Journal of Theoretical and Applied Information Technology
10th July 2015. Vol.77. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

STRATEGIC PROFILING FOR BEHAVIOUR VISUALIZATION OF MALICIOUS NODE IN MANETS USING GAME THEORY

[1]BURHAN UL ISLAM KHAN, [2]RASHIDAH F. OLANREWAJU, [3]ROOHIE NAAZ MIR, [4]ASIFA BABA, [5]BALOGUN WASIU ADEBAYO

[1]Department of Computer Science &Engg., Islamic University of Science & Technology, Kashmir, India
[2]Kulliyyah of Engineering, International Islamic University Malaysia, Kualalumpur, Malaysia
[3] Department of Computer Science &Engg., National Institute of Technology, Srinagar, Kashmir, India
[4]Department of Computer Science &Engg., Islamic University of Science & Technology, Kashmir, India
[5]Lagos State Polytechnic, Ikorodu, Nigeria

E-mail: [1]burhan.iium@gmail.com, [2]rashidah@iium.edu.my,[3]naaz310@nitsri.net, [4]asifababa@islamicuniversity.edu.in, [5]balogunwa1999@yahoo.com

ABSTRACT

In Mobile Adhoc Network (MANET), one of the precarious problems is of identifying the malicious nodes. The identification and later mitigation of the same becomes an immensely difficult task especially when selfish / erroneous nodes exist along with normal collaborative nodes in the Regular camp. The presence of selfish nodes is potentially harmful as similar behaviour can be imitated by malicious nodes which are the point of concern of many security aspects. The paper accentuates the use of game theory and probability theory considering 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 framework 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. A significant focus is given on Perfect Bayesian Equilibrium (PBE) strategy which forms as the basis of all the result analysis. The enhancement is shown in terms of 63% lesser false positives which favors higher overall network utility (modelled as utility of regular nodes in the game) with selfish / erroneous nodes existing in the network when collating the proposed schema with prior work.

Keywords: *Mobile Adhoc Network (MANET), Perfect Bayesian Equilibrium (PBE), Malicious Behaviour, Selfish/Erroneous Behaviour, Security.*

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 neighboring 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 neighbor nodes [2]. When the mobile nodes are required to forward data packets to any of the non-neighboring 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

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

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 behavior in large scale MANET applications as various factors like node behavior, 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]. Although 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 fail-proof security is yet to be seen and standardized for future security protocols.

The paper is organized as: Section 2 gives the overall information about the proposed system. The background knowledge needed for the project, problem definition, main aim and objectives, along with assumptions and dependencies find place here. Section 3 describes formation of proposed model analytically, adopting game theory with exclusive elaboration on game specification, strategy formation, stage game, etc. All important criterion that play critical role in the implementation of the proposed framework have been projected in section 4 followed by their incorporation into an experimental test bed and relative performance analysis in sections 5 and 6 respectively. Finally, section 7 summarizes the cumulative findings and the contribution of the proposed study, furtherdiscusses in brief about the scope of future enhancement for the existing studies to be carried out.

2. PROPOSED SYSTEM

The identified problem of the proposed study can be stated as: *Design a mathematical model based on probability and game theory to exhibit an extremely unpredictable behaviour of the malicious mobile nodes in multiples under diverse vulnerable security condition in MANET as well as considering presence of erroneous or selfish nodes among the regular nodes thereby posing threat to*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

design a decision making model for ensuring mitigating of attack events and deporting mechanism. 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 contributions of the proposed study are i) To formulate a strategic decision making mathematical model using game theory taking into account the tactics adopted by a regular node, a selfish node, and a malicious node and thereby design the game specification, and ii) Conduct a comparative performance analysis, considering the prior work with the proposed system with respect to evaluation of detected false positives and the Utility of regular and malicious nodes. The main assumptions of the framework are as follows:

- Malicious nodes are also rational concerning their goals.
- Malicious nodes are modelled perfectly i.e. they don't exhibit any signs of selfishness during any stage of the game.
- By means of passive observation nodes can track the outgoing packets of their one hop neighbours (network monitoring mechanism).
- Error in observation may occur but with extremely low probability.
- An authentication mechanism exists within a cluster and that the identity is bounded with the physical node which cannot be changed or faked during the node's stay in the cluster.
- When malicious node deports from the cluster in which it conducted attack, it will also erase all its transaction history in that cluster with it thus making the detection process extremely difficult.
- Mobile nodes trust can't be monitored outside the cluster.
- As the proposed study is done considering multi-stage game, hence time factor is assumed to be categorized into slots where each slot exhibits the current progress of game stage.
- Malicious nodes don't conduct attack in the preliminary stages of the game in order to maximize their utility by defecting the trust factor of the regular node.

The paper focuses on enhancing a mathematical schema of strategical decision making that can model the behavioural pattern of regular and malicious nodes in MANET. Previous model [15, 16] is not taking into account the presence of selfish or erroneous nodes among the regular ones while modelling the wrestling between regular and malicious nodes within a MANET environment. A new decision making process is formulated for the same and is benchmarked with the prior one. The enhancement is shown in terms of lesser false positives and higher utility for regular nodes when the selfish / erroneous nodes exist in the network. The proposed framework is designed completely based on the concepts of Basic Game theory; such as Pure and Mixed Strategy, Nash Equilibrium, and Bayesian Game. The potency in modelling of the same completely depends on the effectiveness of the proposed strategy design which is a set of specific action / behaviour that a player (mobile node) adopts. The system presents two types of strategies; pure and mixed strategies. A pure strategy governs a complete specification of actions to be adopted by a node, while a mixed strategy is basically about allocations of a probabilistic factor to each of the pure strategies adopted.

3. FRAMEWORK DESIGN

This section basically introduces the actual scheme that has been formulated for the purpose of designing the proposed framework.

3. 1 Basic Modeling Elements

The proposed system presents a modeling of interactive game between regular mobile node and malicious mobile node as a dynamic Bayesian game [15] and later on finding the Perfect Bayesian equilibrium of the proposed study. The statistical behaviour of the mobile nodes is scrutinized and outcome of the every communication round is recorded for the purpose of analyzing the pattern of malicious behaviour of mobile nodes present in the simulation environment. The framework considers that the private and confidential information should be maintained for type of mobile nodes, which is usually of malicious mobile node or regular mobile node. The regular node forms a statistical belief system towards the mobile nodes which are present in the neighborhood and persistently updates the value (belief) to the actions of neighborhood mobile nodes in due course of progress in game. On the other hand malicious nodes are able to track the belief which regular nodes form for them possess.

Every action of the mobile nodes is very critical and significant that also depends on the counter actions to be undertaken by the ant-party mobile nodes. The optimal outcomes of the responses for both the types of the mobile nodes are

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

guided by the specific actions performed by the other mobile nodes. A specific value of reputation is initialized by a regular mobile node and thereby possessing the potential capability of assessing the type of mobile node's depending upon the updated value of belief as well as specific value of reputation that can be also termed as threshold. On the other hand, the ongoing risk of getting identified is persistently being calculated by malicious mobile node. The malicious mobile node performs a decision action termed 'flee' (shifting from one to another cluster after attacking the prior cluster) depending on the amount of risk and anticipated cost of flee.

The scheme does not limit the phenomenon of selfishness being exhibited by the regular nodes in some stages of the game. There is no degree of selfishness that can approximate the mischievous behavior demonstrated by the malicious node. Unlike the prior work the proposed model includes factors for depicting collaboration and selfishness while formulating the strategies of nodes in Regular and Malicious Node game. The important parameters that have been considered in the proposed formulation are decorated in Table 1.

Table 1: Important Parameters Of The Proposed Framework

List of Actions to be performed by mobile nodes (Regular/Malicious)					
A_{att}	Action of Attack		A_{flee}	Action of Flee	
A_{cop}	Action of Cooperate		A_{rep}	Action of Report	
A_{dec}	Action of Decline				
List of Gain and Cost of Adopted Actions					
G_{att}	Gain of A_{att}		C_{att}	Cost of A_{att}	
G_{cop}	Gain of A_{cop}		C_{cop}	Cost of A_{cop}	
G_{rep}	Gain of A_{rep}		C_{flee}	Cost of A_{flee}	
			C_{rep}	Cost of A_{rep}	
List of Opinion Formulation					
Op_{uncer}	Opinion of uncertainty		Op_{belief}	Opinion of Belief	
$Op_{disbelief}$	Opinion of Disbelief				
Others Parameters					
F	Failure due to false alarm	η_{coop}	Quantity of identified A_{cop}	ρ / ρ^*	Profile of Strategy / Equilibrium strategy
δ	Probability of the node being malicious.	η_{drop}	Quantity of identified A_{att} or A_{dec}	Th	Threshold of uncertainty value
				$E(.)$ / $\sigma(.)$	Anticipated value / Standard deviation
φ	Probability of attack by malicious node	Ψ	Probability of cooperating by regular node	SF	Selfishness Factor associated with a Regular Node reflecting the degree of Selfishness exhibited

3.2 Clustering

The formulation of the cluster is done, where the mobile nodes can independently depart or associate with the cluster in the due course of their mobility within the cumulative simulation environment [17]. Mobile node identity is governed by the physical characteristic of node that is always fixed. Whenever a mobile node wants to join the cluster, the other candidate nodes previously residing in that cluster allocate their initial belief value towardsthe newcomer. Whenever a malicious mobile node arrives into a cluster never visited before, the candidate nodes of new cluster will treat the malicious mobile node as a newcomer and allocate the same initial belief. All nodes within that cluster get the broadcast of reporting information by the regular mobile node. In case of positive report information, the malicious mobile node identified will be penalized. However if the regular node reporting action about the identification of malicious node turns out to be nothing more than a false alarm, the liability of regular node will be badly affected. The proposed scheme considers anticipated gain of legitimate reporting action (G_{rep}) and anticipated failure of non-positive alarm (F) for performing evaluation of the outcomes.

3.3 Neighbour Surveillance

Using the promiscuous environment of the wireless communication system in MANET, a mobile node monitors the outbound data of its neighbour, but they cannot understand the cause of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

communication disruption. This phenomenon in MANET is referred to as Neighbour Monitoring [18]. Hence, the parameters e.g. δ, φ, and ψ are formulated for better distinction of actions of neighbour node and this practice is termed as neighbour surveillance.

3.4 Decision Model

The framework makes use of decision making model that can be considered as a cognitive process that results in judging the course of action out of various possible options. Figure 1 depicts the decision making processes for malicious and regular mobile nodes with regard to the proposed framework. The regular node thus continuously evaluates the option of belief (Op_{belief}) and adequacy of evidence (Op_{uncer}) for the opponent node based on the feedback from the neighbour monitoring. With every successful communication round the regular node increases the η_{coop} by 1. When a communication round fails, the regular node checks for the opponents strategy. If the opponent had opted for A_{dec} / A_{att} then only the value of η_{drop} would be increased by 1, otherwise η_{coop} gets increased by 1. A threshold policy is being followed by a regular node to take reporting decision against the opponent node. If this threshold is not reached the regular node would cooperate or decline based on the current belief it holds for the opponent and the selfishness attribute of itself. Malicious nodes are also modelled to be rational, thus will continuously evaluate the trust factor for itself with the regular node. It also follows a decision rule to flee in order to evade from being reported. The malicious node will evolve an attacking frequency (adopting A_{att}) such that it gets difficult for a regular node to identify its type. A game is played between two nodes one of which has to be regular always as there is no gain associated for malicious nodes while playing the game with each other. Consequently two cases evolve now, (i). Regular node versus Malicious node, and case (ii) Regular node versus Regular node. Although decision process for the regular nodes will be same in both the case, however the diagram for second case also finds mention as figure 2 for clarity of thought.

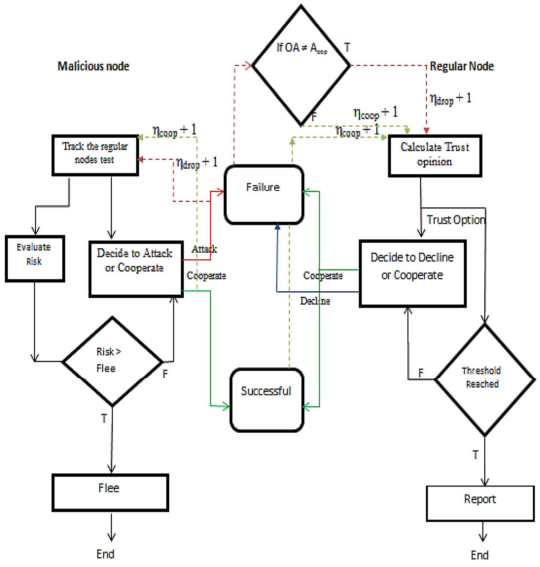


Figure 1: Decision Making Processes For Regular Versus Malicious Game

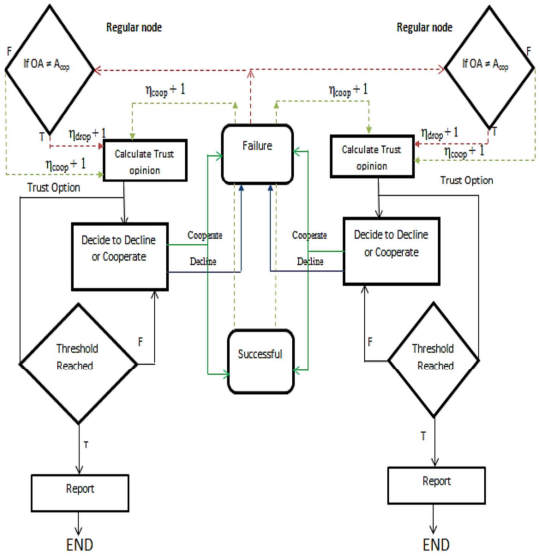


Figure 2: Decision Making Processes for Regular versus Regular game

3.5 Bayesian Signaling Game

The proposed framework considers multi-stage dynamic Bayesian Signaling game [15, 16]. While designing Bayesian games, each mobile node is set with certain classified information that has significant impact on the evolution of the game, while other mobile nodes areconsidered to possess information of the belief system about the classified data. These values of belief are signified by probability distribution and revised by applying Baye's rule in case of availability of novice

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

information. The mobile nodes select their best possible action during the progress of game as per the classified and belief information available. The framework has adopted Perfect Bayesian Equilibrium that ensures the formation of belief for the one type of mobile node about its counter type of mobile nodes, revising their belief information with the completion of every stage, and adopting the optimized actions with the aid of such belief system in the current stage.

3.6 Specification of Game

The proposed framework has formulated the game logic using regular and malicious mobile nodes as players considering multi-stage Bayesian signaling game for investigating the most favourable strategy of both the types of players. The mobile nodes (x, y) are endowed with capability to select a specific action from the set of their allowed strategies. The framework considers regular mobile node strategy set as (A_{cop}, A_{dec}, A_{rep}) and that for malicious mobile node the same would be (A_{att}, A_{cop}, A_{flee}).

The system considers for both the type of mobile nodes, all the feasible set of strategies excluding A_{dec} acquire cost. The framework interprets cost as the certain amount of resources utilized for performing that specific action. The malicious mobile node gains G_{att} from successful accomplishment of attack action A_{att} which is also dependent on the selection of strategies by the ant-party nodes. However, the malicious mobile node can also create confusion by selecting A_{cop} in order to mislead the regular node y. But, in case of single staged game a malicious mobile node doesn't gain by selecting A_{cop} as its goal (attack) varies from the action selected (A_{cop}). This is totally reverse in case of regular node which gains G_{cop} after adopting action for cooperation A_{cop}. Table 1 [16] exhibits the utility considered for the study.

Table 2: Tabulation Of Utility Index Considered

	A_{cop}	A_{dec}	A_{rep}
A_{att}	(G_{att}-C_{att} ,-G_{att}-C_{cop})	(-C_{att} ,0)	(-G_{rep}-C_{att} , G_{rep}-C_{rep})
A_{cop}	(-C_{cop}, G_{cop}-C_{cop})	(-C_{cop} , 0)	(-G_{rep}-C_{cop} , G_{rep}-C_{rep})
A_{flee}	(-C_{flee}, -C_{cop})	(-C_{flee},0)	(-C_{flee}, -C_{rep})

(i) Considering Node x is malicious mobile node.

	A_{cop}	A_{dec}	A_{rep}
A_{cop}	(G_{cop}-C_{cop}, G_{cop}-C_{cop})	(-C_{cop}, 0)	(-C_{cop}, -F-C_{rep})
A_{dec}	(0, -C_{cop})	(0, 0)	(0, -F-C_{rep})
A_{rep}	(-F-C_{rep}, -C_{cop})	(-F-C_{rep} , 0)	(-F-C_{rep}, -F-C_{rep})

(ii) Considering Node x is regular mobile node.

The framework considers anticipated gain for A_{flee} as the dynamic risk factor that maximizes when the regular mobile node y collects the evidence.

3.7 Designing A Belief System

The framework adopts multi-stage Bayesian game where the regular node y will require revising its belief value depending on the progress of game. The system thereby deploys the usual update policy for belief as η_{coop} / (η_{coop} + η_{drop}). The framework assimilates an uncertainty-aware reputation system into decision method of regular mobile node and utilize a third factor called Op_{uncer} for signifying regular mobile node y's opinion towards the other type of node x: (Op_{belief}, $Op_{disbelief}$, Op_{uncer}) ϵ [0, 1]. The Op_{uncer} is the normalized variance for beta distribution [16]. Thus:

$$Op_{belief} = (\eta_{coop} / (\eta_{coop} + \eta_{drop}))*(1-Op_{uncer}) \quad (1)$$

$$Op_{disbelief} = (\eta_{drop} / (\eta_{coop} + \eta_{drop}))*(1-Op_{uncer}) \quad (2)$$

$$Op_{uncer} = 12 * \eta_{coop} \cdot \eta_{drop} / ((\eta_{coop} + \eta_{drop})^2 * (\eta_{coop} + \eta_{drop} + 1)) \quad (3)$$

3.8 Designing A Stage Game

The mobile nodes are rational in nature which will mean that regular mobile nodes will have tendency to identify malicious node and perform reporting action while malicious node will adopt a strategy that reduces the possibility of itself getting identified and thereby maximizing its goal of invoking attack in the network. Figure 3 shows single stage game design. It considers a single stage

Journal of Theoretical and Applied Information Technology
10th July 2015. Vol.77. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

game, where the nature decide the kind of the mobile node *x*, and the kind is *x*'s private information. The mobile node *y* possess current belief information that *x*'s type is malicious signified by the probability factor δ. Hence, according to Baye's rule, δ and (1- δ) are computed as:

$$\delta = \eta_{drop} / (\eta_{coop} + \eta_{drop}) \quad (4)$$

$$(1- \delta) = \eta_{coop} / (\eta_{coop} + \eta_{drop}) \quad (5)$$

When a new node joins a cluster the existing nodes within the cluster assign preliminary values as $\eta_{coop} = \eta_{drop} = 1$ (*i.e.* $\delta = 0.5$ and $Op_{uncer}=1$) for the new comer, which shows that there is no evidence at this point of time or there exists complete uncertainty in the option of the nodes.

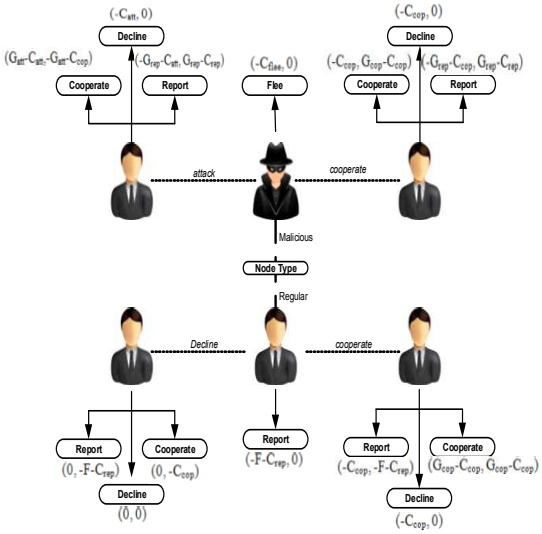


Figure 3: Single Stage Game Design [16]

3.9 Pure Strategy Adoption

In pure strategy, the strategy profile can be represented under two scenarios. In the first case the malicious node *x* will always play attack (A_{att}) while in the second case it will always play cooperate (A_{cop}). In the first case the strategy profile of node *x* can be represented as: ρ_x = (A_{att} if malicious node, A_{cop} if regular node). The above formulation would mean that *x* always adopts A_{att} if it is malicious type of node and A_{cop}if it is regular type of node. Therefore the anticipated payoff $E_y(A_{cop})$ or $E_y(A_{dec})$ of *y* adopting the pure strategy i.e. $\rho_y = A_{cop}$ or $\rho_y = A_{dec}$ are:

$$E_y(A_{cop}) = \delta. (-G_{att}-C_{cop}) + (1- \delta). (G_{cop} - C_{cop}) \quad (6)$$

$$E_y(A_{dec}) = \delta.0 + (1- \delta). 0 \quad (7)$$

The formulation of $E_y(A_{cop})$ and $Ey(A_{dec})$ basically indexes two cases. In the first case, the neighbour mobile node x is considered as malicious mobile node. As per node *y*'s existing belief system, this case surfaces with the probability of δ. As node x will adopt Aatt action, the payoff of node y in such situation will be $(-G_{att} - C_{cop})$ and 0 respectively. In the second type of case, x is a regular node surfacing with a probability (*1*- δ). The payoff of node y in this situation will be $(G_{cop}-C_{cop})$ and 0 respectively. If $E_y(A_{cop}) \geqslant E_y(A_{dec})$, the node *y*will choose to adopt A_{cop} as best possible action.

$E_y(A_{cop}) \geqslant E_y(A_{dec})$

$\rightarrow \delta. (-G_{att} - C_{cop}) + (1- \delta).(G_{cop} - C_{cop}) \geq 0$
$\rightarrow -\delta.G_{att} - \delta. C_{cop} + G_{cop} - C_{cop} - \delta.G_{cop} + \delta.C_{cop} \geq 0$
$\rightarrow \delta. (-G_{att} - G_{cop}) + G_{cop} - C_{cop} \geq 0$
$\rightarrow \delta. (G_{att} + G_{cop}) \leq G_{cop} - C_{cop}$
$\rightarrow \delta \leq (G_{cop} - C_{cop}) / (G_{att} + G_{cop})$

Therefore, when the computed probability $\delta \leq (G_{cop}-C_{cop}) / (G_{att} + G_{cop})$, the Bayesian Nash equilibrium strategy pair for node *x* and *y* is: (ρ_x, ρ_y) = ((A_{att} if malicious node, A_{cop} if regular node), A_{cop}). But, this fact changes when $\delta > (G_{cop}-C_{cop}) / (G_{cop} + G_{att})$ as there is no existence of pure strategy BNE. Consequently, when the malicious node *x* adopts A_{att}, the preeminent response for node *y* in this case will be to adopt A_{dec} but, if the regular mobile node *y* adopts the action A_{dec} than malicious node may choose to adopt A_{cop} as the best possible reaction as C_{att} may by higher compared to C_{cop} in some critical and sensitive scenarios for malicious node.

In the second scenario, the malicious mobile node *x* may select pure strategy A_{cop}. In this situation, the regular node *y*'s best reaction will be to adopt A_{cop}without considering for δ. But, in case regular node *y* adopts the action *Acop*, then the malicious node may adopt the action *Aatt* that minimized to the prior situation. The profiles may be represented as (ρ_x, ρ_y) = ((A_{cop} if malicious node, A_{cop} if regular node), A_{cop}) which is definitely not Bayesian Nash equilibrium.

3.10 Mixed Strategy Adoption

This phase of discussion considers possible circumstances of mixed strategy Bayesian Nash equilibrium. φ signifies the probability of malicious mobile node *x* to adopt the action A_{att}, and ψ signifies the probability of the regular node *y* to adopt the action A_{cop}. Therefore the anticipated payoff of node *y* adopting while adopting A_{cop} and A_{dec} are:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$E_y(A_{cop}) = \delta.\varphi.(-G_{att}-C_{cop}) + \delta.(1-\varphi).(G_{cop}-C_{cop}) + (1-\delta).(G_{cop}-C_{cop})$$

$$= \delta.\varphi.(-G_{att}-C_{cop}) + (1-\delta.\varphi).(G_{cop}-C_{cop}) \quad (8)$$

$$E_y(A_{dec}) = \delta.\varphi.0 + ((\delta.(1-\varphi)) + (1-\delta)).0 \quad (9)$$

In order to render selection among A*cop* and A*dec* have no impact on regular node *y*'s utility; Imposing $E_y(A_{cop}) = E_y(A_{dec})$.

$E_y(A_{cop}) = Ey(A_{dec})$

→ $\delta.\varphi.(-G_{att}-C_{cop}) + (1-\delta.\varphi).(G_{cop}-C_{cop}) = 0$
→ $\delta.\varphi.(G_{att}+C_{cop}) = (1-\delta.\varphi).(G_{cop}-C_{cop})$
→ $\delta.\varphi.(G_{att}+C_{cop}) + \delta.\varphi.(G_{cop}-C_{cop}) = (G_{cop}-C_{cop})$
→ $\delta.\varphi.(G_{att}+G_{cop}) = (G_{cop}-C_{cop})$
→ $\varphi = (G_{cop}-C_{cop}) / (\delta.(G_{att}+G_{cop}))$

Therefore, the malicious node *x*'s strategy for equilibrium will be to adopt the action A*att* with $\varphi = (G_{cop}-C_{cop}) / (\delta.(G_{att}+G_{cop}))$. The anticipated payoff for malicious node x for adoption the action A*att* and A*cop* are respectively as:

$$E_x(A_{att}) = \psi.(G_{att}-C_{att}) + (1-\psi)(-C_{att})$$

$$= \psi.G_{att} - C_{att} \quad (10)$$

$$E_x(A_{cop}) = -C_{cop} \quad (11)$$

Similarly as above, imposing $E_x(A_{att}) = E_x(A_{cop})$ in order to render the actions A_{att} and $A_{cop}$to have no impact on malicious node *x*'s utility, the equilibrium strategy of regular node *y* should be to adopt the action $A_{cop}$with probability $\psi = (C_{att} - C_{cop}) / G_{att}$(when $C_{att} < C_{cop}$, $\psi=0$). Thus, mixed strategy pair (ρ_x, ρ_y) = ((*φ* if malicious node, *Acop* if regular node), *ψ*) is a Bayesian Nash equilibrium for corresponding situation. Hence, the Bayesian Nash equilibrium of the stage game can be finalized as: When $\delta \le (G_{cop}-C_{cop}) / (G_{att}+G_{cop})$; (ρ_x, ρ_y) = ((A_{att} if malicious node, A_{cop} if regular node), A_{cop}); after $\delta > (G_{cop}-C_{cop}) / (G_{cop}-G_{att})$, the regular node *y* turns bit conservative and (ρ_x, ρ_y) = ((*φ* if malicious node, A*cop* if regular node), *ψ*).

3.11 PBE Strategy Formation

When formulating the Bayesian Nash Equilibrium (BNE) for a single stage game, A_{cop} and A_{dec} / A_{att} needed to be considered. However we are still left with two important node actions, a regular node can report another node as malicious by adopting A_{rep}while a malicious node can adopt A_{flee} in order to save itself from being caught, which will complete the sequential rationality of the mobile nodes.

3.11.1 Designing a reporting action

The proposed framework considers sequential rationality only in the situation when the anticipated payoff of the mobile nodes is higher in the progress of the game for the strategies played by its opponent. The regular node *y* after adopting action A_{rep} against node *x* can fetch two responses. i) Either node *x* was identified to be malicious and report was proven as positive or, ii) node *x* after identification was found to be a legitimate regular node and report was proven to be a false positive. However, the probability for occurrence of the second event can't be ruled out if some regular nodes behave selfishly (are forced to adopt A_{dec} unwillingly because of resource constrains at that particular instance) in certain stages of the game. Regular node should attempt to avoid it as a frequent occurrence of such events reduces the capability of the regular node to detect the genuine attacks. Hence, regular node should compute *F* (Private subjective value exhibiting the regular mobile node's properties) in case of false positive report. Smaller value of *F* points out to the aggressive nature of the regular mobile node, while large value of *F* depicts a conformist character.

The proposed design considers usage of threshold factor (*Th*)for accomplishing the best result. *Th* illustrates the integration of both the amount of identified actions A_{att} / A_{dec} in the evidence and the adequacy of evidence as the same being levied together $\delta.(1-Op_{uncer})$. In order to satisfy the sequential rationality, the regular node *y* should choose to adopt action A*rep* only when:

$$E_y(A_{rep}) > \max\{E_y(A_{cop}), E_y(A_{dec})\} \quad (12)$$

Where, $E_y(A_{rep}) = \delta.(1-Op_{uncer}).(G_{rep}-C_{rep}) - ((1-\delta).(1-Op_{uncer})+Op_{uncer}).(F+C_{rep})$. (13)

The regular mobile node should not be opting for A_{rep} when $E_y(A_{cop}) > 0$. Employing A_{rep} with $E_y(A_{cop}) > 0$ would mean circumventing the possibility of achieving gains during from the subsequent stages. Hence, the threshold *Th* should be computed as the state that forms $E_y(A_{rep}) > 0$ [16].

$E_y(A_{rep}) > 0$

→ $\delta.(1-Op_{uncer}).(G_{rep}-C_{rep}) - ((1-\delta).(1Op_{uncer})+Op_{uncer})).(F+C_{rep}) > 0$

→ $\delta.(1-Op_{uncer}).(G_{rep}-C_{rep}) - (1-Op_{uncer} - \delta + \delta.Op_{uncer} + Op_{uncer}).(F+C_{rep}) > 0$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$\rightarrow \delta.(1\text{-}Op_{uncer}).(G_{rep}\text{-}C_{rep}) > (1 - \delta + \delta.Op_{uncer}).(F + C_{rep})$

$\rightarrow \delta.(1\text{-}Op_{uncer}).(G_{rep}\text{-}C_{rep}) + \delta(1\text{-}Op_{uncer}).(F + C_{rep}) > (F + C_{rep})$

$\rightarrow \delta.(1\text{-}Op_{uncer}).(G_{rep} + F) > (F + C_{rep})$

$\rightarrow \delta.(1\text{-}Op_{uncer}) > (F + C_{rep}) / (G_{rep} + F).$

Hence, $$Th = \frac{F + C_{rep}}{G_{rep} + F} \quad (14)$$

Therefore, when $\delta.(1 - Op_{uncer}) \geq \frac{F + C_{rep}}{G_{rep} + F}$, regular mobile node y adopts the action A_{rep}. However, malicious mobile node may have dual selections e.g. i) Setting $\varphi < Th$ will render no action of report by regular node irrespective of its uncertainty, and ii) Setting φ as higher to adopt A_{att} and A_{flee} before adopting the action A_{rep}.

Player y's PBE strategy ρ_y^*

```
A: if δ (1- Op_uncer) ≥ (F + C_rep) / (G_rep + F)
        Report x as Malicious by adopting A_rep;
        goto B;
   else
        if δ ≤ (G_cop - C_cop) / (G_cop + G_att)
            Adopt A_cop with a probability of 1;
        else
            Adopt A_cop with a probability of
            (C_att - C_cop) / G_att;
        end if
    Update η_coop and η_drop to evaluate new values for δ
        and Op_uncer;
        goto A;
B: end if
```

3.11.2 Designing Deporting Action

When a malicious node attempts to deport to some other cluster (A_{flee}) after performing attack, the anticipated gain of the malicious node will be to avoid getting detected by the regular node. The system defines the risk factor as the anticipated loss of being reported. Accordingly $Risk\_factor$ = P ($detect$).G_{rep}, where P (detect) is the probability of getting detected by the regular node. Hence, malicious node computes anticipated gain by employing the Aflee as:

$$E_x(Aflee) = Risk\_factor - C_{flee} \quad (15)$$

When the condition E_x ($Aflee$) > max {E_x ($Aatt$), E_x ($Acop$)} is met the malicious node should deport to a new cluster by employing the $Aflee$. The malicious mobile nodes possess the precise information about the communication record between them and regular mobile node and hence, it can accurately compute the belief of regular node. The malicious node is also expected to have sufficient information about the network hence it knows the statistical information of loss of false report (F) for the regular node. When there are large numbers of nodes within the MANET, (F) should comply with standard normal distribution. The malicious node could know the mean (expected value) and standard deviation for (F) with the network. Probability of detection for a malicious node, P($detect$), is equivalent to the probability that the current δ(1-$Opuncer$) will pass regular mobile node's threshold Th [16].

$$P(detect) = P(\delta.(1\text{-}Op_{uncer}) > Th)$$
$$= P(\delta.(1\text{-}Op_{uncer}) > (C_{rep} + F)/(G_{rep} + F))$$
$$= P(\delta.(1\text{-}Op_{uncer}).(G_{rep} + F) > (C_{rep} + F))$$
$$= P((C_{rep} + F) < \delta.(1\text{-}Op_{uncer}).(G_{rep} + F))$$
$$= P((C_{rep} + F) < \delta.(1\text{-}Op_{uncer}).(G_{rep} + F))$$
$$= P(F.(1 - \delta.(1\text{-}Op_{uncer})) < \delta.(1\text{-}Op_{uncer}).G_{rep} - C_{rep})$$
$$= P(F < ((\delta.(1\text{-}Op_{uncer}).G_{rep} - C_{rep})) / (1 - \delta.(1\text{-}Op_{uncer})))$$
$$= P(F < \frac{\delta(i - Op_{uncer}).G_{rep} - C_{rep}}{1 - \delta(1 - Op_{uncer})}) \quad (16)$$

For a generic normal distribution f with mean μ and deviation σ, the cumulative distribution functionis:

$$F(x) = \Phi\left(\frac{x-\mu}{\sigma}\right) \quad (17)$$

Thus, we have,

$$P(\text{detect}) = \Phi\left(\frac{\frac{\delta(1 - Op_{uncer})G_{rep} - C_{rep}}{1 - \delta(1 - Op_{uncer})} - E(F)}{\sigma(F)}\right) \quad (18)$$

Where, $$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} \exp\left(-\frac{Op_{uncer}^2}{2}\right) dOp_{uncer}$$

It can be seen that a malicious mobile node benefits from selecting its optimum value for φ when invoking A_{att} and latter bypass penalization with the aid of deporting to a new cluster (A_{flee}). The malicious node persistently needs to compute the risk of residing and playing further within a cluster.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Malicious-type player x's PBE strategy ρ_x^*

A: if $E_x(A_{flee}) \geq \max\{E_x(A_{att}), E_x(A_{cop})\}$
Deport to a new cluster by adopting A_{flee};
goto B;
else
if $(\delta \leq (G_{cop}\text{-}C_{cop}) / (G_{cop} + G_{att}))$
Adopt A_{att} with a probability of 1;
else
Adopt A_{att} with a probability of $(G_{cop}\text{-}C_{cop}) / (\delta.(G_{att} + G_{cop})$;
end if;
Track regular nodes values for δ and Op_{uncer};
Update $E_y(A_{flee})$;
goto A;
B: end if

3.12 Modelling Selfish Behaviour

The proposed scheme does not limit the phenomenon of selfishness being exhibited by the regular nodes in some stages of the game where ordinarily it should have revealed collaboration only. Existence of selfish mobile nodes is being considered, wherein it is anticipated that certain regular nodes may choose to behave selfishly at certain instances. Selfishness may be exhibited due to two reasons; either the node tries to behave rationally to save its resources or otherwise there may exist some hardware or software issues with the regular node at particular instances of time. However in both the cases the end result is common the regular nodes refuse to take part in the communication round and thus adopt an action of decline (A_{dec}). We shall not be going to the sophistication of why the nodes are exhibiting selfishness, but rather try to capture the selfishness as a discrete quantity. Although, some regular node may behave selfishly at some events but it doesn't mean it has a consistent harmful intention for deterioting the communication in MANET. It needs to be clearly understood that there is no degree of selfishness that can approximate the nasty behaviour demonstrated by the malicious node.

In the current framework the behaviour of nodes is completely governed by the strategy they are adopting. So the selfishness characteristic also needs to be imposed upon the strategies alone. It was shown in Table 1 that *SF* signifies the degree of selfishness exhibited by a regular node. *SF* represents the probability of a regular node playing decline strategy $A_{dec}$when it should have actually cooperated (A_{cop}) based on its current beliefs it is holding. Embedding selfishness into the strategies of regular node:

Pure strategy will become: $A_{cop}$with a probability of (1-*SF*)

Mixed strategy will become:$A_{cop}$with a probability of (1-*SF*). $((C_{att} - C_{cop}) / G_{att})$

PBE strategy will become:

A: if $\delta\,(1\text{- }Op_{uncer}) \geq (F + C_{rep}) / (G_{rep} + F)$
Report *x* as Malicious by adopting A_{rep};
goto B;
else
if $\delta \leq (G_{cop}\text{-}C_{cop}) / (G_{cop} + G_{att})$
Adopt A_{cop} with a probability of (1-*SF*);
else
Adopt A_{cop} with a probability of (1-*SF*).$(C_{att} - C_{cop}) / G_{att}$;
end if
Update η_{coop} and η_{drop};
Evaluate new values for δ and Op_{uncer};
goto A;
B: end if

The above transformation leads to two implications. First, the regular nodes only exhibit selfishness while playing the cooperate strategy A_{cop}. They never exhibit selfishness when they want to report the other node as malicious by adopting A_{rep}. This is because otherwise the opposite players in the game (mobile nodes) will no longer be completely rational. This is also in line with the definition of selfishness that the regular nodes are rational while playing the game with each other. Second, if the regular node is assumed to be always collaborative i.e. the selfishness factor SF is zero then actually there is no change in strategies.

4. IMPLEMENTATION

The simulation has been carried out in Matlab considering four different scenarios for the purpose of assessment. The simulation is initiated by deploying the mobile nodes randomly via random based mobility model which is illustrated in next section. The simulation study basically considers the target of the malicious node to invoke an attack while retaining all the strategies to be adopted for getting itself caught or being reported by the regular node. On the other hand, the update and reporting activities of the regular nodes should reduce the extent of damage or disruption in communication caused by the attack of malicious nodes. The following are the important criterion in the simulation setup:

1. One hundred nodes are randomly placed in a 900 m × 900 m region which is evenly divided into nine clusters.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2. Any two nodes within the same cluster are considered neighbours.

3. Mobile nodes follow random waypoint mobility model.

4. The default number of malicious nodes is 40.

5. The default number of regular nodes is 100.

6. Number of selfish nodes among regular nodes (for scenarios 3 and 4) =30.

7. The expected value of cost parameters are C_{att}=5, C_{cop}=4, C_{rep}=5, C_{dec}=0 and C_{flee}=40.

8. We select the drop-packet attack as the sample attack in the simulation.

9. The default values for the expected gain parameters are G_{att} = 20, G_{cop} = 30, and G_{rep} = 80.

10. F complies to the normal distribution with $E(F)$ = 100 and $\sigma(F)$ =20.

11. Selfishness factor (for scenario 3 and 4), $SF \epsilon$ {0.20, 0.25, 0.40}.

12. Pause time for a regular node = {4:6 stage games}.

13. Identity of the Node in governed by the index it holds. Regular nodes are indexed as (1- 100) while selfish nodes within the regular ones are indexed from (1- 30) and malicious nodes are indexed from 101-140.

14. Consideration of a free space propagation model.

15. Network consists of homogenous nodes and individual nodes move independently.

16. Each scenario is simulated 16 times and their average is taken as final result.

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. RESULT DISCUSSION

This section discusses about the result being accomplished from the study. The results were estimated for 50 index of the multi-stage game considering average utility, which is scaled to 100 times. The simulations have been conducted for monitoring the trends of pure strategy, mixed strategy, and PBE strategy adoption for visualizing behavioural pattern of regular and malicious node exclusively. A significant focus is given on PBE (Perfect Bayesian Equilibrium) strategy which will form the basis of all the result analysis in the next section as compared to other two strategies i.e. pure strategy and mixed strategy. Simulations for each scenario are carried out 16 times and the average data is used to formulate final results. In all of the scenarios it is assumed that malicious nodes don't conduct attacks in the preliminary stages of the game to escalate their utility.

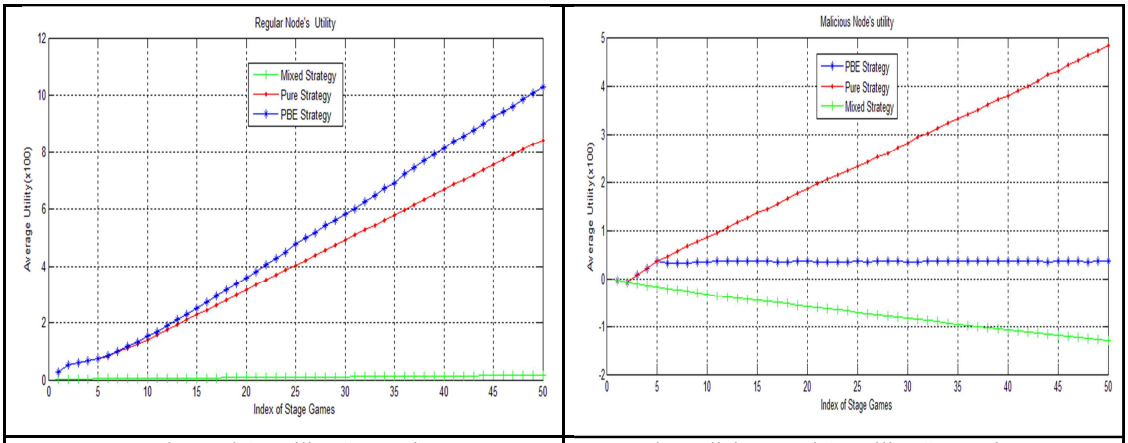
5.1 Results Accomplished From Scenario-1

Figure 4 and 5 highlights the simulation results of scenario 1, wherein the prior model is evaluated in a completely collaborative environment. Figure 4 depicts the strategy comparison for a regular node in terms of average utility scored per node when the malicious nodes employ their PBE strategy. It can be seen from figure 4 (a) that utility of regular nodes is maximum when they follow their PBE strategy. This is so, because by employing PBE, the regular node is in a position of catching a malicious node which otherwise is not possible. Furthermore the regular nodes are in a position to collaborate most of the times with other regular nodes when following the PBE strategy. Utility gained by regular nodes when employing pure strategy is also high; this is because here the regular nodes don't miss any opportunities to collaborate with other regular nodes and even malicious nodes. However the utility gained by employing Pure strategy is lower than what it was with PBE strategy. This is so, because the while employing the Pure strategy,

Journal of Theoretical and Applied Information Technology
10th July 2015. Vol.77. No.1

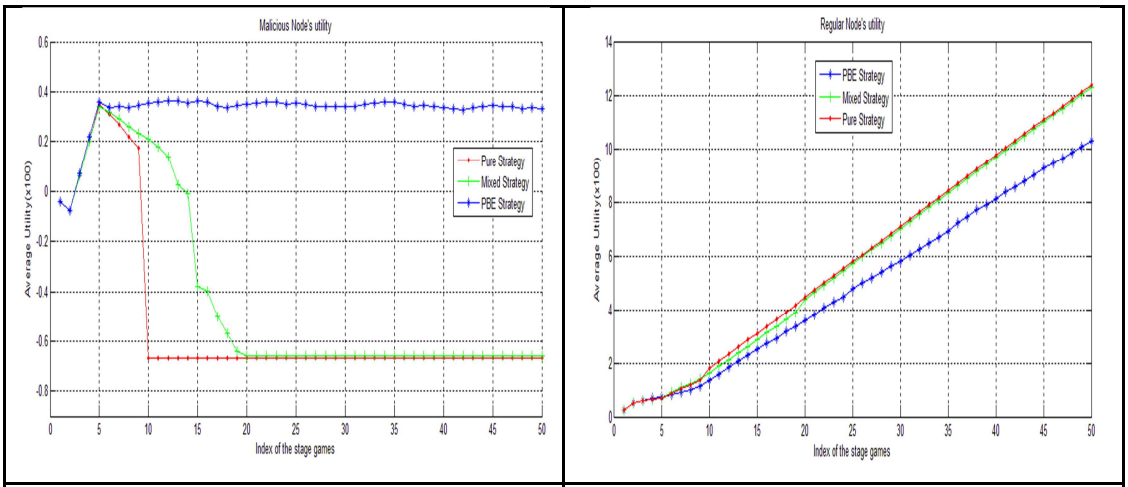
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the regular nodes were not able to defend themselves from any of the attacks conducted by the malicious nodes. This can be verified as utility of malicious nodes is the highest when regular nodes employ its pure strategy in Figure 4 (b). When regular nodes employ their mixed strategy the utility of malicious nodes becomes negative. However utility of regular nodes is also least in this case. It can be clearly comprehended from the results of Figure 4 that regular nodes PBE strategy is the best response as compared to the other two i.e. pure and mixed strategies.



Regular Node's Utility Comparison | b. Malicious Node's Utility Comparison

Figure 4.1 Strategy Comparison For Regular Nodes When Malicious Nodes Employ PBE Strategy.



a. Malicious Node's Utility Comparison | b. Regular Node's Utility Comparison

Figure 4.2 Strategy Comparison For Malicious Nodes When Regular Nodes Employ PBE Strategy.

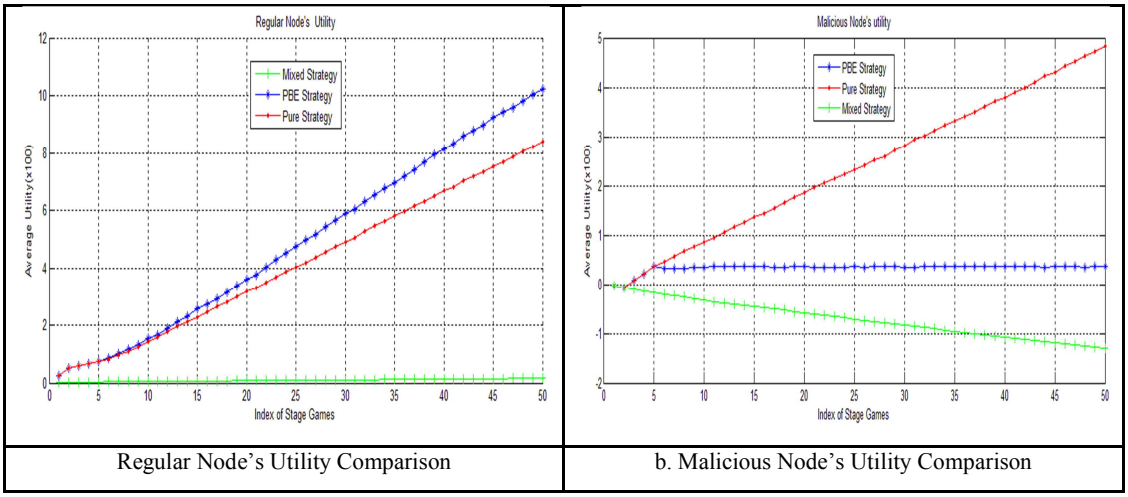
Figure 5 depicts the strategy comparison for a malicious node in terms of average utility scored when PBE strategy is being employed by the regular nodes. It can be seen from figure 5 (a) that the utility of malicious nodes remains positive for the initial stages of the game only and latter falls vividly to a point of no return when pure or mixed strategies are employed by the same. This would mean that all the malicious nodes are being identified by the regular nodes during the initial stages of the game only. Furthermore when malicious nodes employ pure or mixed strategies the corresponding utility for the regular nodes is highest as depicted in Figure 4.1 (b). Moving to the PBE strategy of malicious nodes, it can be clearly

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

seen that when malicious nodes employ their PBE strategy the average utility score for the same is highest and never falls below zero. Corresponding utility for regular nodes is again least, when PBE strategy is being employed by malicious nodes. Hence PBE for the malicious nodes clearly outperforms the other two strategies i.e. pure and mixed strategies. The implication from the above discussion is that PBE strategy is the only feasible strategy for a mobile node to adopt irrespective of its type, whether it is regular or malicious. There was not a single false positive detected in the current scenario with Regular PBE versus Malicious PBE game.

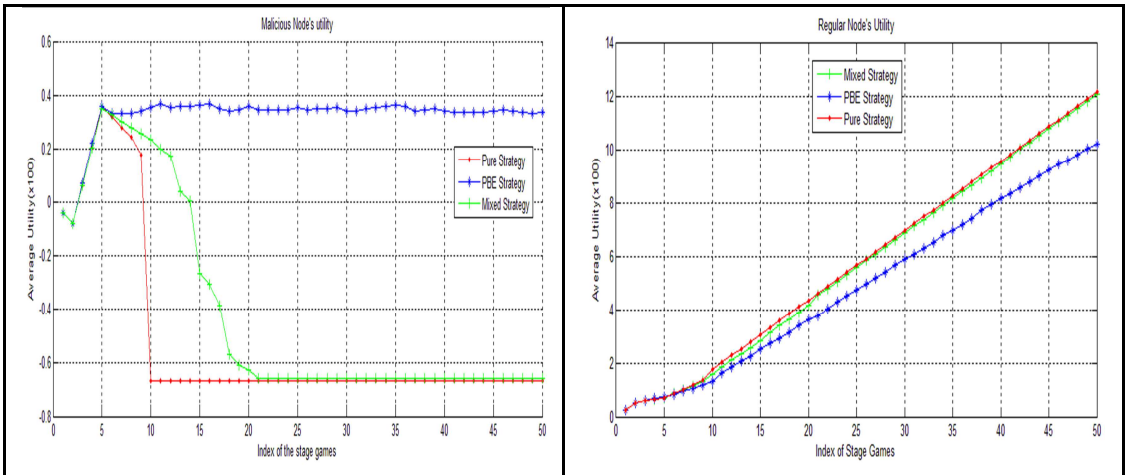
5.2 Results Accomplished From Scenario-2

Figure 5.1 and 5.2 show the simulation results of scenario 2, wherein the proposed model is evaluated in a completely collaborative environment. Figure 5.1 depicts the strategy comparison for a regular node in terms of average utility scored when the malicious nodes employ their PBE strategy while Figure 5.2 depicts the strategy comparison for a malicious node in terms of average utility scored when PBE strategy is being employed by the regular nodes. It can be easily comprehended from the above results that PBE strategy outperforms other two strategies i.e. mixed and pure, for both regular and malicious nodes. There was not a single false positive detected in the current scenario with Regular PBE versus Malicious PBE game.



Regular Node's Utility Comparison | b. Malicious Node's Utility Comparison

Figure 5.1 Strategy Comparison For Regular Nodes When Malicious Nodes Employ PBE Strategy.

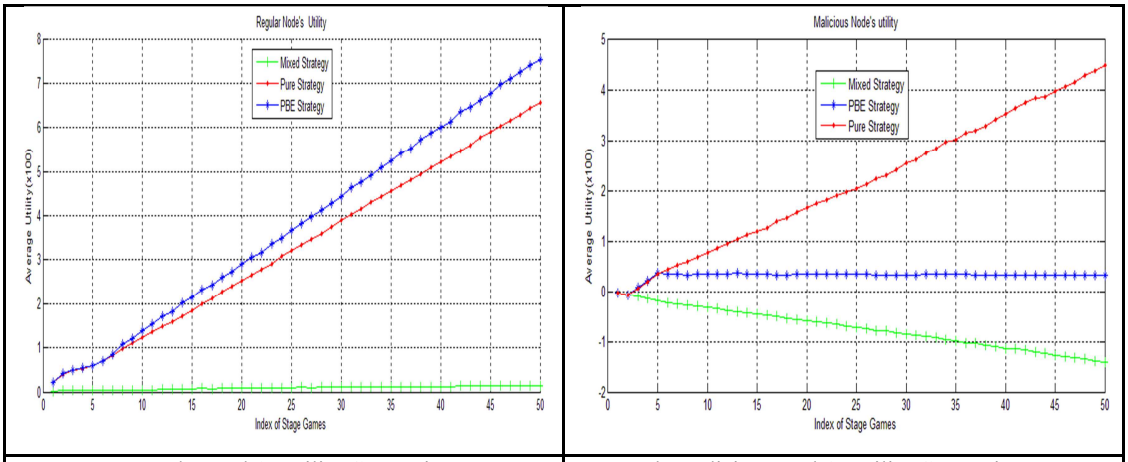


a. Malicious Node's Utility Comparison | b. Regular Node's Utility Comparison

Figure 5.2 Strategy Comparison For Malicious Nodes When Regular Nodes Employ PBE Strategy.

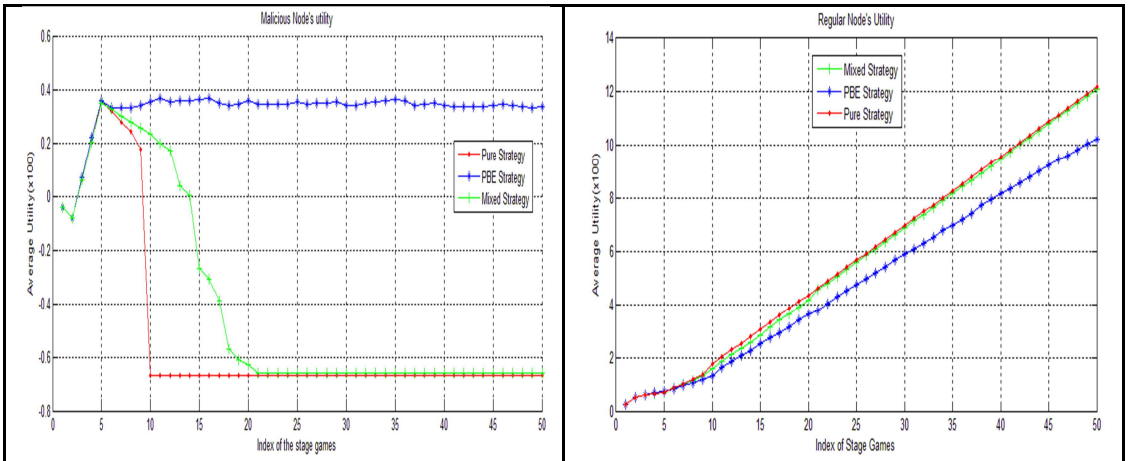
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5.3 Results Accomplished From Scenario-3



a. Regular Node's Utility Comparison | b. Malicious Node's Utility Comparison

Figure 6.2 Strategy Comparison For Malicious Nodes When Regular Nodes Employ PBE Strategy.



a. Malicious Node's Utility Comparison | b. Regular Node's Utility Comparison

Figure 6.1 Strategy Comparison For Regular Nodes When Malicious Nodes Employ PBE Strategy.

Figures 6.1, 6.2 and 6.3 present the simulation results of scenario 3, wherein the prior model is evaluated in a partially collaborative environment. Among 100 regular nodes 30 have been modeled to behave selfishly with varying degrees. Figure 6.1 depicts the strategy comparison for a regular node in terms of average utility scored when the malicious nodes employ their PBE strategy while Figure 6.2 depicts the strategy comparison for a malicious node in terms of average utility scored when PBE strategy is being employed by the regular nodes. It can be easily comprehended from the results that PBE strategy outperforms other two strategies i.e. mixed and pure, for both regular and malicious nodes.

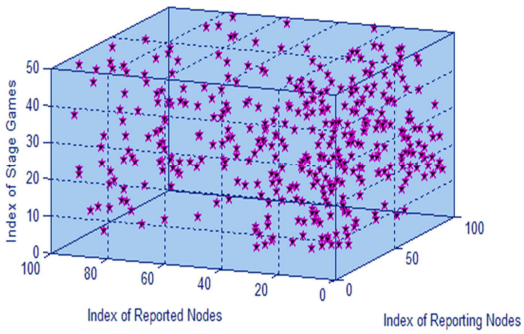


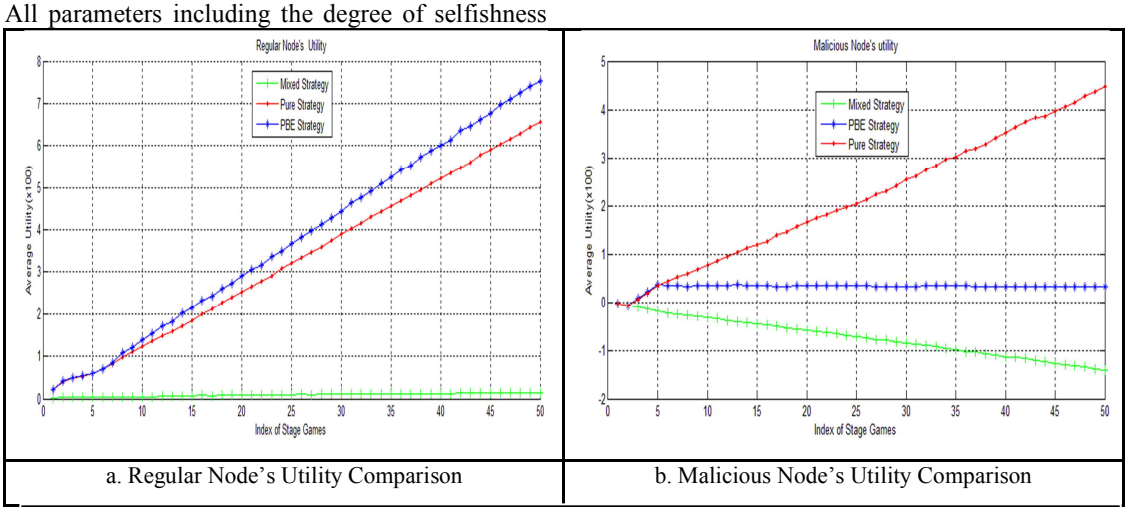
Figure 6.3 Detected False Positives In Regular PBE Versus Malicious PBE Game

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Figure 6.3 presents the false reporting done by regular nodes against other regular nodes. False alarms are considered with Regular PBE versus Malicious PBE only. Reporting regular nodes in figure 6.3 implies the index of the regular node which made the false alarm while Reported regular node indicates the index of the regular node against whom the alarm was made. Index of stage game connotes the stage in which this false alarm occurred. There were a total of 391 false reports detected in total in all the 50 stages of the game when simulation was carried out 16 times.

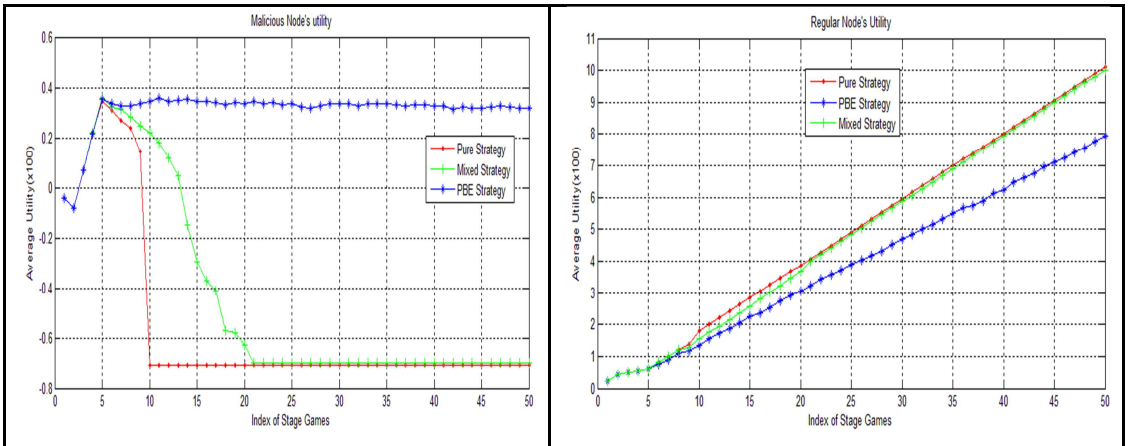
5.4 Results Accomplished From Scenario-4

Figures 7.1, 7.2 and 7.3 present the simulation results of scenario 3, wherein the proposed model is evaluated in a partially collaborative environment. All parameters including the degree of selfishness are identical to that of Scenario 3. Figure 7.1 depicts the strategy comparison for a regular node in terms of average utility scored when the malicious nodes employ their PBE strategy while Figure 7.2 depicts the strategy comparison for a malicious node in terms of average utility scored when PBE strategy is being employed by the regular nodes. It can be easily realized from the below results that PBE strategy outperforms other two strategies i.e. mixed and pure, for both regular and malicious nodes. Figure 7.3 presents the false reporting done by regular nodes against other regular nodes. False alarms are considered with Regular PBE versus Malicious PBE only. There were a total of 146 false reports detected in total in all the 50 stages of the game when simulations were conducted 16 times.



a. Regular Node's Utility Comparison | b. Malicious Node's Utility Comparison

Figure 7.1 Strategy Comparison For Regular Nodes When Malicious Nodes Employ PBE Strategy.



a. Malicious Node's Utility Comparison | b. Regular Node's Utility Comparison

Figure 7.2 Strategy Comparison For Malicious Nodes When Regular Nodes Employ PBE Strategy.

Journal of Theoretical and Applied Information Technology
10th July 2015. Vol.77. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

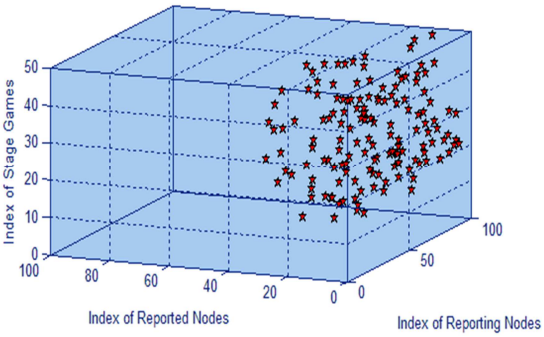


Figure 7.3 Detected False Positives In Regular PBE Versus Malicious PBE Game.

6. PERFORMANCE ANALYSIS

The results accomplished in section 5 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:

6.1 Utility Of Regular Nodes

It has already been ascertained that the PBE strategy outperforms other strategies in all the four scenarios considered, hence will be formed as the basis of all the result analysis. Figures 8.1 and 8.2 depict the utility comparison of regular nodes for the proposed and prior model in completely collaborative and partially collaborative MANET environments respectively. It can be clearly established from Figure 8.1 that the average utility score of regular nodes is almost the same with the prior and the proposed design model in completely collaborative environment. The red and blue streaks beat each other continuously all along the graph without any continuous domination of a single one. The proposed decision model although being much more rational to the prior one could not outshine the prior one because there was no wrong reporting detected on the part of regular nodes in collaborative environment.

When moving to the partially collaborative environment in figure 8.2 it is established that red streaks overwhelmingly surpass the blue ones for most of the stage games. From stage six of the game to the end, the blue streaks continuously dominate the red ones and this domination is only increasing in magnitude. This is due to two reasons; one, larger false positive encountered with the prior model and second, reduction in the unnecessary adoption of mixed strategy by regular nodes with the proposed decision model. The results fetched in figures 8.1 and 8.2 clearly point out to an important fact that there is a radical decrease in the overall network utility (modeled as regular node utility here) when selfish nodes exist among them. Average decline in regular node utility due to selfishness accounts to 24% (approximately). This means the selfishness when exhibited by nodes is in particular one of the core reasons for communication degradation in MANET.

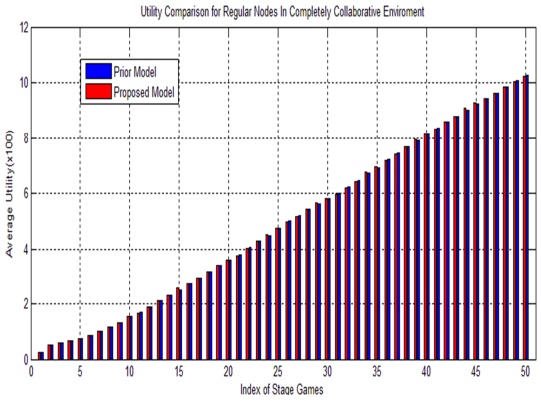


Figure 8.1 Regular Nodes Utility Comparison With Proposed And Prior Model In Completely Collaborative Environment.

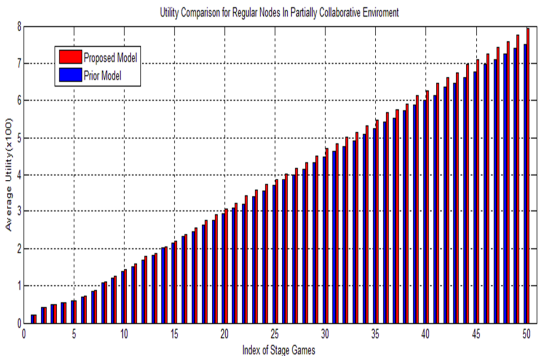


Figure 8.2 Regular Nodes Utility Comparison With Proposed And Prior Model In Partially Collaborative Environment.

6.2 Utility of Malicious Nodes

PBE strategy is formed as the basis for analyzing the utility of malicious nodes. Figures 9.1 and 9.2 depict the utility comparison of malicious nodes for the proposed and prior model in

Journal of Theoretical and Applied Information Technology
10th July 2015. Vol.77. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

completely collaborative and partially collaborative MANET environments respectively.

It can be clearly established from figures 9.1 and 9.2 that the average utility score of malicious nodes is almost the same with the prior and the proposed decision model in both MANET environments. The red and blue streaks beat each other continuously all along the graphs without any continuous domination of a single one. One more implication that can be drawn is the utility of malicious nodes is also slightly decreased when selfishness is exhibited by the regular nodes but it is no match to the decrease which regular nodes suffered.

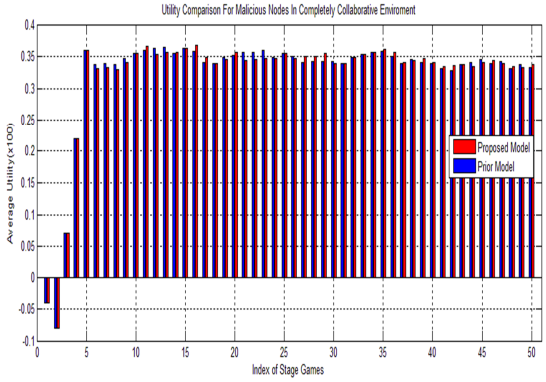


Figure 9.1 Malicious Nodes Utility Comparison With Proposed And Prior Model In Completely Collaborative Environment.

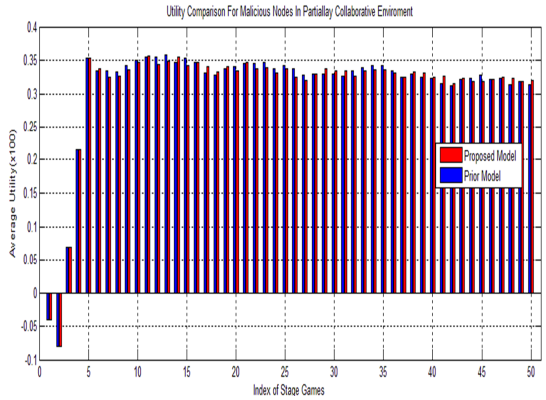


Figure 9.2 Malicious Nodes Utility Comparison With Proposed And Prior Model In Partially Collaborative Environment.

6.3 Detected False Positives

When the proposed and prior models were checked for false positives in completely collaborative environment none was recorded. Figure 10 presents the false reporting done by regular nodes against other regular nodes. False positives have been considered with Regular PBE versus Malicious PBE game only. Red spots in the graph mark the false positives detected with the proposed model while blue ones signify the false positives with the prior one. Following observations can be made from the results fetched in figure 16. Numbers of false positives encountered with the prior model (391) are 2.68 times more than what were detected when employing the proposed model (146). Whenever a regular node makes a false alarm, it suffers a loss of *L;* Thus with more false positives would mean reduced utility for regular nodes as depicted in figure 8.2. The nodes which were wrongly reported as malicious were all selfish nodes only with the proposed model, but that has not been the case with the prior model, even collaborative regular nodes have been alleged as malicious. Occurrence of false positives started early with the prior model in the sixth stage of the game, however with the proposed model the first false positive was detected after the twelfth stage only. Some occurrences of false positives were found in identical triplets (wherein two regular nodes rat each other as malicious in a single stage game) with the prior model, however no such occurrence was observed with the current one.

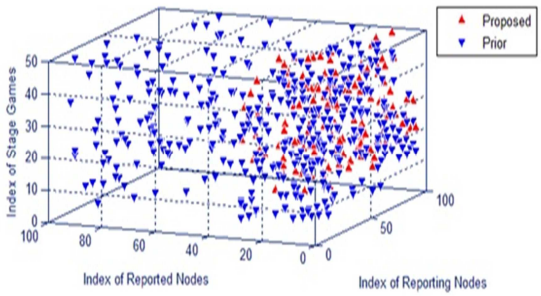


Figure 10: Detected False Positives With Prior And Proposed Model In Partially Collaborative Environment.

7. CONCLUSION AND FUTURE WORK

The current study employed game theory and probability theory to effectively represent the various unpredictable actions of node cooperation, node declination, node attacks, as well as node reporting thus, model the strategic profiling of various mobile nodes. The paper illustrated the formulation of a strategic decision making mathematical model using game theory taking into account the tactics adopted by a regular node, a malicious node and a selfish node, thereby designs

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

game specification. A dynamic Bayesian signaling game is developed for assessing the hidden connection between the various attributes e.g. cost, gain, preferred strategy etc. A comparative work analysis has been conducted for collating the current model with the existing one and to show the enhancement in terms of lesser false positives and higher utility of regular nodes. Results are discussed considering four scenarios to justify that proposed model is successfully able to accomplish similar or better results as compared to base implementation discussed by [16] while preserving the rationality of the mobile nodes. Results fetched show 62.67% decline in occurrence of false positives thus higher overall network utility when selfish or erroneous nodes exist within the regular ones in the MANET.

Currently, the proposed framework doesn't consider the detection or identification of a specific malicious node present in the simulation environment; however, it extracts cumulative and quantified empirical results of the malicious behaviour. Hence, in future we are interested in combining the proposed model with an existing credit based approach to form an Intrusion Detection System. Present study has considered implementing game theory for modelling the malicious behaviour of nodes in MANET. There are some potential results and higher flexibility in implementation approach by the contributory features of game theory. However, the same model can be also reverse engineered using mechanism design (Reverse game theory).

REFRENCES:

[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. Ul Islam Khan, R. Olanrewaju and M. Hadi 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] R. Olanrewaju, B. Ul Islam Khan, R. Naaz Mir and B. Wasiu Adebayo, '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.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[16] F. Li, Y. Yang and J. Wu, 'Attack and Flee: Game-Theory-Based Analysis on Interactions Among Nodes in MANETs', *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, vol. 40, no. 3, pp. 612 - 622, 2010.

[17] R. Agarwal and M. Motwani, 'Survey of clustering algorithms for MANET', *International Journal on Computer Science and Engineering*, vol. 1, no. 2, pp. 98-104, 2009.

[18] K. S. Win, 'Analysis of Detecting Wormhole Attack in Wireless Networks', in *Proceedings of World Academy of Science: Engineering & Technology*, 2008, p. 48.