American Journal of Computer Science and Engineering
2015; 2(3): 10-19
Published online May 10, 2015 (http://www.openscienceonline.com/journal/ajcse)

Behaviour Visualization for Malicious-Attacker Node Collusion in MANET Based on Probabilistic Approach

Rashidah F. Olanrewaju[1], Burhan Ul Islam Khan[2, *], Roohie Naaz Mir[3], Balogun Wasiu Adebayo[4]

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

Email address

burhan.iium@gmail.com (B. U. I. Khan)

To cite this article

Rashidah F. Olanrewaju, Burhan Ul Islam Khan, Roohie Naaz Mir, Balogun Waisu 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, 2015, pp. 10-19.

Abstract

Inspite of wide range of exploration towards the mitigation techniques for malicious nodes in past few years, the effective solutions for addressing the behavioral pattern of malicious nodes are still largely unfound. One of the most challenging dynamics related to this issue is an effective visualization of malicious nodes in the considered simulation techniques. As the malicious nodes will never adopt any strategies which has fairer chances of getting detected, hence, they will perform much confusive behavior based on which it is almost difficult to identify whether it is regular node or malicious node. The current paper accentuates the potentials of game theory considering multi-attacker collusion as the new enhancement that can effectively represent the various unpredictable actions of node cooperation, node declination, node attacks, as well as node reporting that can model the tactical profiling of various mobile nodes.

Keywords

Node Misbehaviour, Mobile Adhoc Network, Malicious Nodes, Routing Misbehaviour, PBE

1. Introduction

In the modern era of networking and communication system, mobile adhoc network [1, 2] has increasingly attracted many researchers for its potential benefits in the line of infra-structure free communication system. From the last decade there has been an extensive research [2] on the grounds of secure routing in mobile adhoc network (MANET). Due to the inherent characteristics of dynamic topology, excessive energy consumption, difficult in taking decision for appropriate routing protocol and no certificate authorization in mobile adhoc network, it has pose a huge challenge in field of security of routing in MANET. Various prior researches have focused on different protocols like reputation systems, virtual currency, batter economy etc. to understand the cause of misbehavior of mobile nodes. The MANET consists of regular as well as malicious node, whose objective is to increase the destruction of valuable resources in the MANET. Identification of mobile nodes types as regular, selfish, or malicious is one of the most difficult task to be accomplished, especially in the presence of large scale MANET system and its unpredictable topology. Hence, the prime factor that controls this study is to extract the illustration of various strategies adopted by different types of the nodes in the simulation study. For the purpose of representing a mathematical decision model of various strategies that could be possible adopted in the communication of large scale MANET system, game theory with multi-level game is used in this study. While doing the preliminary study about the topic, it was found that game theory has been adopted by various scholars for preserving power factor in large scale distributed system [3, 4]. It has also been explored that prior research work didn't emphasize much on the feasibility of various types of strategies of attack methods against various vulnerable node condition, therefore, the proposed study chooses to fill this trade-off by considering collusion based scenario of attacks with

consideration of uncertainty that will be estimated based on the behavior of the malicious nodes.

One of the critical demerits of MANET system is its decentralization as well as its ongoing node mobility which consumes unwanted power and decision of routing protocol thereby posses a great challenging task. Due to this unwanted power drainage as well as limitation of channel capacity, there are some groups of nodes that may chose to reject forwarding or carrying any request from its neighborhood nodes due to its resource constraint. Such nodes are basically termed as erroneous Nodes [5] which rises due to technical issues of power or software/hardware problems. Existence of such nodes can be easily taken advantages by the malicious node which will always have certain harmful intention in order to paralyze the operational aspects of MANET system. However, there is a presence of other types of node in MANET which majorly imitates the behavior of erroneous Node called as selfish node [6].

The characteristics adopted by selfish nodes targets to gain the benefit of network at the cost of other node's resources opportunistically. Selfish nodes do not take part in packet forwarding and they are considered to behave very much rationally as they act opportunistically to gain network resources as advantages. Hence the presence of selfish node is potentially harmful as the similar behavior of the selfish node can be easily imitated by malicious node, which is the point of concern of many security aspects. As there is no presence of integrated digital certificate based node verification policy among two mobile nodes in MANET, hence it becomes almost impossible task to identify the nodes to be regular, or selfish, or malicious.

A malicious node can easily furnish false information at the time of route discovery process by other regular nodes; they choose to participate even in node forwarding in the preliminary phases. This treacherous act of malicious mobile node will eventually gain the trust and belief system of the network where the malicious nodes seeks for an optimal opportunity to initiate a brutal attack on the network. It is to be noted that once the malicious node gains the trust, the more is the intensity of the attack potentially caused damaging various resources in MANET system. One of the most critical issues of such phenomenon is the identification of behavior of different types of nodes. Eventually, using cryptography or any other techniques will do stop and mitigate such attacks but cannot help if the attacking strategy is changed by malicious nodes. Hence, working on intrusion detection system or detecting a malicious node will broaden the scope of study and optimal results on security on large scale MANET cannot be accomplished. Thus, the current research chooses to simulate the decisions adopted by various types of nodes using game-theory that gives a better statistical probability of equilibrium stages.

The paper is organized as: Section 2 explores various security solutions that have been put forth in the prior literature to thwart the misbehaviour of mobile nodes. Section 3 describes formation of proposed model adopting game theory with exclusive elaboration on multi-attacker collusion model, clustering, neighborhood surveillance, etc. All important algorithms 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 section 5. Finally section 6 summarizes the cumulative findings and the contribution of the proposed study.

2. Related Work

From the networking viewpoint, in mobile adhoc networks (MANET), every individual intermediate node is considered to forward the data packet to its neighbor nodes such that the same reaches its destination owing to its mobility. This characteristic of MANET is found to be common in majority of routing protocols as defined by RFCs [7]. However, due to scarcity of enough resources, the same is found to malfunction sometimes that eventually leads to the evolution of selfish nodes [8]. The characteristics adopted by selfish nodes target to gain the benefit of network at the cost of other node resources opportunistically. Selfish nodes do not take part in packet forwarding and they are considered to behave very much rationally as they act opportunistically to gain network resources as advantages. The previous record of studies [9, 10]shows that various attempts has been made to make sure the selfish node doesn't exist much and even if it exist, the routing protocols are amended using various incentive techniques for ensuring forwarding of data packets. 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. Furthermore some credit based solutions (e.g. virtual currency and barter economy) have been also found from the literature to stimulate cooperation among the participating nodes [11, 12]. These credit based solutions generally are not able to draw a line between selfish and malicious behaviour of nodes.

The wireless nature of environment in MANETs actually makes the network more vulnerable and susceptible to various types of attacks which are further heightened by open architecture of MANET system [13]. One of the prominent secure strategies formulated in past studies is by deploying secure routing protocols [14]. Unfortunately, the disadvantage explored even in the secure routing protocols in the past is that they are accompanied by extensive computational overhead that has an exponential adverse effect on the efficiency of communication system in MANET [14].One of the prime targets of the intruder (malicious node) in MANET is to victimize the routing process and thereby affect the entire communication system by not obeying the secure specifications of routing protocols. This fact is further made worse by the dynamic topology and decentralized nature of MANET that welcomes majority of the attacks in such vulnerable wireless atmosphere [15, 16]. One of the most challenging issues in the identification process of malicious node is that the nature of attacking policies are

extremely hard to determine as MANET doesn't have enough security system in their policies and moreover due to the existing correlation between selfish and malicious node behavior. The secondary challenges in the identification process of malicious activities are lack of systematic network surveillance process due to lack of centralized system especially in large scale environment [16]. Attacks on frequently used routing protocols like: Ad hoc On-Demand Distance Vector Routing (AODV) and Destination-Sequenced Distance Vector routing (DSDV) are studied in [17-19]. One of the major discrepancies in all the above mentioned studies are that at any cost, even to a little extent, the intruder node is always successful to block the packet forwarding activities of regular node and thereby they gain an advantage factor at the cost of other regular nodes. All the intrusion studies [17-19] conclude that malicious nodes are highly capable enough to intrude the regular node, capturing the data, corrupt and disrupt the routes, leading to compromisation of the entire large scale environment of MANET system. This fact is really scary when it comes to real time usage of MANET for any specific commercial applications.

Hence, in nutshell, it can be concluded that malicious behavior of MANET is something which is challenging to investigate due to the complex design of attack policies and inherent characteristics of MANET that accelerates the entire vulnerable situation. The summary of the recent work pertaining to mitigation of misbehavior problems of nodes in MANETs is summarized in Table 1 [22].

Table 1. *Summary of the findings*

Author	Contribution	Result Obtained	Limitations
(Suganya and Priya, 2013) [20].	New replication allocation technique	Reduced routing misbehavior in delay tolerant network.	-Effect of false positives is not considered. -Existence of Malicious Nodes not considered.
(Sengathir and Manoharan, 2013) [10].	Developed a security add-on for Multicast Adhoc On Demand Distance Vector protocol.	Effective in detecting misbehaving node.	- No line drawn between Selfish and Malicious nodes. - Malicious Nodes Modeled as fragile. - Not applicable to other routing protocols.
(Kumar et al., 2011) [21].	Designed a novel mechanism to detect misbehavior by a 2 hop acknowledgement.	- Increase in Packet delivery ratio with the add-on for the DSR routing Scheme. - System works pretty good even in presence of comparable number of misbehaving nodes	- Focused on the problem of detecting misbehaving links instead of misbehaving nodes. - Result fetched on a single Routing Protocol i.e. DSR - Effective with consideration of dense MANET environment otherwise will cause network partitioning.
(Rachedi et al., 2010) [11].	Applied Reverse game theory on cluster model to simulate cooperation.	- Prolonged cluster lifetime. - Increased number of clusters and reduction in Cluster's size.	-Validation with respect to security is not done. - Malicious behaviour is not discussed
(Wang and Wu, 2012) [12].	Global punishment based repeated-game model to stimulate node cooperation.	Proposed model enhances node forwarding probability	- Focusing on the node forwarding process rather than malicious behaviour detection or analysis. -Not applicable for Sybil attack, newcomer attack, collusion attacks.
(Li et al. 2010) [23].	Proposes a game theoretic framework to analyze the strategy profiles for regular and malicious nodes.	Formulated PBE strategy outperforms both pure and mixed strategies.	- Does not consider the selfish nodes in the regular node camp. - Collusion between Malicious nodes not considered.
(Anil and Venugopal, 2011) [24].	Created a Virtual Competition situation for Analyzing Behaviour of Malicious Nodes.	Framework is able to recognize the abnormal behaviour of the mobile nodes.	Collusion between Malicious nodes not considered.

3. Proposed System

The current work enhances a mathematical schema of strategical decision making that can model the behavioral pattern of regular and malicious nodes in Mobile Adhoc Network (MANET) inspired by [23, 24]. The work done by the authors is highly empirical and results are evaluated based on consideration of single attacker mobile nodes.

Although the authors have introduced multiple malicious node in the simulation study but presence of multiple malicious node doesn't confirm the presence of multiple-attack events, (attacker nodes coordinating while attacking). Therefore, it is felt that complexity can be more increased when multiple attacker nodes exists in the network with synchronous coordination among them. Therefore, the current study primarily investigates the inherent issues in MANET that poses a potential security threat in MANET by impairing its traditional characteristics of identifying the malicious behavior of the nodes. Review of prior work conducted in the similar area concludes the usage of complex cryptography or proposing Intrusion Detection System or proposing a model for identifying malicious nodes in the network. However, it is explored from literature survey (exclusively from [2, 21, 25]) that such techniques are quite computationally complex leading to less promising results for ensuring better safety traits in MANET. While reviewing some more techniques on security system in MANET, it was also found that game theory has also prime contribution in past few years due to potential accuracy in its probabilistic approach and computational efficiency. Therefore, the proposed system highlights the use of game theory and probability theory considering multi-attacker collusion as the new enhancement that can 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. The proposed framework also considers variation of the patterns with respect to index of stage games (multi-stage) and average utility scored as a measure when performing benchmarking the proposed schema [23]. The prime aim of the proposed study is to perform a statistical analysis and thereby design a mathematical model that illustrates the disagreement in node cooperation by malicious nodes in large scale environment of mobile adhoc network. In order to establish this study aim, following objectives should be met:

1. To consider a large scale environment of MANET for performing the simulation study of node behaviour as classified for regular node and malicious node in formation of multiple clusters on n-number.
2. To formulate a strategic decision making mathematical model using game theory for evaluating the tactics adopted by regular node and malicious node and thereby designs game specification.
3. To assess the complexity of malicious node behaviour by simulating the multiattacker collusion scenario 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 [24] (single attacker) with the proposed system (multi-attacker collusion) with respect to evaluation of belief, utility, and uncertainty.

Although there has been a considerable amount of work done in security aspects of the routing protocols for mobile adhoc networks, but the proposed system gives contrast results compared to all major previous work by considering the probabilistic approach of identifying the routing behaviour of the malicious node. One of the most significant criteria considered for the proposed system is analyzing and distinguishing the behaviour of either regular or the malicious node. The proposed framework will decompose MANET environment into multiple logical regions where the mobile nodes will be distributed and an interactive virtual competition between regular node and malicious node, modeled as Perfect Bayesian Equilibrium (PBE) will be initiated.

Virtual Competition represents the implications of respective roles of individual actions for regular nodes and malicious nodes. For the proposed approach of virtual competition, the mobile nodes will scrutinize the results of each specific communication occurring. In the experiment, each mobile node designs a trust factor towards its neighboring nodes and updates its trust information in accordance to the neighbor's actions as the virtual competition evolves. The best responses of the both regular and malicious node are governed by the threats about specific events from opposite mobile nodes which are completely dependent on their current trust level. The regular node configures a reputation threshold and decides the trust level and its threshold. Whereas the malicious nodes will also estimates the risk, which is computed by the feasibility that a regular node will decide to update other mobile nodes under that condition.

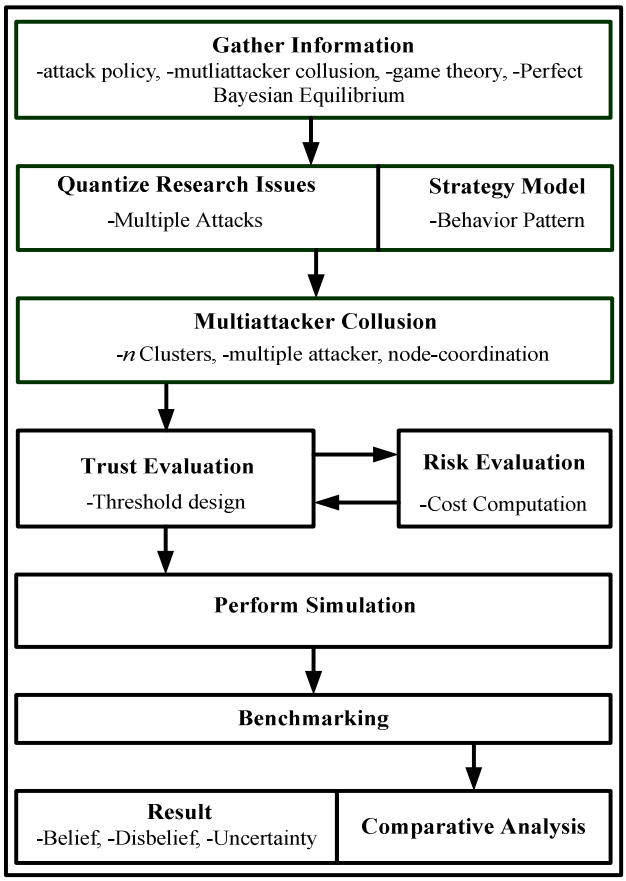
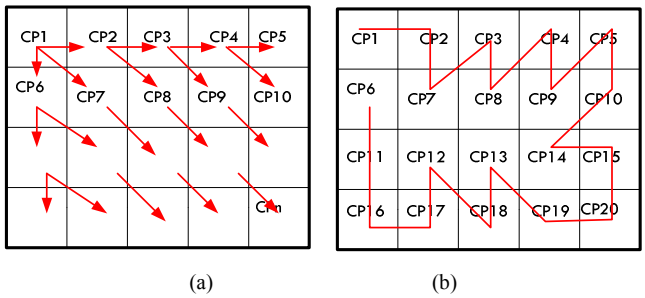


Figure 1. *Process Flow of the Research*

Depending on the threat intensity and expected decamping cost, the malicious node makes an assessment on decamping to other logical region. The contributions of the proposed framework are as follows: 1) Formulation of a Perfect Bayesian Equilibrium considering collusion and co-ordination among the attacker nodes; 2) Projection of decision rules for regular nodes to update and malicious nodes to escape; 3) Securitization of the equilibrium strategy profiles for both parties based on the trust and expected payoff; exposes the association between node's superlative response and the cost and gain of each individual policy. The main target of the framework will be to understand the condition of decamping to other logical region by malicious nodes, as the behaviour of the malicious node will be programmed in such a way that whenever they will attempt to decamp to another logical region, it will completely erase the routing history of the previous logical region where it was previously residing in.

The process flow diagram of the current research is revealed in Fig 1. Prior researches in this field [10] have not succeeded to consider the feasibility that an intruder might select different threat frequencies toward different opponents whereas the proposed work considers more *Smart and Sophisticated* malicious nodes, making the regular and malicious node competition in this proposed model more realistic. The proposed framework characterizes the regular / malicious node with virtual competition as a multi phase scheme to find the optimal policy of regular and malicious nodes for computing the general decision process of regular and malicious mobile nodes. The neighboring surveillance policy assists the regular node to receive the feedback from neighboring mobile node at that instant and computes the trust and adequacy of the proof towards the opposite mobile node depending on the quantity of the identified cooperation and attacks on routing. The system incorporates in itself a threshold schema to choose whether to rat other mobile nodes as malicious in the logical region or not. If not the regular node chooses to assist with the probability which is estimated depending on the trust level. Not only this, the malicious node also estimates the threat of being caught in its existing location, so it follows its protocol to decide whether it should decamp to another logical region or not. If not, the malicious mobile node will choose to attack. The prime issue in this decision process is working out of decision rules for both regular and malicious nodes corresponding to the event profiles shown by the probability that the regular node cooperates and the probability that the malicious node attacks. Furthermore the system analyzes the mobile adhoc network milieu to identify the optimal decision protocols and events by deploying the framework which chooses to achieve Perfect Bayesian Equilibrium.

A unique attacker model based on multi-collusion has been incorporated wherein the attacker nodes coordinate before conducting any attacks. Collusion is an conformity between two or more parties, sometimes illegitimate and therefore secretive, to limit open competition by deceiving, misleading, or defrauding others of their legal rights, or to obtain an objective forbidden by law typically by defrauding or gaining an unfair advantage[26].



(a) (b)

Figure 2. *Example Scenario of malicious node coordination.*

The design aspect of the proposed considers that framework has initially completely vague information about the type of the nodes, which would mean that the user doesn't have any control over the attack behaviour, user just creates it and distribute them (malicious nodes) inside the simulation area. However, interestingly understanding how collusion attacking works seems perceptive, but the focal point is that, Can it be targeted for massive collateral damage in the network? Hence, in order to support for higher degree of damage in the network, a novelty in the attacker module has been proposed by introducing the concept of auto-coordination among all the attacker nodes present in the simulation area. The prominent concerns to be understood here are:

- Even a malicious node also possesses resource constraint due to which reason they may too act as selfish nature. In that situation, the communication among the malicious nodes will not be possible. So, how to make a dedicated communication channel among the malicious nodes and how it helps them.
- Another important issue is how to segregate malicious node and regular node?

The prime objective behind employing the particular attacker module is to introduce supplementary security challenges in order to evaluate the protocols. Considering the example shown in Fig.2, the malicious node present in cluster position CP_1 after initiating an attack and before performing the decamping mechanism, it has a very limited time to perform this coordination activity. Another important fact is existence of same believe between two set of nodes does not mean that both are regular node. The dominant characteristics of regular node are always to cooperate in terms of communication viewpoint and thereby belief increases. However, a malicious node cooperates with an objective of breaching the belief system of the regular node. Hence, the system performs temporal analysis of the simulation to extract 3 main parameters:

- Belief
- Uncertainty
- Probability of Malicious Node

Evaluation of the above terms would highlight the difference between regular and malicious nodes. Hence, it is highly feasible to establish a dedicated communication channel among the malicious nodes, provided parallel task performs above three parameters computation. Referring Fig.2 (a), it can be seen that malicious node present in cluster position CP1 have chances to communicate with its neighborhood attacker nodes CP2, CP6, and CP7. Similarly, once communication established, anyone among them can extend to their respective neighbor attacker nodes. The process continues while storing the cluster ID in order to avoid redundancy of C_{info} among them. In nutshell, it would mean that the overall communication channel which encapsulates all the attacker nodes without any repetition will be compromised as depicted in Fig.2 (b).

4. Implementation

The comparative performance analysis has been conducted by considering strategies adopted in proposed system to that of prior research work conducted [24] in the run-time of

simulation. Although there are various types of event simulators like NS2, OMNet++, OPNet, but, the proposed system will be designed on Matlab. The discreet event simulators are good for evaluating routing protocols and any security issues where the parameters (size of keys, mobility, etc) are quite fixed. However, our requirement is quite different. We require a tool that can perform better simulation considering multiple case studies (consideration of multiple stage games) and evaluate the results. The focus here is not actually the accomplishment of animated simulation that can be seen in discrete event simulator but we are looking forward to implement probabilistic model and check the results of various strategies. It should be noted that development of strategies in dynamic and highly unpredictable environment of MANET is quite challenging to design in discreet event simulators as customization is extremely less in scripting, whereas Matlab do not have any such restrictions. If the design pattern can be created for various vulnerable scenarios of MANET, than programming in Matlab can lead to effective results. Thus the current framework has been designed and simulated in Matlab environment with a visualization of MANET environment described above along with empirical values being extracted from each phases of simulation study that can potentially assist the researcher to investigate the malicious behavior of mobile nodes in MANET.

In order to carry out the discussed objectives, the proposed study has made the following assumptions:

- Existence of free space propagation model.
- Malicious mobile node doesn't initiate an attack in the preliminary stages of node cooperation in order to prevent getting them from being caught.
- As the computational scenario of the proposed system is extremely challenging task, so it is assumed that there is a less probability of error in any observation.
- It is assumed that the verification procedure takes place in each cluster where the individuality of a node is bounded with its physical properties that cannot be altered or duplicated when the mobile node resides in the transmission range of its cluster.
- As the proposed communication system is modeled in game theory, so, each node (player) are permitted to access the part of the confidential information (in order to show the attack event), so this process may highly influence the progress of the game (as multi-stage game is considered in proposed system).
- It is assumed that each type of the nodes selects their action and formulates their strategies based on their belief system and confidential information.
- 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.

The proposed system has considered a wide range of policies of intrusion within a dynamically generated mobile adhoc network in Matlab platform. The regular node is considered to follow its respective neighboring transmitted message by neighbor monitoring. A simulation framework of 1600 x 1600 m is designed with 240 mobile randomly positioned with a transmission range of 300 meters. The entire simulation area is designed with multiple logical areas (clusters). A random waypoint mobility model is designed and any two nodes in the same cluster are considered as neighboring nodes. The algorithm for packet forwarding by the malicious node while performing auto-coordination among them is as below:

Algorithm-1: Co-ordination between malicious nodes

Objective: The prime objective is to create a dedicated stabilized link between the considered attacker node and attacker nodes in its proximity.

Input: Location of cluster being compromised, node parameters, time (T_h), neighbor nodes.

Output: A Stabilized link between multi-attacker nodes

Steps:

1. *Start*
2. *If*
3. *A malicious node MN_2 is interested in forwarding within T_h*
4. *Then*
5. *MN_1 checks the possible cluster position CP_2 so that CP_2 can carry the compromised event information C_{info} to*
6. *If cluster position CP_2 is closer to the destination D than CP_1*
7. *Then*
8. *MN_1 forwards the C_{info} to MN_2*
9. *Else*
10. *MN_1 continues to wait other malicious node which is interested in forwarding C_{info}.*
11. *End*
12. *Else*
13. *When there is no malicious node which is interested in forwarding the C_{info} at position P1, MN1 has to drop the bundle packet, since the next-hop route is not immediately available*
14. *End*
15. *End*

Algorithm-2: Design of Random Mobility Model.

Objective: The goal of this algorithm is to estimate all the attributes related to mobility and also allocate new positions for the mobility of the nodes from its prior position.

Input: Current positional coordinates for a node, Simulation area length and breadth, estimated velocity pertaining to node movement, random waiting time.

Output: The program estimates all the attributes pertaining to the mobility of nodes within Simulation Area.

Steps:

1. *Start*
2. *Induct current coordinates for the node i.e. x_{old} and y_{old}.*
3. *Formalize Velocity, Sim_{length} and Sim_{width}.*
4. *Design a function for calculating attributes.*
5. *Apply Relative Euclidean distance formula.*
6. *Compute primary arbitrary node location (Ar_{loc1}) .*

7. *Compute secondary arbitrary node location (Ar_{loc2}).*
8. *Compute new location of x_{old} coordinate (x_{newPos}).*
9. *Compute new location of y_{old} coordinate (y_{newPos}).*
10. *If ($x_{newPos}<0$ || $x_{newPos}>Sim_{length}$)*
11. *Assign (x_{old}-Ar_{loc1}) to x_{newPos}*
12. *End*
13. *If ($y_{newPos}<0$ || $y_{newPos}>Sim_{width}$)*
14. *Allocate (y_{old}- Ar_{loc2}) to y_{newPos}.*
15. *End*
16. *End*

Algorithm-3: Estimating likelihood of Attacker Node [24].

Objective: The goal is to estimate the likelihood of an attacker node in the MANET environment.

Input: Number of detected attacks and Cooperation.

Output: Computation of the likelihood of an attacker node.

Steps:

1. *Start*
2. *Formalize the quantity of identified successful communications (Q_{com}).*
3. *Formalize the quantity of identified communication disruptions (Q_{int}).*
4. *Design a function for computing likelihood of an attacker node.*
5. *Initialize likelihood that the node is an attacker node (L_{attack}).*
6. *Apply Formula:* $L_{attack} = \frac{Q_{com}}{(Q_{com} + Q_{\text{int}})}$.
7. *End*

Algorithm-4: Computing attribute of Trust [24].

Objective: The goal is to compute the attribute of trust by considering quantity of identified communication, intrusion, and uncertainty in the susceptible environment of MANET

Input: Number of detected cooperation and declines, degree of uncertainty level.

Output: Computation of attribute of Trust

Steps:

1. *Start*
2. *Formalize quantity of identified communication (Q_{com})*
3. *Formalize quantity of identified intrusion (Q_{int})*
4. *Formalize Uncertainty in the decision (U_{dec})*
5. *Design a function for computing the trust*
6. *Allocate L_{attack} (from Algorithm-3) to $Trust_{vector1}$*
7. *Allocate (1-U_{dec}) to $Trust_{vector2}$*
8. *Computer ultimate Trust ($Trust_{Ultimate}$) in the decision by applying formula: $Trust_{Ultimate}$= $Trust_{vector1}$+ $Trust_{vector2}$.*
9. *End*

Algorithm-5: Computation of uncertainty of decision [24].

Objective: The goal is to compute the uncertainty in the decision process of the regular node.

Input: Number of detected cooperation and declines.

Output: The program gives the estimation of uncertainty in decision.

Steps:

1. *Start*
2. *Formalize quantity of identified communication (Q_{com}).*
3. *Formalize the quantity of identified failures (Q_{int})*
4. *Design a function for computing uncertainty.*
5. *Estimate Uncertainty in the decision (U_{dec}) by formula: U_{dec} = 12 x Q_{com} x Q_{int} / {(Q_{com} + Q_{int})2 x(Q_{com} + Q_{int} +1)}.*
6. *End*

5. Result Discussion

This section discusses about the results being accomplished from the experimental test bed. For the purpose of benchmarking, the proposed system is collated with the base work done in [23, 24]. Similar simulation parameters have been selected as that put forth in [23] for the purpose of comparative analysis. The results accomplished are basically of two kinds, one representing the single attack scenario [24] and other depicting the proposed multi-attacker module.

Fig.3 shows the performance analysis of [24] with the proposed system considering Regular Node Utility (a), Malicious Node Utility (b), Belief (c), and Uncertainty (d). In first hand, visualizing the results in this case shows no much significant difference in both the approaches as the experimentation test bed has been kept same. In [23, 24] authors have worked on 9 clusters considering packet drop attack and accomplished the above mentioned results, which illustrates that occurrence of malicious nodes for fleeing activity causes the vibrations (very close peaks in the curve-(c) and (d)) in belief and uncertainty. After the malicious nodes flee to a new destination, it is intruding again with a clean history. As the malicious nodes' strategy selection becomes more diverse in later stages, the regular node's belief are found to converge. When the malicious node uses the mixed strategy, it is more deceptive. It can be seen that the curve for the mixed strategy has a ladder shape (b). However, the malicious node will still be reported by the regular node. When applying the Perfect Bayesian Equilibrium (PBE) strategy, the malicious node has a good chance of escaping from being reported by employing fleeing action. However, it should be noted that the attack module which has been considered here is more complicated than [23]. The current study considers multi-attacker collusion where the dimensionality of attack is many folds fatal than that of [23, 24]. The bigger issue here is once the attacker node migrates to a new cluster, the C_{info} is passed on to its neighbor attacker nodes, who can also initiate an attack in the same old cluster position. Basically, it would not be possible for any attacker node to compromise all the nodes present in one cluster, and hence, when the attacker nodes allows its neighboring attacker nodes to perform re-attack on the same cluster, possibility of compromisation of all the nodes present in a cluster exponentially increases. To summate, it can be concluded that present attacker module has the capability to compromise a larger number of nodes present in large scale mobile adhoc network. Hence, the individual

compromisation result accomplished as depicted in Fig.3 eventually shows the best result as similar simulation environment is considered.

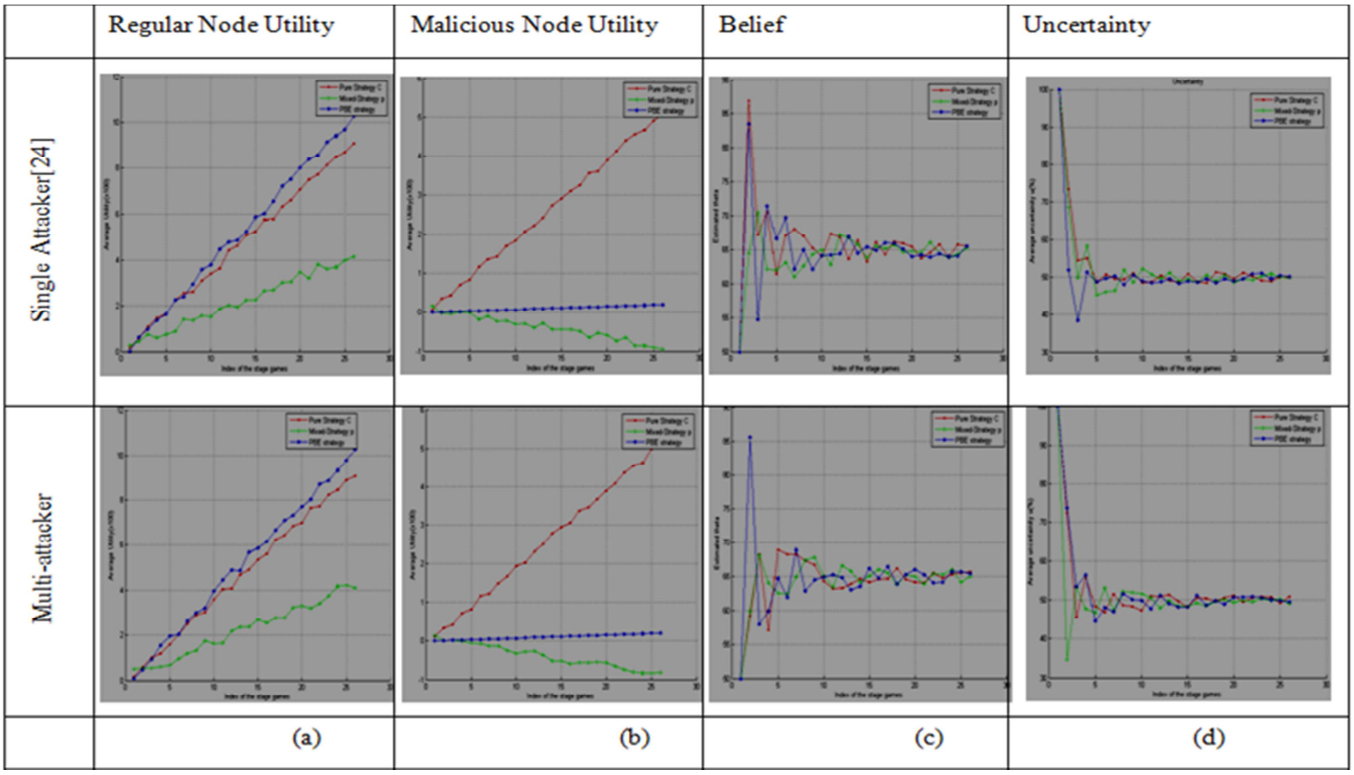


Figure 3. *Analysis of Single and Multiple Attacker Modules.*

It can be seen from Figure 4 when the proposed framework when evaluated with respect to multi-stage games, that, increase of index of games are witnessed by minimization of belief system of the malicious nodes as the countermeasure. Hence, the proposed system not only performs computation of the dominant strategies to accomplish Perfect Nash Equilibrium but also it performs mitigation of the belief system of the malicious nodes. In nutshell, it ensures that probability of the node being malicious (theta) is minimized thereby safeguarding the communication system in large scale MANET.

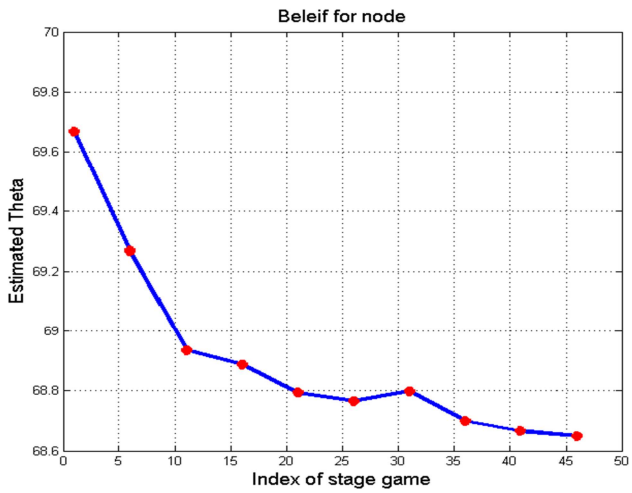


Figure 4. *Benchmarked Computation of Belief of proposed system*

One of the prime goals of the proposed study is to formulate decision making. Hence, lower the value of uncertainty, higher is the extensibility of decision making strategies of the node. The simulation results obtained in Fig.5 shows that with the increase in index of games, the uncertainty converges down showing the best possible mitigation procedure being applied.

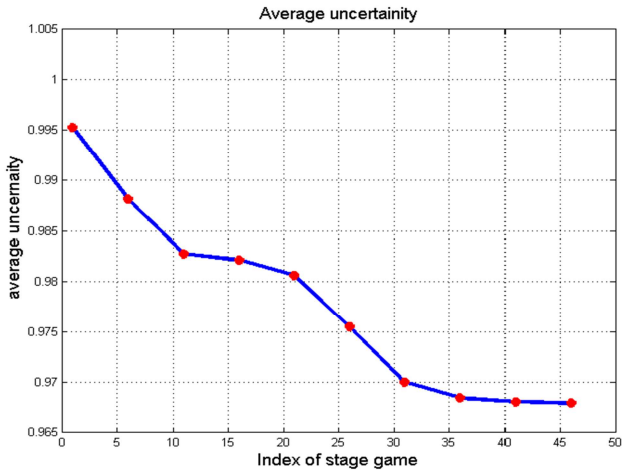


Figure 5. *Benchmarked Computation of Uncertainty of proposed system*

It is always seen that whenever security protocols designed by any means are studied, it usually comprises of study of packet delivery ratio to ensure that whether higher computation has any adverse effect on its communication

system. Hence, in this paper it is decided to consider evaluating packet drop ratio hypothetically just to check whether potential computation of belief, uncertainty and extracting dominant strategies to accomplish Perfect Bayesian Equilibrium has any effect on packet delivery ratio as it involves multi-stage games. It can be ascertained from Fig. 6 that packet drop ratio is found to increase for proposed attacker module as compared to single attacker [24]. Hence, it can be accertained that proposed system has successfully accomplished perfect Bayesian equilibrium both from security and QoS viewpoint. Thus, countermeasures highly effective in the scenario of, black hole attack or Distributed Denial of Service attack in a large scale MANET.

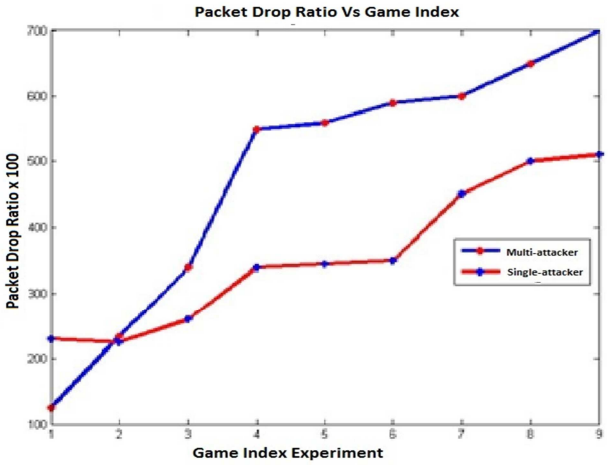


Figure 6. *Evaluation of Packet Drop Ratio*

6. Conclusion

In this paper, framework projected has been designed as virtual competition which is mapped with expected policies to be adopted by regular node to update and malicious node to attack using Perfect Bayesian Equilibrium. The simulation shows better accuracy of catching the malicious nodes, their behavior at every cycle, and their policy adopted to decamp to a new logical region. The current study has identified some of the computationally challenging task pertaining to the security aspects of mobile adhoc network using game theory to analyze the behavioral pattern of various nodes in mobile adhoc network. The system can illustrate the rationale behind the node's adopted behavior considering both regular as well as malicious node. The efficiency of the proposed system can be claimed due to adoption of perfect Bayesian equilibrium for understanding the effect of various empirical parameters (number of detected cooperation/attack, payoff, uncertainty, belief, etc) being evaluated in the due course of simulation. It is believed that the accomplished results can open up various research works in further and can address the modeling of dynamic behavior of malicious activities of the nodes present in MANET effectively. However, it should be known that study on MANET security aspect is still in infancy stage that requires more standardization on security protocols and evaluation in large scale networking system as the network is highly susceptible to attacks as compared to any other wired network and infrastructure based networks.

Acknowledgements

I would like to express my sincere gratitude towards Prof. A. G. Lone; I could see myself becoming a researcher just because, coincidently he was teaching mathematics at the same Engineering College from where I graduated. Second, I appreciate the efforts of my FYP students Bisma Rasool and Tehseen Mehraj in this very venture.

References

[1] Loo, Jonathan, Jaime Lloret Mauri, and Jesús Hamilton Ortiz, eds. *Mobile Ad Hoc Networks: Current Status and Future Trends*. CRC Press, 2011.

[2] Visalakshi, P., and S. Anjugam. "Security issues and vulnerabilities in Mobile Ad hoc Networks (MANET)-A Survey." *International Journal of Computational Engineering Research (IJCER) ISSN*: 2250-3005.

[3] Abraham, Ittai, Danny Dolev, Rica Gonen, and Joe Halpern. "Distributed computing meets game theory: robust mechanisms for rational secret sharing and multiparty computation." In *Proceedings of the twenty-fifth annual ACM symposium on Principles of distributed computing*, pp. 53-62. ACM, 2006.

[4] Roy, Sankardas, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, Vivek Shandilya, and Qishi Wu. "A survey of game theory as applied to network security." In *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*, pp. 1-10. IEEE, 2010.

[5] Yang, Hao, Haiyun Luo, Fan Ye, Songwu Lu, and Lixia Zhang. "Security in mobile ad hoc networks: challenges and solutions." *Wireless Communications, IEEE* 11, no. 1 (2004): 38-47.

[6] Schütte, Martin. "Detecting selfish and malicious nodes in MANETs." In *seminar: sicherheit in selbstorganisierenden netzen, hpi/universität potsdam, sommersemester*. 2006.

[7] Junhai, Luo, Ye Danxia, Xue Liu, and Fan Mingyu. "A survey of multicast routing protocols for mobile ad-hoc networks." *Communications Surveys & Tutorials, IEEE* 11, no. 1 (2009): 78-91.

[8] Yoo, Younghwan, and Dharma P. Agrawal. "Why does it pay to be selfish in a MANET?." *Wireless Communications, IEEE* 13, no. 6 (2006): 87-97.

[9] Probus, Michael Wayne. "Selfish node isolation in mobile ad-hoc networks." PhD diss., University of Louisville, 2007.

[10] Sengathir, J., and R. Manoharan. "Security Algorithms for Mitigating Selfish and Shared Root Node Attacks in MANETs." *International Journal of Computer Network and Information Security (IJCNIS)* 5, no. 10 (2013): 1.

[11] Rachedi, Abderrezak, Abderrahim Benslimane, Hadi Otrok, Noman Mohammed, and Mourad Debbabi. "A secure mechanism design-based and game theoretical model for manets." *Mobile Networks and Applications* 15, no. 2 (2010): 191-204.

[12] Wang, Kun, and Meng Wu. "Nash equilibrium of node cooperation based on metamodel for MANETs." *journal of information science and engineering* 28, no. 2 (2012): 317-333.

[13] Jiang, Ning, Kien A. Hua, and Danzhou Liu. "A scalable and robust approach to collaboration enforcement in mobile ad-hoc networks." *Communications and Networks, Journal of* 9, no. 1 (2007): 56-66.

[14] Striki, Maria, John S. Baras, and Kyriakos Manousakis. "New Algorithms for the efficient design of topology-oriented Key Agreement Protocols in Multi-hop Ad Hoc Networks." In *Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops, 2008. WiOPT 2008. 6th International Symposium on*, pp. 384-393. IEEE, 2008.

[15] Goyal, Priyanka, Sahil Batra, and Ajit Singh. "A literature review of security attack in mobile ad-hoc networks." *International Journal of Computer Applications* 9, no. 12 (2010): 11-15.

[16] Khan, Burhan Ul Islam, Rashidah Funke Olanrewaju, and Mohamed Hadi Habaebi. "Malicious Behaviour of Node and its Significant Security Techniques in MANET-A." *Australian Journal of Basic and Applied Sciences* 7, no. 12 (2013): 286-293.

[17] Zapata, Manel Guerrero. "Secure ad hoc on-demand distance vector routing." *ACM SIGMOBILE Mobile Computing and Communications Review* 6, no. 3 (2002): 106-107.

[18] Hu, Yih-Chun, Adrian Perrig, and David B. Johnson. "Ariadne: A secure on-demand routing protocol for ad hoc networks." *Wireless networks* 11, no. 1-2 (2005): 21-38.

[19] Singh, Gunjesh Kant, Harminder Singh Bindra, and A. L. Sangal. "Performance Analysis of DSR, AODV Routing Protocols based on Wormhole Attack in Mobile Ad-hoc Network." *International Journal of Computer Applications* 26, no. 5 (2011): 38-41.

[20] Suganya, N. R., and S. Madhu Priya. "Detecting Selfish Nodes in a MANET through Fragmentation in Distributed Environment." *International Journal of Science, Engineering and Technology Research* 2, no. 6 (2013): pp-1370.

[21] Kumar, Rakesh, Piush Verma, and Yaduvir Singh. "Design and Development of a Secured Routing Scheme for Mobile Adhoc Network." *International Journal of Computer Applications (0975–8887) Volume* (2011).

[22] Khan, Burhan Ul Islam, Rashidah Funke Olanrewaju, Farhat Anwar, and Asadullah Shah. "Manifestation and mitigation of node misbehaviour in adhoc networks." *Wulfenia Journal* 21, no. 3 (2014): 462-470.

[23] Li, Feng, Yinying Yang, and Jie Wu. "Attack and flee: game-theory-based analysis on interactions among nodes in MANETs." *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on* 40, no. 3 (2010): 612-622.

[24] Anil, G. N., and A. Venugopal Reddy. "Strategical Modelling with Virtual Competition for Analyzing Behavior of Malicious Node in Mobile Adhoc Network to Prevent Decamping." *IJCSI* (2011).

[25] Cordasco, Jared, and Susanne Wetzel. "Cryptographic versus trust-based methods for MANET routing security." *Electronic Notes in Theoretical Computer Science* 197, no. 2 (2008): 131-140.

[26] Wang, Xin-ping, Cui-hua Wu, Shao-hui Zou, Wan-xian Li, and Wei-wu Wan. "Research On The Questions Of Collusion And Collusion-Proof Equilibrium On The Quality Management System Certification Market In China." In *Service Systems and Service Management, 2006 International Conference on*, vol. 2, pp. 1299-1304. IEEE, 2006.