Strategical Modelling with Virtual Competition for Analyzing Behavior of Malicious Node in Mobile Adhoc Network to Prevent Decamping

Anil G.N[a], Dr. A. Venugopal Reddy[b]
[a]Assistant Professor, Department of CSE, BMS Institute of Technology, Bangalore, India,
[b]Professor & Principal, University College of Engineering, Osmania University, Hyderabad, India,

Abstract: The proposed system highlights a novel approach of identifying dynamic misbehaviour of the malicious node in mobile adhoc network. The main aim of the proposed work is to implement a new technique in the attack scenario of distributed network of MANET in order to analyse the policies and patterns of attack originated from malicious node and their tendency to decamp to another new logical region from the old one after attack which is accomplished using Perfect Bayesian Equilibrium. The architecture is also designed in most challenging scenario as when the mobile node will decamp to new logical region it will erase its previous actions in old logical region, for which it will be most difficult task to identify the malicious node. Such situation also will give rise to false positive rate of detection by the regular nodes. Therefore a trust model is designed which is always updated by the regular node. The proposed simulation identifies an instance of decamping with estimation of improbabilities as well as various policies owned by the malicious node.

Keywords: Node Misbehaviour, Mobile Adhoc Network, Non-Cooperation, Routing Misbehaviour

I. INTRODUCTION

From the last decade there has been an extensive research [1] for the cause of secure routing in mobile adhoc network (MANET). Due to the inherent charecteristics 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 has focused on different security protocols designed like reputation system, virtual currency etc. has been implemented to understand the cause of misbehaviour 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. The main focus of the proposed system will be:

- How to distinguish between the regular and malicious node in MANET environment based on their dynamic behaviour which is difficult to predict?
- What exactly happens when the any malicious node attempt to drop the packet, which is quite possible even by using reputation system used extensively in prior research work?
- In case of multiple-logical region of simulation, what if the malicious node generates an attack in one logical region and itself arrives in one new logical region by erasing the past identification of the malicious node?
- As malicious node will attempt to behave exactly like a regular node in distributed environment of MANET for gaining the trust, it will eventually violate the price-based system proposed in the many prior research work [2].
- Can the appropriate value of the probability of malicious node and regular node can be estimated in run-time?
- Can the uncertainty or the trust value can be estimated? Can the number of detected co-operation or attacks can be estimated accurately in run-time?

If the above mentioned parameters can be defined and computed, there is a possibility of creation of a robust and secure model for better analyzation of nodes strategy (Regular / Malicious) in the MANET system. The rest of this paper is organized as follows. We discuss Problem Statement in Section II. The related work is discussed in Section-III. Proposed System will be discussed in Section-IV. Methodology for the research work is elaborated in Section V. Implementation is described in Section-VI and performance analysis followed in Section-VII. Finally Conclusion is discussed in Section-VIII.

II. PROBLEM STATEMENT

The fundamental issue with frequently used routing protocols is that they rely all mobile nodes of network and based on the assumption that nodes will behave or cooperate properly but there might be a condition where some nodes are not behaving properly. Majority of the adhoc network routing protocols becomes inefficient and shows reduced performance while mitigating with big number of misbehaving nodes. Such set of misbehaving nodes support the flow of route discovery traffic but interrupt the data flow, causing the routing protocol to restart the route-discovery process or to select an alternative route if one is available.

The absence of an infrastructure and consequently the absence of authorization facilities impede the usual practice of establishing a line of defense-distinguishing nodes as trusted or non-trusted. Freely roaming nodes form transient associations with their neighbors: they join and leave sub-domains independently with and without notice. In such vulnerable situation, the compromised mobile node will definitely cause potential Byzantium failures in the routing protocols in MANET. In such type of Byzantine failure, a set of the mobile nodes could be attacked in a specific procedure that erroneous and malicious actions cannot be even identified.

The malicious node present has the policy of decamping to another logical region from their present one in order to circumvent of being trapped. The worst situation is when the malicious node decamps to a new logical region; they will tend to erase the previous history of their actions which will defiantly results in increase in false positive rates in updates in MANET. However, this supplementary approach does not confirm that malicious nodes will incessantly compromise other nodes present in the network and will attempt to escape since decamping is also connected with a cost (e.g., the power depleted to shift to the newly chosen destination).

III. RELATED WORK:

Recently, numerous approaches have been proposed to deal with the node non-cooperation problem in wireless networks. They generally can be classified into two main categories: reputation systems and price-based systems. We use a monitoring and reputation system [3] as the basic setting for regular nodes. Many related works also use reputation systems [4]–[6] and a game theory model [7] to analyze the problem. Some recent works have studied the incentives for malicious nodes and modeled their behavior more rationally. In [8], Liu et al. present a general incentive-based method to model the attackers' intents, objectives, and strategies. In [9], Theodorakopoulos and Baras further study the payoff of the malicious nodes and identify the influence of the network topology. However, the good nodes' behavior in [10] is simple, and it fails to consider the possibility that an attacker might choose different attack frequencies toward different opponents.

The security problem and the misbehaviour problem of wireless networks including MANETs have been studied by many researchers e.g. [10], [11], [12], [13].Various techniques have been proposed to prevent selfishness in MANETs. These schemes can be broadly classified into two categories: credit-based schemes and reputation based schemes. The basic idea of credit-based schemes is to provide incentives for nodes to faithfully perform networking functions. Nodes get paid for providing services to other nodes. When they request other nodes to help them for packet forwarding, they use the same payment system to pay for such services.

Sanjeev Rana [14] has created a mechanism with the help of which it prevents various replay attacks and also activate the neighboring nodes to control the behavior of its neighbors to thwart active attacks. Rakesh Kumar e.t. al [15] has implemented a prototype of key management service by using genetic algorithm. Rajib Das e.t. al [16] has proposed a solution against black hole attack and has illustrated the effect of black hole attack on network performance. However, the results cannot be considered as optimal. Kannan e.t. al [17] has published an extensive survey on various attacks, and their respective countermeasures with respect to vulnerability in routing protocols. Aishwarya Sagar [18] has proposed an approach based on reputation system that deals with routing misbehaviour and consists of identification and separation of misbehaving nodes. Hariharan e.t. al [19] has proposed a new technique termed as recommendation based on identification of routes with misbehaved nodes. Usman e.t. al [20] have analyzed the effects of different types of jammers using Conservation of Flow (CoF), which has been useful for detecting other attacks, in the wired networks. Abbas [21] have categorized reputation based schemes based on monitoring approaches: active and passive based acknowledgments. Finally, the authors have discussed their pros and cons as well as some other important identity related issues.

IV. PROPOSED SYSTEM

Although there considerable amount of work done in security of the routing protocols on mobile adhoc network, but the proposed system gives higher contrast result 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 node or the malicious node. The proposed model will be composed for multiple logical regions where the mobile nodes will be distributed and will be addressed as an interactive virtual competition between regular node and malicious node as Perfect Bayesian Equilibrium.

Virtual Competition represents the implications of respective roles of individual actions for regular nodes and malicious nodes. In this proposed approach of virtual competition, the mobile nodes will scrutinize the results of each specific communication occurring. In the experiment, each mobile node will design a trust factor towards its neighboring nodes and update their 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 computated by the feasibility that a regular node will decide to update other mobile nodes under that condition.

Depending on the threat level and expected decamping cost, the malicious node makes a decision on decamping to other logical region. The contributions of this proposed system are as follows: 1) We formulate a Perfect Bayesian Equilibrium to study the behavior policy of regular and malicious nodes in mobile adhoc network with respect to its routing; 2) we propose decision rules for regular nodes to update and malicious nodes to escape; 3) we study the equilibrium strategy profiles for both parties based on the trust and expected payoff and expose the association between nodes' superlative response and the cost and gain of each individual policy; and 4) we will present several countermeasures to restrict the decamping policy. The main intention of the proposed system will be to understand the condition of decamping to other logical region by malicious nodes, because 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 almost erase the routing history of the previous logical region where it was prior residing.

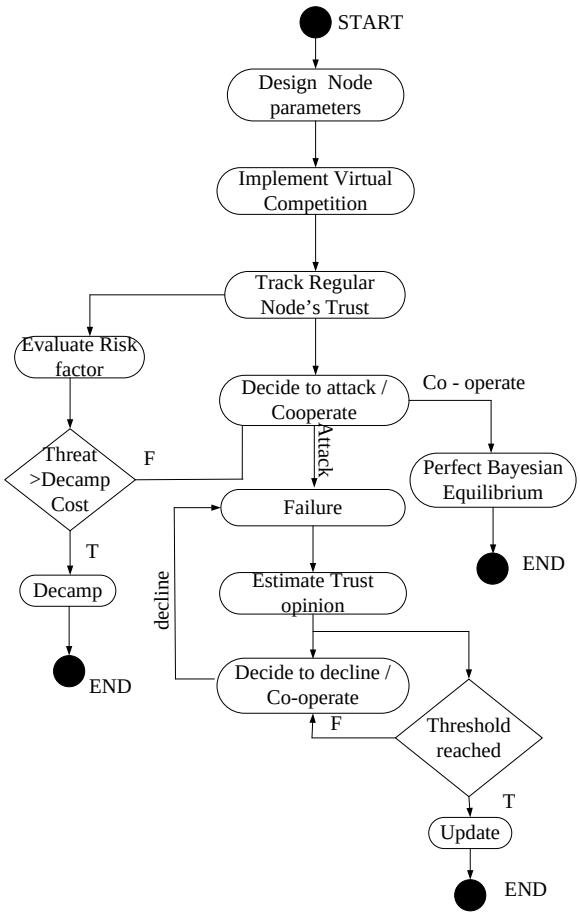

Fig 1. Flow of the Proposed Model

The flow diagram of the proposed system is shown in Fig 1. Prior researches in this field has not succeeded to consider the feasibility that an intruder might select different threat frequencies toward different opponents whereas the proposed project work considers more "Smart" malicious nodes, making the regular and malicious nodes' competition in this proposed model more realistic. This is the reason of deploying the proposed algorithm.

V. METHODOLOGY

The proposed contribution for project is to represent 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 monitoring policy will assist 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 identifying cooperation and number of identifying attacks on routing. The proposed system also observes a threshold schema to choose whether to update other mobile nodes 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 the decision rules for both regular and malicious nodes and the event profiles shown by the probability that the regular node cooperates and the probability that the malicious node attacks. The proposed system analyzes the mobile adhoc network to identify the optimal decision protocols and events by deploying the framework which chooses to achieve perfect Bayesian Equilibrium.

The algorithms deployed are discussed below.

Algorithm: Mobility Model
Objective: The main objective of this algorithm is to estimate all the parameters (nodes, velocity of node, length and width etc) and it also assigns the new positions for the movement of the nodes from its old position.
Input: x-node, y-node, speed, length and width
Output: The program estimates all the parameters responsible for the mobility model of MANET.
Steps:
1 *Initialize x-node, y-node, speed, length and width*
2 *Create a function for calculating parameters*
3 *Calculate first random position (r_1) for the node to travel*
4 *Calculate second random position (r_2) for the node to travel*
5 *Estimate new position of x-node (x-new)*
6 *Estimate new position of y-node (y-new)*
7 *If (x-new<0 || x-new>length)*
8 *Assign (x-node-r_1) to x-new*
9 *End*
10 *If (y-new<0 || y-new>width)*
11 *Assign (y-node-r_2) to y-new*
12 *End*

Algorithm: Estimating Probability of Malicious Node
Objective: The main objective of the algorithm is to estimate the probability of malicious node in the MANET environment.
Input: N_c and N_a
Output: Calculation of the probability of malicious node.
Steps:
1 *Initialize number of detected cooperation (N_c)*
2 *Initialize numbers of detected attacks (N_a)*
3 *Create a function for estimating probability of malicious node.*
4 *Initialize probabilities that the node is a malicious node (P_m)*
5 *Apply Formula:*

$$P_m = N_a / (N_c + N_a)$$

Algorithm: Estimating Trust Factor
Objective: The main objective of the algorithm is to estimate the trust factor by considering number of detection cooperation, attacks, and improbability in the vulnerable environment of MANET
Input: N_c, N_a, I_o
Output: The program estimate the trust factor
Steps:
1 *Initialize number of detected cooperation (N_c)*
2 *Initialize number of detected attacks or declines (N_a)*
3 *Initialize improbabilities in the opinion (I_o)*
4 *Create a function for calculating the trust system*
5 *Assign ($N_c/(N_c + N_a)$) to t_{v1}*
6 Assign ($1-I_o$) to t_{v2}
7 *Estimate trust (t) in the opinion by applying formula*

$$t = t_{v1} + t_{v2}$$

Algorithm: Calculating improbability of opinion
Objective: The main objective of the algorithm is to estimate the improbability
Input: N_c, N_a, I_o
Output: The program gives the estimation of uncertainty.
Steps:
1 *Initialize number of detected cooperation (N_c)*
2 *Initialize number of detected attacks (N_a)*
3 *Create a function for estimating improbability*
4 *Estimate improbability in the opinion (I_o) by formula:*

$$I_o = 12 \times N_c \times N_a / \{(N_c + N_a)^2 \times (N_c + N_a + 1)\};$$

VI IMPLEMENTATION

The proposed system has considered a wide range of policies of intrusion in 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 1000 x 1000 m is designed with 200 mobile randomly positioned with a transmission range of 300 meters. The entire simulation area is designed with 9 logical area. A mobility model is designed and any two nodes in the same cluster are considered as neighboring nodes.

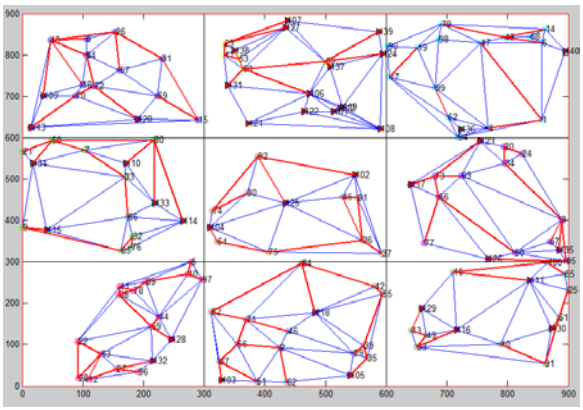

Fig 2. Nine logical region with 200 mobile nodes randomly distributed.

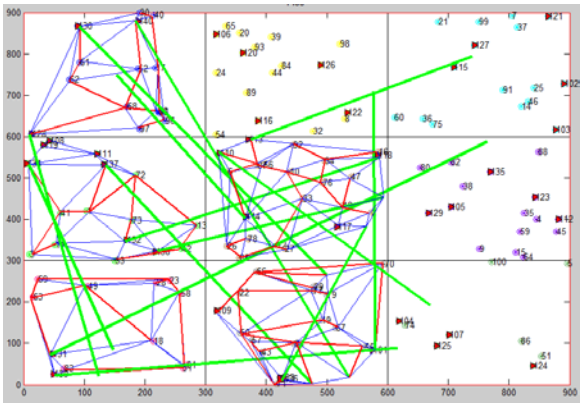

Fig 3. Nine logical region with 200 mobile nodes with an attempt of decamping.

Fig 2 represents an instance of simulation where 200 mobile nodes are randomly distributed in nine logical region. The red colored line shows the communication between two mobile nodes in the same logical region. The blue colored line represents probable communication link between two mobile nodes in the same logical region. In figure 3. The green colored line represents the process of decamping from region of attack to a new logical region.

VII. PERFORMANCE ANALYSIS

The performance analysis is done by checking the outcomes of various phases of the virtual competition to understand the abnormal behaviour of the mobile nodes. Figure 4 shows the graphical representation of the normal node movement with respect to the simulation time. A polynomial trend line is used to understand the graphical representation.

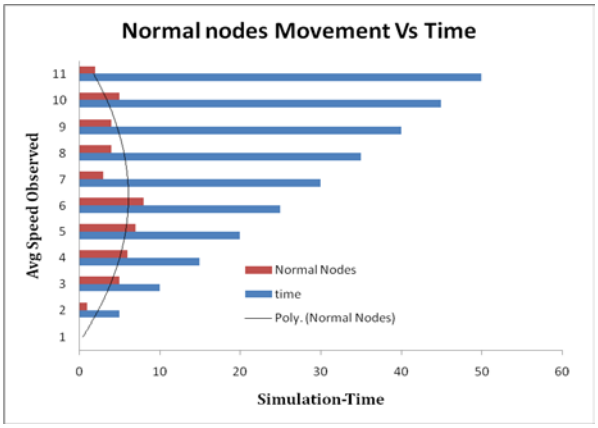

Fig 4. Analysis of Normal node movement Vs Time

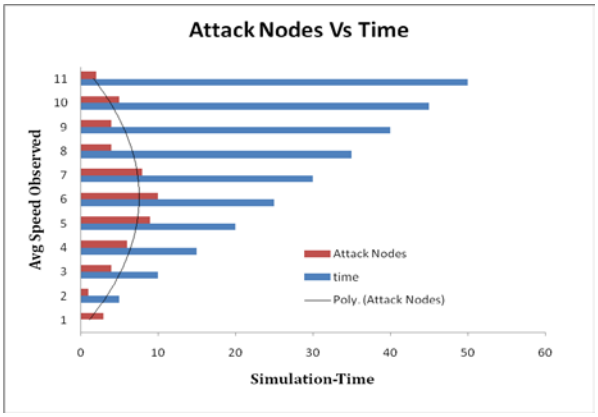

Fig 5. Analysis of Attack node movement Vs Time

In Fig-4 and Fig 5, trend line is almost similar, but a slight deviation on average speed at 5, 6, 7 seconds. Which represents that almost all the normal node and malicious node poses the same behavior with respect to mobility in mobile adhoc network topology, which will provoke the application very difficult situation to distinguish between the normal and attack nodes.

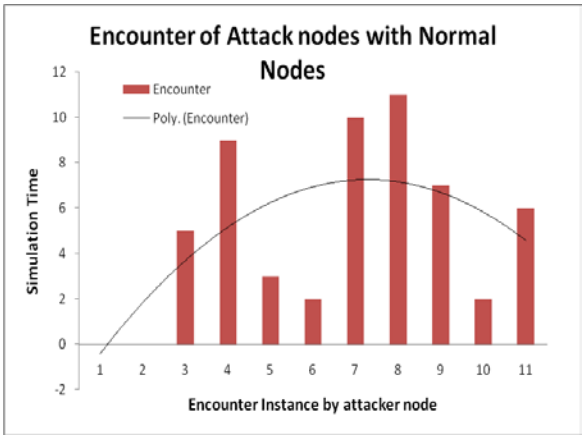

Fig 6. Analysis of Encounter of attack nodes with Normal node

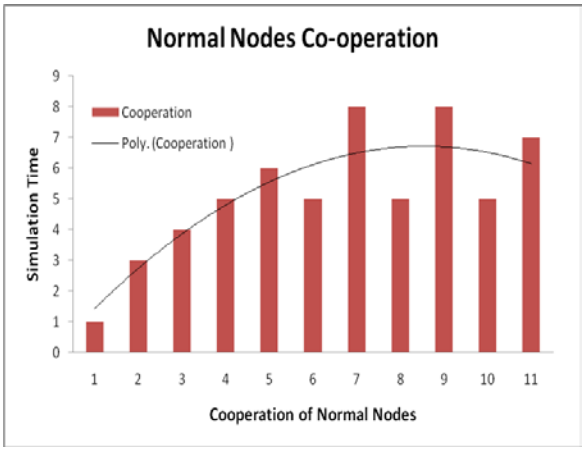

Fig 7. Analysis of Normal Nodes Co-operation

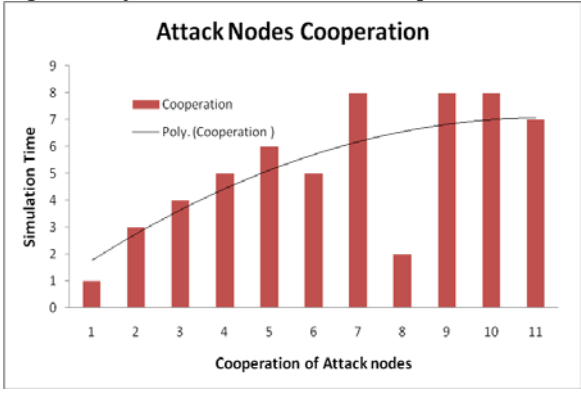

Fig 8. Analysis of Attack Nodes Cooperation

Fig-6 represents encounter of attack nodes with regular nodes. The graph represents very uneven variation proving difficult to predict the encountering strategy of attack nodes in the MANET environment. Fig-7 and Fig-8 represents cooperation instances of attack nodes and regular nodes. Comparison proves that malicious nodes try to duplicate the similar behavior of the regular node. The observation is carried out in 60 second interval. In case of continuing for another cycle of observation, it can be observed that attack nodes have higher tendency of cooperation at the end of each simulation, which indirectly proves the detrimental strategy of infection by the malicious nodes.

The simulation results also highlight the various coperation probabilities of the nodes in the MANET as shown in Figure 9.

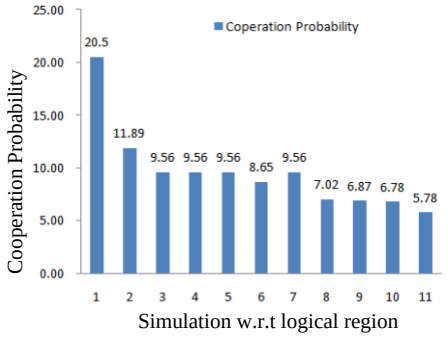

Fig 9. Graphical Representation of Cooperation Probability by nodes [regular / selfish].

This also highlights that when the simulation has been conduted in various stages with respect to every individual clusters defined, the co-opration factor decrease down which is an indication of advent of either selfish or malicious node. Once the attack has been created by any malicious node in a specific cluster, when it attempts to jump to another cluster, the proposed methodology also makes sure that any such attempt information will be instantly updated to all other clusters in the neighborhood for providing security against instrusion from such malicious nodes. With every communication the belief system and the trust opinion is gathered for estimating this information.

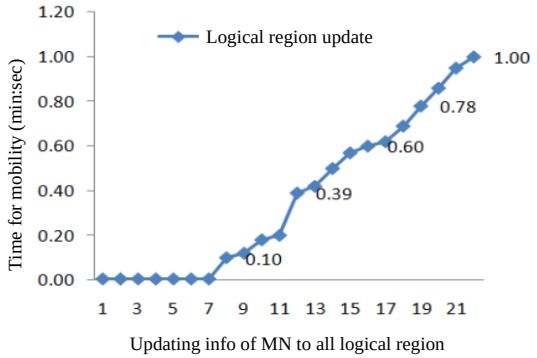

Fig 10. Cluster updates during attack by malicious nodes

Figure 10 represents that with every attempt of attack, the countermeasures provided to update the

attack information to the other cluster increase, which shows the robustness of the proposed methodology.

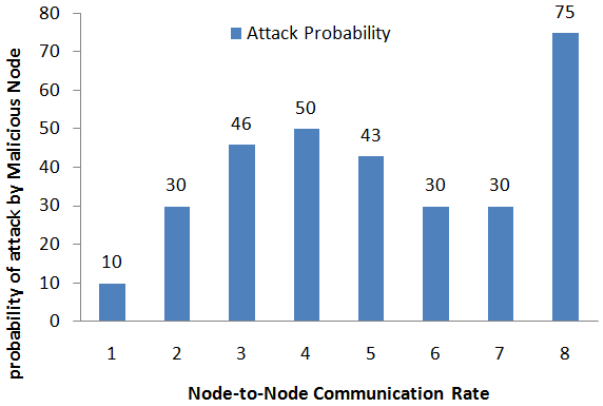

Fig 11 Attack probability by malicious node

One of the main attempts of the proposed system is to understand the misbehaviour of the nodes in the manet environment. In real-time scenario, it is almost difficult task to estimate time of the attack probability, which pose a great threat to the existing cluster as well as neighborhood clusters. So the figure 11 represents that with every node-to-node communication, there is a peak seen representing highest attack probability. This also represents that it is highly possible to understand the attack strategy if the simulation parameters are kept on changes based on multi-stages according to game theory

VII CONCLUSION

In this paper, we have discussed about a novel technique of analyzing the behaviour of the malicious node in the MANET. A framework is 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.

ACKNOWLEDGEMENT

I'm thankful to the R&D division of CBK Infotech India (P) Ltd, Bangalore to conduct my experiment for validating simulation prototype.. I'm also thankful to Dr. G. Narsimha, Assistant Professor, JNTUH College of Engineering, Jagtial, Karimnagar, Hyderabad for his valuable guidance and inputs.

REFERENCE:

[1] Sunita Sahu & Shishir K. Shandilya, "A comprehensive survey on intrusion detection in MANET", *International Journal of Information Technology and Knowledge Management*, July-December 2010, Volume 2, No. 2, pp. 305-310

[2] Azadeh Omrani and Mehran S. Fallah, "Stimulating Cooperation in MANETs Using Game Theory", Proceedings of the *World Congress* on Engineering 2007 Vol II, WCE 2007,

[3] S. Buchegger and J. Boudec, "A robust reputation system for P2P and mobile ad-hoc networks," in Proc. 2nd Workshop Econ. Peer-to-Peer Syst., 2004, pp. 403–410.

[4] F. Li and J. Wu, "Mobility reduces uncertainty in MANETs," in Proc. IEEE INFOCOM, 2007, pp. 1946–1954.

[5] A. Josang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," Decis. Support Syst., vol. 43, no. 2, pp. 618–644, Mar. 2007.

[6] F. Li, A. Srinivasan, M. Lu, and J. Wu, "Uncertainty mitigation for utility-oriented routing in MANETs," in Proc. IEEE GLOBECOM, 2007, pp. 427–431.

[7] F. Li and J. Wu, "Hit and run: A Bayesian game between malicious and regular nodes in mobile networks," in Proc. IEEE SECON, 2008, pp. 432–440.

[8] P. Liu, W. Zang, and M. Yu, "Incentive-based modeling and inference of attacker intent, objectives and strategies," ACM Trans. Inf. Syst. Secur., vol. 8, no. 1, pp. 78–118, Feb. 2005.

[9] G. Theodorakopoulos and J. Baras, "Malicious users in unstructured networks," in Proc. IEEE INFOCOM, 2007, pp. 884–891.

[10] Kejun Liu, Jing Deng, Pramod K. Varshney, and Kashyap Balakrishnan, "An Acknowledgment-Based Approach for the Detection of Routing Misbehaviour in MANETs", IEEE Transactions on mobile computing, Vol. 6, NO. 5, May 2007.

[11] Dhanalakshmi, Dr.M.Rajaram ," A Reliable and Secure Framework for Detection and Isolation of Malicious Nodes in MANET", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.10, Oct2008

[12] Zan Kai Chong, Moh Lim Sim, Hong Tat Ewe, and Su Wei Tan ," Separation of Detection Authorities (SDA) Approach for Misbehavior Detection in Wireless Ad Hoc Network",PIERS Online, VOL. 4, NO. 8, 2008.

[13] S. Buchegger and J.-Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes, Fairness in Dynamic Ad-Hoc Networks," Proc. MobiHoc, June 2002.

[14] Sanjeev Rana, Manpreet Singh, "Performance Analysis of Malicious Node Aware Routing for MANET using Two-Hop Authentication", International Journal of Computer Applications (0975 – 8887), Volume 25– No.3, July 2011
[15] Rakesh Kumar, Piush Verma, Yaduvir Singh, "Design and Development of a Secured Routing Scheme for Mobile Adhoc Network", International Journal of Computer Applications (0975 – 8887) Volume 13– No.2, January 2011
[16] Rajib Das, Bipul Syam Purkayastha, Prodipto Das, "Security Measures for Black Hole Attack in MANET: An Approach", International Journal of Engineering Science and Technology (IJEST), 2011
[17] S. Kannan, T. Maragatham, S.Karthik, V.P. Arunachalam, "A study of Attacks, Attack Detection, and Prevention Methods in Proactive and Reactive Routing Protocols", International Business Management, 2011
[18] Aishwarya Sagar, Anand Ukey, Meenu Chawla, "Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No 1, July 2010
[19] Sowmiya Hariharan, Jothi Precia, Suriyakala.C.D, Prayla Shyry, "A Novel Approach for Detection of Routes with Misbehaving Nodes in Manets", International J. of Recent Trends in Engineering and Technology, Vol. 3, No. 2, May 2010
[20] Usman Yaseen, Ali Zahir, Faraz Ahsan, and Sajjad Mohsin, "Estimating the Effects of Jammers via Conservation of Flow in Wireless AdHoc Networks", International Journal for Advances in Computer Science, Volume 1, Issue 1, 2010
[21] Sohail Abbas, Madjid Merabti, and David Llewellyn-Jones, "A Survey of Reputation Based Schemes for MANET", The 11th Annual Conference on The Convergence of Telecommunications, Networking & Broadcasting (PGNet 2010), Liverpool, UK, 21-22 June 2010