bypass the designed security [16].

The proposed study attempts to design a mathematical model that captures the actual pattern of malicious activities in MANET based on probability theory as well as considering presence of erroneous/selfish nodes among the regular nodes. The scenario is considered in this way to address the loopholes of security in large scale MANET considering multi-stage game theory. Understanding the pattern and then deploying the algorithms in security products will reduce the intrusion or malicious behavior to a greater extent. Evaluating the pattern can give an empirical finding about the feasibility of various events (good or malicious activities) of a mobile node that can actually exhibit lots of hidden traits of the strategies adopted by mobile nodes (that may be regular or malicious). Therefore, providing solution as mitigation

techniques can be designed precisely based on actual analysis of the behavior of the malicious nodes in MANET.

2. Background

MANET in the IoT perspective can be designated as a group of smart machines capable of communicating self-sufficiently even in absence of any centrally governing infrastructure and this network is progressively prominent in transmission of future smart peripheral procedures in Internet of Things. Research is going on by MANET work group for systematizing secure routing conventions for such type of IoT empowered MANETS. At the present, MANET based Routing protocols have their own margins; therefore, designing advanced routing protocols is very much indispensable for securing MANETS since the Mobile MANET Smart devices have to concurrently operate as intermediary nodes for forwarding, routers, data sources and endpoints. Maintaining Quality of service for IoT applications is a challenging task as well. Moreover, the interest of the research community in security games has consistently increased during the last years since they provide a quantitative framework for modeling the interactions between malicious users and defense systems. The previous record of studies concerned with the mitigation of misbehavior problem of nodes in MANET environment has been tabulated in Table 1. Although such techniques are quite successful in formulating tactics for managing selfish nodes in the environment of MANET, however, same couldn't successfully accomplish the ultimate effective routing policies and maximize QoS throughput. Further, this section also discusses about the literature which specifically employs Game Theory as a tool while securing MANETS.

Table 1. Summary of the findings

AUTHOR	CONTRIBUTION	RESULT OBTAINED	LIMITATIONS
(Wang et al., 2014) [17]	Proposed Mean Field Game Theoretic Approach for security enhancements in	-Significantly improves the lifetime of MANET and reduces the	-Scenario of multiple attackers and multiple defenders not taken into account

	Mobile Ad hoc Networks	compromising probability -Enables an individual node in MANET to make distributed security defense decisions	
(Hamdi and Abie, 2014) [18]	Proposed a model based on game theory for IoT adaptive security emphasizing on e-Health applications	- Extends the smart-things' lifetime by 47% in comparison to the existing models - Strikes a balance between energy-efficiency and security-effectiveness	- Simulated on limited threat scenarios only
(Abegunde et al., 2016) [19]	Presented a dynamic game for IEEE 802.15.4 and IoT in which nodes can select and adapt their strategies of play according to the 'state of the game' and their energy level	- Better performance and security over the default IEEE 802.15.4 access mechanism - Improvement in utility, and fairness in channel sharing, as well as efficiency in energy usage	- Proposed model does not account for the reality of variation in the loads level
(La and Cavalli, 2016) [20]	Presented a node misbehaviour detection algorithm by employing weighted-link in a hierarchical	- Supported by some experiments in the real platform displaying promising results with lesser false positives and no false negatives	- Mobility of nodes has not been considered - Vulnerable to some complicated attacks/intrusions in application and network layer

	6LoWPAN sensor network		
(Das et al., 2015) [21]	Put forward a new game theoretic approach for selfish node detection in MANET	- Guarantees the least idle time and secure low-cost data transfer	- Presence of malicious nodes has not been considered
(Taheri et al., 2016) [22]	Presented an approach for detecting malicious nodes using Game Theory	- Showed better efficiency in malicious node detection and lesser false positives than previous algorithms	- Multiple attacker-defender scenarios have not been considered
(Rajkumar and Narsimha, 2016) [23]	Proposed a CA distribution and Trust-based threshold revocation mechanism to enhance MANET security	- Eliminates misbehaving nodes - Simulation revealed better delivery ratio, resilience and packet drop	- Network overhead, inaccuracy, and slow revocation issues
(Sengathir and Manoharan, 2013) [24]	Developed a security add-on for Multicast Ad-hoc On-Demand Distance Vector protocol	- Effective in the detection of misbehaving nodes	- No clear distinction between Malicious and Selfish nodes. - Malicious nodes have been modeled as fragile. - Cannot be applied to other routing protocols

3. Objectives

The prime aim of the proposed study is to perform a statistical analysis and thereby design a mathematical model that illustrates the tussling among regular and malicious nodes under diverse vulnerable security condition taking into account the disagreement in node cooperation by the selfish / erroneous nodes within the regular camp. The specific objectives are following:

1. To design a strategic decision-making mathematical model using game theory considering the tactics adopted by regular node, selfish node, and malicious node and thereby design the game specification.
2. To conduct a critical review into various sets of the prior research works done in the area of security system in mobile adhoc network that pertains to the misbehavior problems of the mobile nodes to discuss the prominence of open issues in the same.
3. To assess the complexity of node misbehavior by simulating the disagreement in node cooperation due to selfishness along with malicious node attacks in multiple levels of game and formulate the condition of belief system when the nodes chooses to cooperate, or decline, or initiate attack in the considered environment of MANET.
4. To formulate the assessment parameters that results either in attack or in deporting mechanism to other clusters in order to study the decision level of the mobile nodes and perform extracting the information related to the condition of decision model for regular nodes to report and update the MANET and attacker node to deport from the attacked cluster.
5. To conduct a comparative performance analysis, considering the prior work with the proposed system with respect to evaluation of detected false positives, the utility of regular and malicious node, throughput and attack detection.

4. Methodology

The developed model is based on Game Theory approach. There are few different methods that are going to be illustrated which include pure strategy, mixed strategy, and Perfect Bayesian Equilibrium. The efficiency of a chosen set of actions depends on the chosen strategy

to be adopted. The developed model suggests set of actions to be taken by a node, while following the probabilistic approach that game theory offers. The system depicts both regular nodes, and malicious to have rational nature. This implies that each type of node will look to get the most out of each situation. The developed model considers the presence of selfish nodes which are defined as regular nodes that encounter power, bandwidth, or other resource limitations that caused them to act selfishly.

The process flow diagram for the proposed system is given in Figure 1. The past research works in this domain [19] have failed to take into account the feasibility that diverse threat frequencies may be chosen by an intruder towards diverse adversaries, but the proposed study takes into consideration more sophisticated and smart malicious nodes thus causing the competition between malicious and regular nodes to be more realistic. The framework proposed has classified the malicious/regular nodes by making use of a multi-phase strategy i.e. virtual competition for finding the optimal scheme of malicious and regular nodes to compute general decision-making process. The Decision-Making model is formed to act as the brain of each type of node in the network. It is responsible for determining when to carry out a set of actions depending on the situation the node finds itself in. This is done by following a system that keeps record of the previous interactions of neighbouring nodes. The regular node is assisted by the neighbouring surveillance strategy for receiving feedback from the adjacent neighbouring nodes at that time and also computing the adequacy and trust of proof towards conflicting nodes based on the number of attacks on routing and the identified cooperation. A threshold schema is incorporated in the proposed system for choosing the rating of nodes in the logical region as malicious or not. If the node is not rated as malicious, then regular node opts to provide probability support based on the level of trust. Other than this, malicious nodes estimate the risk to get caught in their present locations; therefore, they follow their protocol for deciding whether or not they should decamp to some other logical region. The malicious node decides to attack if the node does not decamp to some other region. The most significant issue in such a decision process is to work out deciding rules for regular as well as malicious nodes consequent with the event profiles given away by the probability of cooperation by regular nodes or probability of attack by the malicious node. Moreover, the system identifies the events and best possible decision protocols by analysing the mobile adhoc network when the framework desiring to attain Perfect Bayesian Equilibrium is deployed. The proposed

system incorporates a multi-collusion-based attacker model in which attacker nodes cooperate with each other in order to conduct attacks.

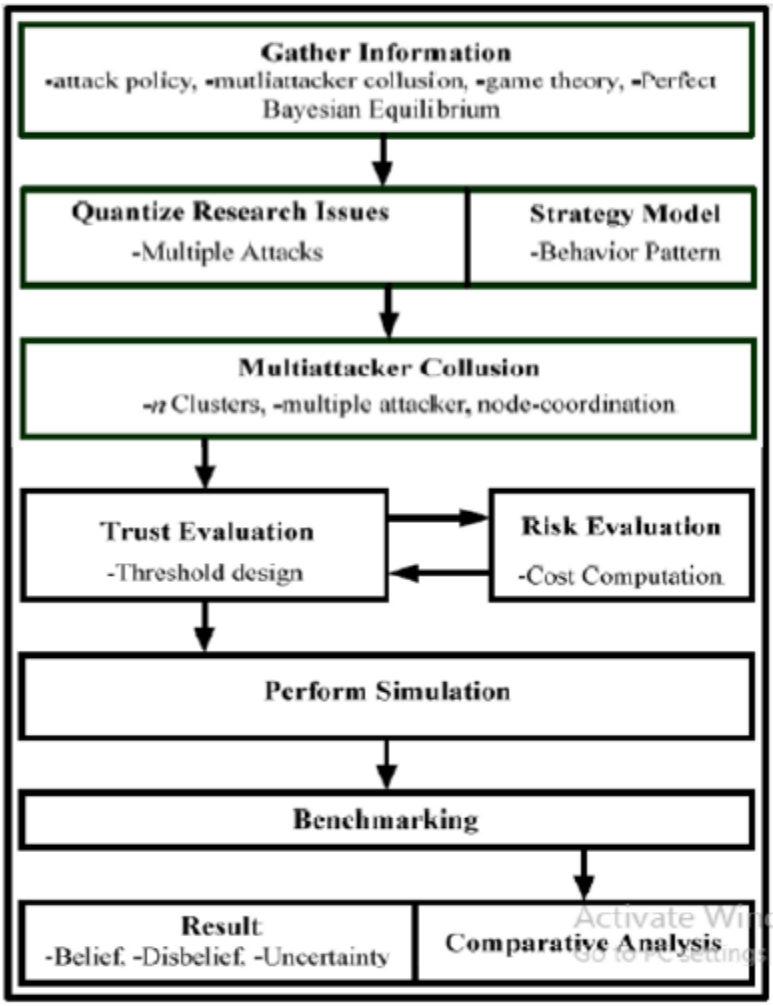

Figure 1. Process Flow of the Research

The simulation is being carried out for four different combinations, thus giving rise to four scenarios as described below:

Scenario-1: This scenario considers the prior decision-making model in completely collaborative environment.

Scenario-2: This scenario considers proposed decision-making model in completely collaborative environment.

Scenario-3: This scenario considers prior decision-making model in partially collaborative environment.

Scenario-4: This scenario considers proposed decision-making model in partially collaborative environment.

Completely collaborative environment means all nodes within the regular nodes are always collaborative; selfishness is never exhibited by regular nodes (*SF* for all regular nodes = 0). Partially collaborative environment portrays a situation wherein regular nodes may choose to behave selfishly at some point of time in the game i.e. (*SF* for all regular nodes ≠ 0).

5. Findings

The results accomplished in this study are the outcome of the collective evaluation of i) Pure Strategy, ii) Mixed Strategy, and iii) PBE strategy. The evaluation is performed under a controlled research environment where every simulation parameter has played a significant role in furnishing the results from various scenarios however the simulation parameters were kept constant for all of the four scenarios for the purpose of comparison. Hence, the accomplished results can be further debated as below:

5.1. Average of Node Utility

The node utility shall display the real values of node payoffs. The average payoff can be computed by considering the expected payoff values that are taken from the payoff matrix. The expected payoff incorporating the behaviour of players towards danger shall examine the category of product probability, and thus every payoff action shall be chosen.

5.2. Nodes Strategies

In the present study, three diverse strategies are included viz. i) pure, ii) mixed and iii) Bayesian Equilibrium, where nodes choose offering actions to all the players. The strategies chosen assess the utility of nodes. The comparison of these strategies with the utility of nodes has been shown in Figure 2 and 3. The regular nodes' utility is maximum when BE strategy is followed in the first comparison. This is due to the presence of regular nodes that hold all the chances of cooperating with every regular node and with a lower proportion of malicious nodes. From Figure 3, it is evident that the utility of malicious nodes is high. In this case, the regular nodes

may choose either mixed or pure strategy; the payoff of malicious nodes is reduced, and their utility drops considerably. Also, it can be observed from Figure 3 that BE shows efficient performance in comparison to others when malicious nodes employ a mixed or pure strategy. The outcome from the simulation reveals that the presented system using BE strategy is apt for normal nodes that lower the malicious node utility.

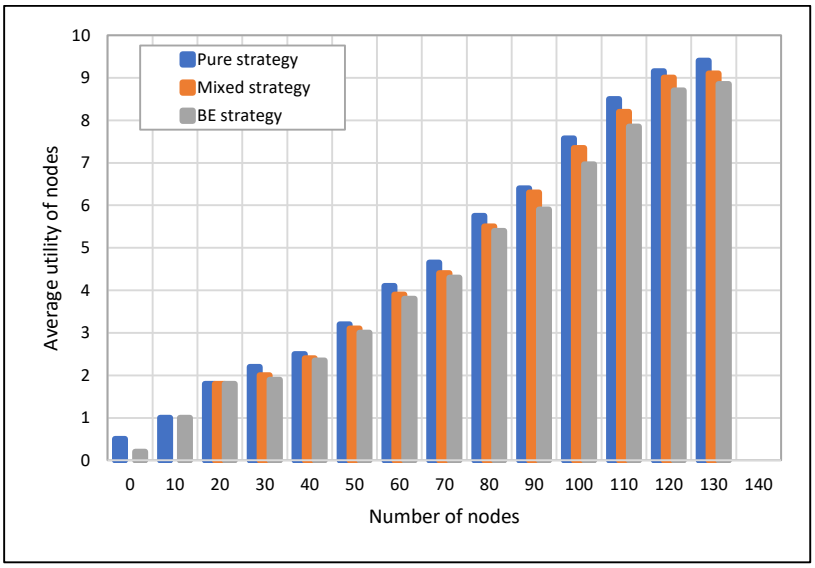

Figure 2. Comparison of Regular Node Utility Under a Malicious Node Strategy

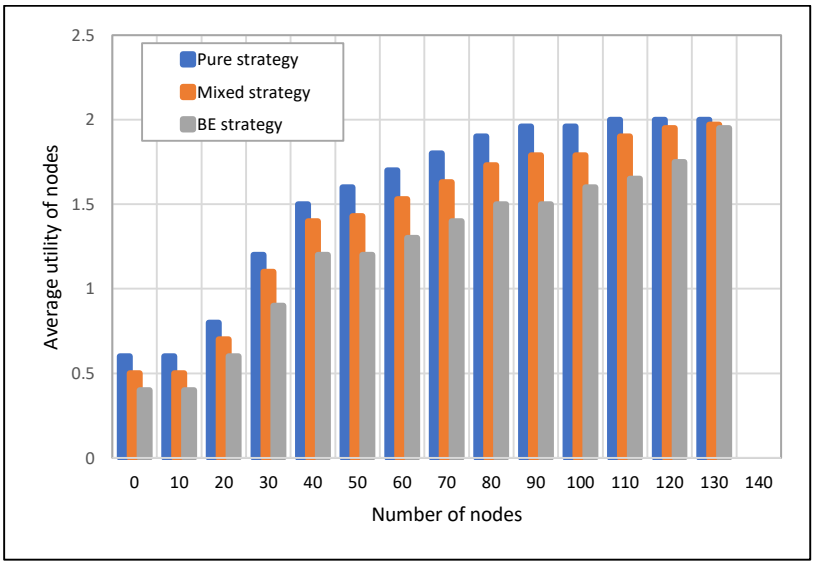

Figure 3. Comparison of Malicious Node Utility Under Malicious Node Strategy

5.3. False Positive Rate and Detection Rate of Malicious Nodes

The malicious node detection rate and normal node misdetection rate in the proposed system have been examined after their comparison with the algorithms presented in [22] and [25] when run under changing conditions. The results achieved have been displayed in Figure 4 and 5.

The regular nodes' false positive rate (FPR) and the malicious nodes' detection rate have been exhibited in Figure 4 and Figure 5 respectively, with the percentage of malicious nodes ranging between 10 and 40. The results attained show the effective performance of the proposed system in malicious node detection in comparison to algorithms [22] and [25].

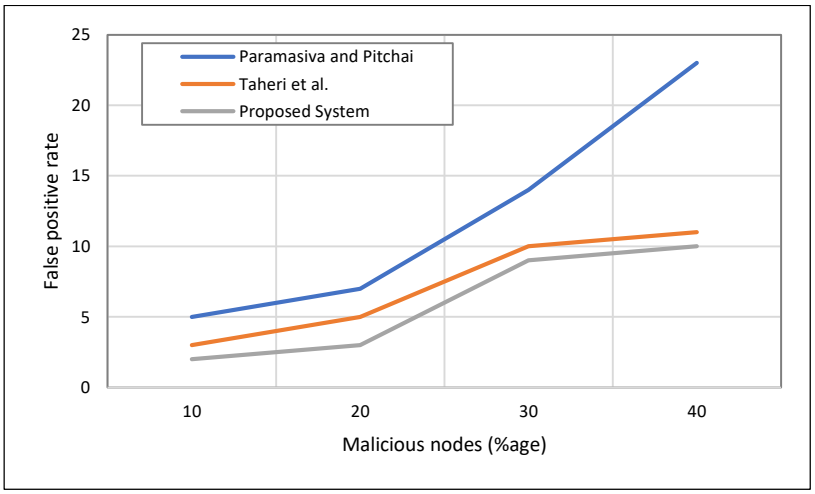

Figure 4. False Positive Rate vs Percentage of Malicious Nodes

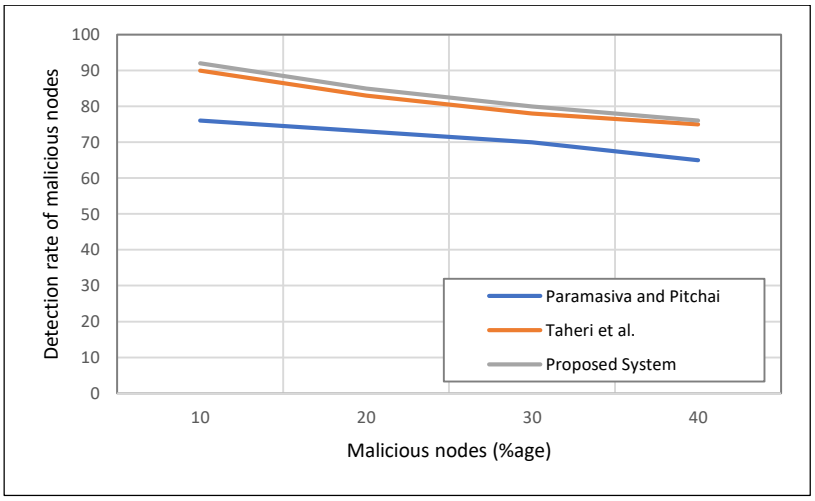

Figure 5. Detection Rate of Malicious Nodes vs Percentage of Malicious Nodes

5.4. Throughput and Attack Detection

Parameters such as attack detection percentage and throughput were also examined in each simulation round as the percentage of malicious nodes rose, and the outcome was contrasted with the algorithm in [25].

From Figure 6, it is seen that the throughput drops with the growing percentage of malicious nodes in the network. This suggests the better throughput obtained in the proposed system as compared to the system in [25]. Further, Figure 7 depicts the decline in attack detection as the malicious node percentage grows.

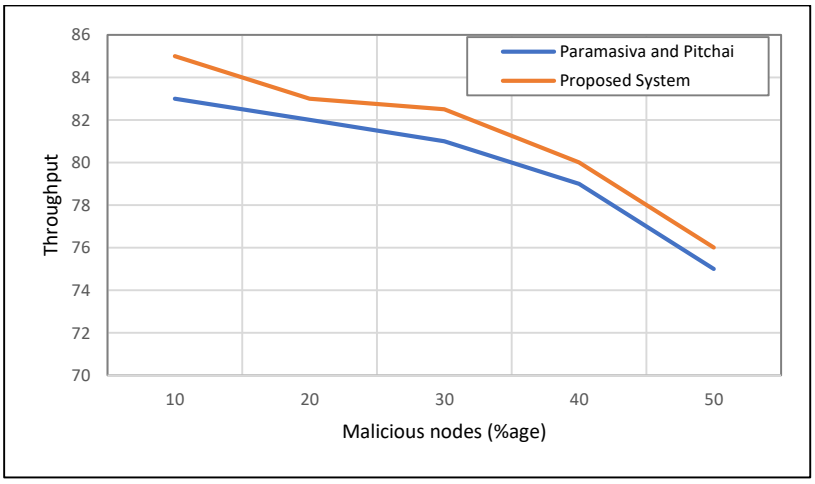

Figure 6. Throughput vs Percentage of Malicious Nodes

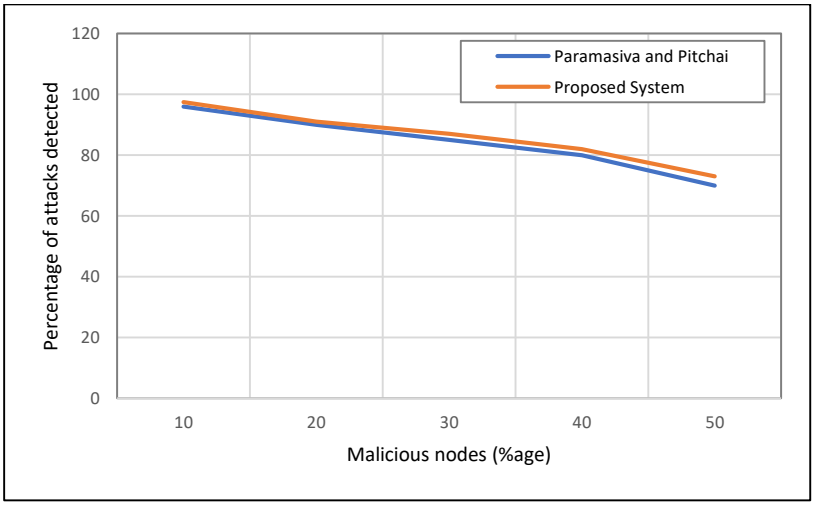

Figure 7. Percentage of Attacks Detected vs Percentage of Malicious Nodes

6. Conclusion

The framework presented in this study has been conceived as virtual competition that is mapped with expected strategies so that it can be used for updating by regular node and attacking by malicious node employing Perfect Bayesian Equilibrium. The simulation results have shown improved accuracy for capturing malicious nodes, with respect to their behaviour at all stages and their strategy for decamping to some other logical region. The proposed study has been able to identify some computationally challenging task related to the security of MANETs by employing game theory for the analysis of behavioural patterns of different kinds of nodes in a MANET. The proposed system is able to demonstrate the motivation behind the behaviour adopted by the nodes taking into account malicious as well as regular nodes. The efficiency of the framework proposed can be owed to the employment of Perfect Bayesian Equilibrium in order to understand the impact of several empirical parameters (such as payoff, belief, cooperation/attack, uncertainty, etc.) that are evaluated during the simulation process. It is understood that the results obtained can further lead to research works in this domain for effectively addressing the modelling of malicious node activities in MANETs.

7. Output

1. Formulation of a Bayesian game framework to study the strategy of collaborative, selfish/erroneous and malicious nodes in MANETs.
2. A comprehensive evaluation of various sets of prior research works done in the area of security system in mobile adhoc network that pertain to the misbehaviour problems of the mobile nodes and latter deducing open issues from the same.
3. Proposition of decision rules for regular nodes to report and malicious nodes to depot, which comply with the sequential rationality requirement.
4. Comparison of Equilibrium strategy profiles for different types of nodes to reveal the hidden connection between a mobile nodes best response and cost and gain of each individual strategy.
5. Patent on the novel framework that illustrate the rationale behind the node's adopted behaviour considering regular, selfish, erroneous and malicious nodes within the

MANET environment; thus, validating itself as a feasible non-cryptographic solution for securing deployed adhoc networks.

8. Future Plan of the Research

Currently, the proposed system doesn't consider the detection or identification of a specific malicious nodes present in the simulation environment. Nevertheless, it extracts cumulative and quantified empirical results of the malicious behaviour. However, combining the proposed model with an existing credit-based approach can lead to the formation of a non-cryptographic Intrusion Detection System which would solve major security hurdles in continual deployment of IOT.

In future, further pattern of behaviours based on machine learning process can be evolved for mitigating effect of malicious node by distinguishing nodes as collaborative, selfish and malicious with the MANET system. In order to have real time adoption, many possible game scenarios should be developed, and the pattern-based machine learning mechanism should be adopted to mitigate the effect of malicious node effect in real time scenario.

9. References

[1] I. Chlamtac, M. Conti and J. Liu, "Mobile ad hoc networking: imperatives and challenges", *Ad Hoc Networks*, vol. 1, no. 1, pp. 13-64, 2003.

[2] S. Basagni, M. Conti, S. Giordano and I. Stojmenović, *Mobile ad hoc networking*. Piscataway, NJ: IEEE Press, 2004.

[3] S. Hu, Multicast Routing Protocols in Mobile Ad Hoc Networks. ProQuest, 2008.

[4] P. Visalakshi and S. Anjugam, "Security issues and vulnerabilities in Mobile Ad hoc Networks (MANET)-A Survey", *International Journal of Computational Engineering Research*, pp. 189- 194, 2015.

[5] J. Chen and J. Wu, "A Survey on Cryptography Applied to Secure Mobile Ad Hoc Networks and Wireless Sensor Networks", in *Handbook of Research on Developments and Trends in Wireless Sensor Networks: From Principle to Practice*, 5th ed., IGI Global, 2010

[6] J. Cordasco and S. Wetzel, "Cryptographic Versus Trust-based Methods for MANET Routing Security", *Electronic Notes in Theoretical Computer Science*, vol. 197, no. 2, pp. 131-140, 2008.

[7] B. Wu, J. Chen, J. Wu and M. Cardei, "A survey of attacks and countermeasures in mobile ad hoc Networks", in *Network Security*. Springer US, pp.103-135, 2007.

[8] M. O. Pervaiz, M. Cardei and J. Wu, "Routing security in ad hoc wireless networks", in *Network Security*. Springer US, pp.117-142, 2010.

[9] S. Khan and A. Khan Pathan, *Wireless networks and security*. Berlin: Springer, 2013.

[10] B. U. I. Khan, R. Olanrewaju and M. H. Habaebi, "Malicious Behaviour of Node and its Significant Security Techniques in MANET-A", *Australian Journal of Basic and Applied Sciences*, vol. 7, no. 12, pp. 286-293, 2013.

[11] J. Parvez and M. Ahmad Peer, "A Comparative Analysis of Performance and QoS Issues in MANETs", in *World Academy of Science, Engineering and Technology 48, 2010*, pp. 937- 948.

[12] K. Arulanandam and B. Parthasarathy, "A New Energy Level Efficiency Issues in MANET", *International Journal of Reviews in Computing*, pp. 104-109, 2009.

[13] 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.

[14] J. Parvez and M. Ahmad Peer, "A Comparative Analysis of Performance and QoS Issues in MANETs", in *World Academy of Science, Engineering and Technology 48, 2010*, pp. 937- 948.

[15] S. Lalar, "Security in MANET: Vulnerabilities, Attacks & Solutions", *International J. Multidiscip. Curr. Res*, vol. 2, pp. 62-69, 2014.

[16] J. Kwak, R. H. Deng, Y. Won and G. Wang, G, Information Security, Practice and Experience, *6th International Conference, ISPEC 2010, Seoul, Korea, May 12-13, 2010, Proceedings*: Springer, 2010.

[17] Y. Wang, F. Yu, H. Tang and M. Huang, "A mean field game theoretic approach for security enhancements in mobile ad hoc networks", *IEEE Transactions on Wireless Communications*, vol. 13, no. 3, pp. 1616-1627, 2014.

[18] M. Hamdi and H. Abie, “Game-based adaptive security in the Internet of Things for eHealth”, in *IEEE International Conference on Communications (ICC)*, pp. 920-925, IEEE, 2014.

[19] 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*, pp. 473-480, IEEE, 2016.

[20] V.H. La and A.R. Cavalli, “A misbehavior node detection algorithm for 6LoWPAN Wireless Sensor Networks”, in *36th International Conference on Distributed Computing Systems Workshops (ICDCSW)*, pp. 49-54, IEEE, 2016.

[21] D. Das, K. Majumder and A. Dasgupta, “Selfish node detection and low-cost data transmission in MANET using game theory”, *Procedia Computer Science*, 54, pp. 92-101, 2015.

[22] Y. Taheri, H. 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.

[23] Rajkumar B., Narsimha G.: Trust-based certificate revocation for secure routing in MANET. Procedia Computer Science 92, 431-441, (2016).

[24] 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 (IJCNIS)*, vol. 5, no. 10, 2013.

[25] B. Paramasiva, and K. Pitchai, “Modeling intrusion detection in mobile ad hoc networks as a non-cooperative game”, in *International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME)*, pp. 300-306, 2013, IEEE.