International Journal of Control Theory and Applications

ISSN : 0974–5572

Volume 9 • Number 42 • 2016

Modelling and Analysis of Solution to Misbehaviors in MANETs

G.S. Mamatha[a] V. Chayapathy[a] Ramaa A[a] and G.N. Srinivasan[a]

[a]*Associate Professor, Dept. of ISE, RVCE, Bangalore-560059, India*

E-mail: mamathags@rvce.edu.in, chayapathyv@rvce.edu.in, ramaaa@rvce.edu.in

[b]*Professor, Dept. of ISE, RVCE, Bangalore-560059, India*

E-mail: srinivasangn@rvce.edu.in

Abstract: MANETs (Mobile Ad Hoc Networks) have certain unique features which make them highly vulnerable to attacks. The network topology needs an evaluation to show how node behaviors will keep on changing with respect to time. This will in turn affect connectivity also. Design and development of analytical modeling faces numerous challenges and issues as how node exhibits misbehavior due to several failures including network layer attacks. In this paper we propose a robust model to illustrate node behaviors using a semi-Markov process. An analysis of node misbehaviors has been carried out and solution to misbehaviors has investigated as to isolate the malicious node launching network layer attacks. The analysis is also done to show how network throughput increases with the solution provided. The results obtained show effectiveness of the approach and certainly can be used to improve the network performance.

Keyword: *MANETs, node behaviors, isolation, intermediate nodes, network layer attacks, throughput.*

1. INTRODUCTION

The unique features for MANETs makes them highly susceptible to attacks, especially network layer attacks are more severe. There is a need to improve upon the research to mitigate the path misbehavior through a solution to identify the probability of genuine state. The solution to tackle these kinds of problems is very much useful in research issues to design attack resilient ad hoc protocols, analyzing performance of the network considerably. As MANETs are very dynamic and mesh topologies, the consequences of the node misbehaviors should not be ignored and it requires an in-depth research on the identification of node misbehavior. The problem starts when malicious intermediate nodes are present in the path chosen for communication. Basically the paper gives us a formal classification to node statuses based on their behavior and thereby provides the solution. semi-Markov process is used to characterize node behaviors [1]. In our node behavior model, a mobile node can change its behaviors among three states, *i.e.*, genuine, malicious and failure according to imbedded Markov chain, when the time of transition among any two states may not be exponentially distributed, but it is said to be a random variable. Using the dynamic or stochastic features of the design proposed an analysis on how to isolate a node

which is misbehaving can be done. The remaining paper is organized as follows: In section 2 the literature survey of related works has been discussed on misbehavior detection in MANETs, Section 3 focuses on the node behavior model with problem formulation is given, Section 4 concludes on how this analytical solution results can be tested for the performance analysis.

2. RELATED WORK

An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it. Several schemes were proposed to overcome network node failures in MANETs such as an on demand routing protocol for byzantine attacks in [2], which shows resilience to node misbehaviors in terms of byzantine failures and in [3] MANETs resilience to DoS attacks using SCTP is discussed. However most of these works have not revealed the adverse effect of misbehaviors nodes and improper links and in turn to check the network keeps connected or not. In [4] the impact of black hole attack and jelly fish nodes is discovered. In [5], a neat study of attacks affecting the performance using a technique called resilience-oriented security design is shown. Among security threats for MANETs the concentration is more on the network layer attacks like black hole, gray hole, message tampering and replication attacks, as packet forwarding has a profound effect on the network connectivity, performance and survivability. Besides analyzing and modeling only DoS type of attacks we have come out with a technique which is theoretically modeled as to show the node misbehaviors, thereby isolation of malicious nodes launching network layer attacks.

In [6], a method has been proposed on how to control network topology by maintaining few communication links. In [7], a 2ACK scheme was proposed to show how an add-on technique can mitigate routing misbehavior by using an analytical model. In the present paper we are trying to propose an idea which uses ACK scheme and misbehavior ratio to identify and mitigate malicious nodes. In papers [8, 9 10] a model has been proposed to classify the node misbehaviors based on a semi-Markov process. The concept used in these works is used to develop, analyze and enhanced further for modeling and isolation of misbehaving nodes in the present paper.

3. PROBLEM STSTEMENT

There exists several types of misbehaviors in MANETs as battery power wearing out, inflections in software or hardware, communicating outside the transmission range, leaving the network as they will etc;. Apart from these there exists other type of misbehaviors as malicious and failure nodes, which tries to actively participate in route discovery phase.

To identify and mitigate the vulnerabilities in the form of network layer attacks, first the optimal path should be chosen between source and destination nodes. Using the node transition behaviors, the transition probabilities are identified for each state. The node behaviors are represented in a state space S. S contains all the genuine, malicious and failure node states, represented as $S = \{g, m, f\}$. Whenever malicious nodes are identified in the chosen optimal path, the communication will be disturbed by the attacks. This situation will lead to find an alternative solution to continue communication without much delay, to isolate the malicious nodes and rerouting the traffic to the next hop of the isolated nodes.

3.1. Node Behavior Model

As MANET nodes are more susceptible to network layer attacks and thereby exhibiting the packet forwarding misbehaviors. Based on this assumption the nodes are classified as:

Genuine nodes: Nodes that actively takes part in route discovery phase and packet forwarding and are not acting malicious. These nodes can also be called cooperative nodes. A Genuine node (g) may change its state to malicious or failure node.

Malicious nodes: Nodes that actively participate in both route finding and packet forwarding process, but intentionally launch attacks to disturb the normal operation of the network. A Malicious node (m) may change its state to failure node, but not back to genuine even the behaviors are sporadic in nature.

Failure nodes: These are the nodes which are susceptible to power failures and such nodes should be identified and recharged instantly. A Failure node (f) can change its state to genuine again, if it gets recovered from power depletion and becoming active in routing operations.

The proposed model assumes that the mobile nodes are power constrained and work with respect to time. This feature makes the analyzing of nodes behavior in a probabilistic sense. The dynamic nodes in MANET can change its behavior from genuine to misbehaving node.

Using a semi-Markov process the node behaviors can be modelled to show the transitions from one state to another state. Through analysis of behavioral transitions the stochastic properties of nodes are identified, then deduce the state transition model and transition matrix for node behaviors can be formed. AS MANET nodes are found to be failed over time, the probability of behavioral changes is always dependent on time. This time dependent property suits to semi-Markov rather Markov process. The statement for semi-Markov process is stated as [8, 9]:

$$Z(t) = Xn, \forall\ tn \geq 0 \tag{1}$$

The node behavior transition probabilities are denoted using the semi-Markov model as shown in Figure. 1.

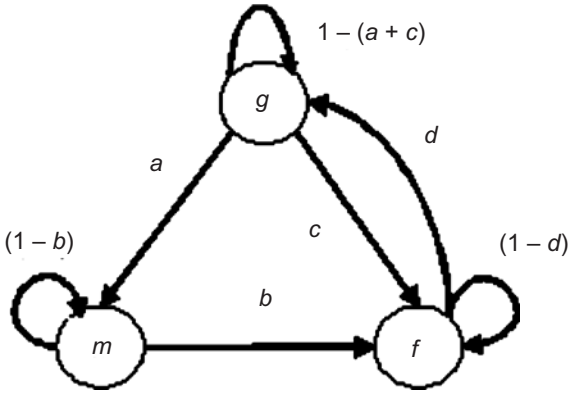

Figure 1: Semi-Markov model for node behavior transitions

In (1), Xn denotes the embedded Markov chain, as depicted in Figure 1, the state transitions can occur in finite steps and itself within one step. This makes Xn irreducible and ergodic means it is complex and not periodic in nature [11]. For Z(t), we need to find the transition probability matrix.

In (1), Xn denotes the embedded Markov chain, as depicted in Figure 1, the state transitions can occur in finite steps and itself within one step. This makes Xn irreducible and ergodic means it is complex and not periodic in nature [11]. For Z(t), we need to find the transition probability matrix.

$$\begin{aligned} T_{ij} &= \lim_{t \to \infty} Pr\,(t(n+1) = j, -tn \leq t \mid Xn = i) \\ &= Pr\,(X(n+1) = j \mid Xn = i) \end{aligned} \tag{2}$$

Let us represent P = (T_{ij}), is the transition probability matrix of Xn. The matrix P is formed as shown in Table 1. The node state transition model based on semi-Markov process is as shown in Figure 1.

Let us assume that the genuine node always tries to forward packets and indicate that state by (g), malicious nodes always tries to inject new or additional packets, drop packets or duplicate packets and indicate that state by (m). Finally the failure nodes will face loss of packets due to power exhaustion and indicate that state by (f). Consider that the probability of genuine nodes for forwarding packets as (1– (a + c)), the probability of malicious node for dropping, modifying and replicating packets as, b and the probability of failure nodes which tend to loss of packets due to power constraints as, c. As depicted in Figure 1, the failure nodes can change back to genuine state once they are recharged or recovered. Let the probability of recovery from failed state to genuine state be **d**, once the node is recharged or recovered from failures.

Table 1
Transition Probability Matrix

From \ To	*g* (State 1)	*m* (State 2)	*f* (State 3)
g (State 1)	$1 - (a + c)$	a	c
m (State 2)	0	$(1 - b)$	b
f (State 3)	d	0	$(1 - d)$

3.2 Solution to Misbehaviors

The effect of misbehaviors in MANETs is explained in the above section with the graph showing linear increase in malicious probability. Previously various solutions were proposed to overcome such impacts [1, 8, 9 and 10].

One such solution is illustrated in the current paper is that of isolating a malicious intermediate node or nodes launching network layer attacks from its neighboring intermediate nodes. The proposed solution in this paper is different from other related works in isolating the malicious intermediate node from the path chosen for communication. The previous works dealt with isolating the genuine or cooperative node itself from its malicious neighbors. The following Figure 2 explains an example scenario where all the neighbors of a node X are genuine and sends the packets to destination node Y. To make the situation worst, if there exists only one optimal path obtained for communication between X and Y, then if any of the intermediate node say X_1 as in Figure 2, becomes malicious either by launching gray hole or message tampering attack or attains a failure state due to its energy constraints, immediately there will be a chance that all the packets forwarded to it are either dropped or lost or failed or tampered.

To tackle this kind of situations, that node can be isolated from the path and the packets can be forwarded to the very next hop node in the same path to continue the communication. Moreover if other intermediate nodes in the path are also malicious, definitely it will reduce the throughput performance of the network. This kind of solution exactly reduces the number of hops travelled from 5 to 4 hops.

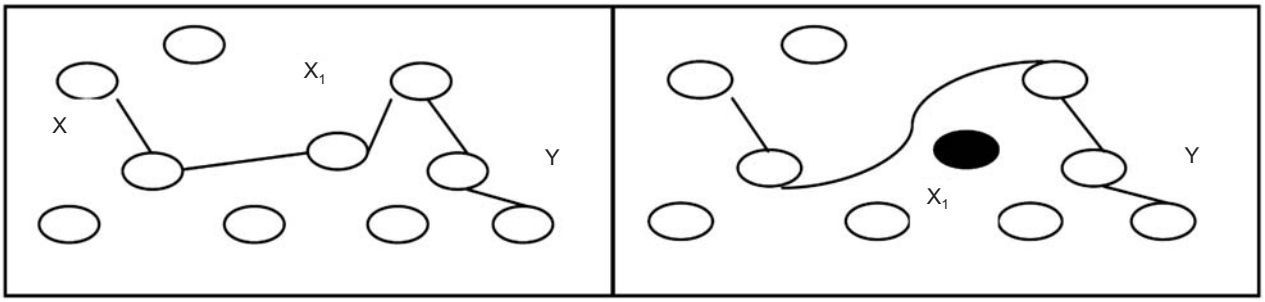

Figure 2: Intermediate node isolation scenario

From this analysis, it is got to know that the attacks have a severe impact on MANETs. The probability that a node is isolated due to misbehavior like this can be analyzed and shown as follows:

Proposition : The intermediate nodes occurring between the selected source and destination nodes are isolated, if and only if it is a gray hole or message tampering intermediate node. This derives that the probability of a node being in genuine state is obtained with regard to the total number of intermediate nodes present in between source and destination pairs and the number of malicious intermediate nodes the selected path has got for isolation.

Proof: Let S = {*g*, *m*, *f*} be a set of 3 states of transition. Let us assume the following notations for derivation to assess the probability of genuine nodes with intermediate nodes present in the selected path between source and destination nodes. As mentioned earlier only malicious intermediate nodes are considered for derivation and failed nodes are not taken in to account.

Let L (XY) denotes the optimal path selected for communication. Where X will be the source node and Y will be the destination node. All the other nodes in between them are called intermediate nodes, represented as I.

Let I (XY) denotes the total of intermediate nodes between X and Y. The total of malicious intermediate nodes will be denoted by node degree **i**, which varies from 1 to n and are neighbors to genuine nodes in the same path.

Here we are applying the following conditions for developing a analytical solution of such malicious behaviors in the form of attacks.

1. First we assume an ideal network with probability of occurrence of misbehavior as nil. Always we assume that the malicious activity is launched by intermediate nodes existing between selected source and destination pair. Where M_N is the total number of nodes in the network.

2. Next we assume a constant probability of a node being malicious, either by launching gray hole (GH) or message tampering attack (MT) is minimum as 0.01.

$$Pr(n(GH)) = Pr(n(MT)) = 0.01$$

3. Where, n(GH) be the gray hole intermediate node out of I between X and Y and n(MT) be the message tampering intermediate node between X and Y. Therefore total number of malicious nodes probability in the selected optimal path will be denoted by Pr(m) and is given by,

$$Pr(m) = (Pr(n(GH)) + Pr(n(MT))) \quad (3)$$

4. We can increase the probability of occurrence of malicious nodes in the form of network layer attacks and check how the link performs and isolated such nodes. The maximum number of intermediate nodes considered is 50. The probability is calculated for 50 nodes as follows:

$$Pr(I) = \left(\frac{1}{n}\right) \quad (4)$$

Using the formulae in the above Equation (4), the probability of occurrence of 50 intermediate nodes becomes 0.02, with n = 50.

5. The solution illustrated to this problem is to isolate a malicious node and reroute the traffic in the same link.

$$\text{If } Pr(m) = 0.02,$$
$$\text{then } M_N = ((S, I, D) - (Pr(N_m(GH)) + Pr(N_m(MT))) \quad (5)$$

Where, (S, I, D) denotes the chosen source, destination and other intermediate nodes in the chosen link for communication. As only intermediate nodes are taken for modelling and analysis purpose, we can consider only the probability of occurrence of intermediate nodes as in equation in (4).

$$\text{Since I (XY)} = i, \text{ the malicious node is isolated from the network if,}$$
$$n(GH)\ (I) \geq 1$$
$$\text{or } n(MT)(I) \geq 1\ .$$

To denote the probability of total number of intermediate node occurrence between source an destination as Pr(I) for given I (XY) = i and is given by,

$$Pr(I \mid I(XY) = i) = Pr(n(G) = |I(XY) = i) \quad (6)$$

Where,

Pr(n(G)) represents probability of all the intermediate nodes as genuine and number of malicious intermediate nodes,

$$i = 0.$$

From the semi-Markov node behavior transition model as presented in Figure 1, the Genuine state probability is given by Pr(P_{gg}). From the model and transition probability matrix (Table 1), it can be deduced that the probability of a node to be in the genuine state itself is given as,

$$Pr(P_{gg}) = 1 - (a + c) \quad (7)$$

Where, c can be considered zero, as we are concentrating on only malicious behaviors, so equation (7) becomes,

$$Pr(P_{gg}) = 1 - a \quad (8)$$

As a represents misbehavior which is considered as only two network layer attacks in the current work for simplicity purpose, it can be analyzed as misbehaviors are isolated from genuine probability equal to 1. This 1 can be assumed as the maximum probability of total number of intermediate nodes present between source and destination *i.e.*,

$$Pr(I) = 1.0,$$

means only one intermediate node is present between source and destination pair.

According to the analysis for isolation probabilities carried in the previous work[1, 8 and 9], it can be referred that the isolation of a misbehavior can be presented as follows with respect to the proposed problem stated in the proposition. From equation (3) Pr(a) is written as,

$$\begin{aligned} Pr(a) &= Pr(m) \\ &= [Pr(n(GH)) + Pr(n(MT))], \end{aligned}$$

which can be rewritten with reference to the equations (6) and (4) in papers [1, 9] as,

$$\begin{aligned} Pr(a) &= n(GH) + n(MT) \\ &= [(1 - (1 - Pr(n(GH)))) + (1 - (1 - Pr(n(MT))))] \end{aligned} \quad (9)$$

As the malicious intermediate node degree can vary accordingly due to MANETs changing topology, there may be a possibility that more and more adversaries may enter the range. So only the equation (9) becomes,

$$Pr(a) = [(1 - (1 - Pr(n(GH)))) + (1 - (1 - Pr(n(MT))))]^i \quad (10)$$

The effects of Pr(I) and i on the probability of node being in a genuine state are illustrated as given in equation (12). It can be analyzed that the probability of node being in a genuine state is directly proportional to Pr(I). As the given number of intermediate nodes are increased, Pr(P_{gg}) also linearly increases with isolating misbehaviors from other intermediate nodes with fixed node degree and misbehavior probability. This analysis is shown as graph in the Figure 3.

There are possibilities in a network like MANETs the node degree for malicious intermediate nodes can increase. In such cases also, the Pr(P_{gg}) linearly keeps on increasing as node degree increases with maximum of 50 intermediate nodes between source and destination pairs, *i.e.*, Pr(I) = 0.02. This analytical result is shown as graph in Figure 4.

This clearly states that the proposed solution for misbehavior is capable of isolating more number of malicious intermediate nodes, thereby keeping the Pr(P_{gg}) to higher value. There are possibilities that the Pr(P_{gg}) can be saturated and stabilized to some probability value, even if more malicious intermediate nodes are isolated from the selected path. This exactly follows the inverse weibull distribution which is a very flexible reliability model and approaches different distributions [12] as shown in Figure 5.

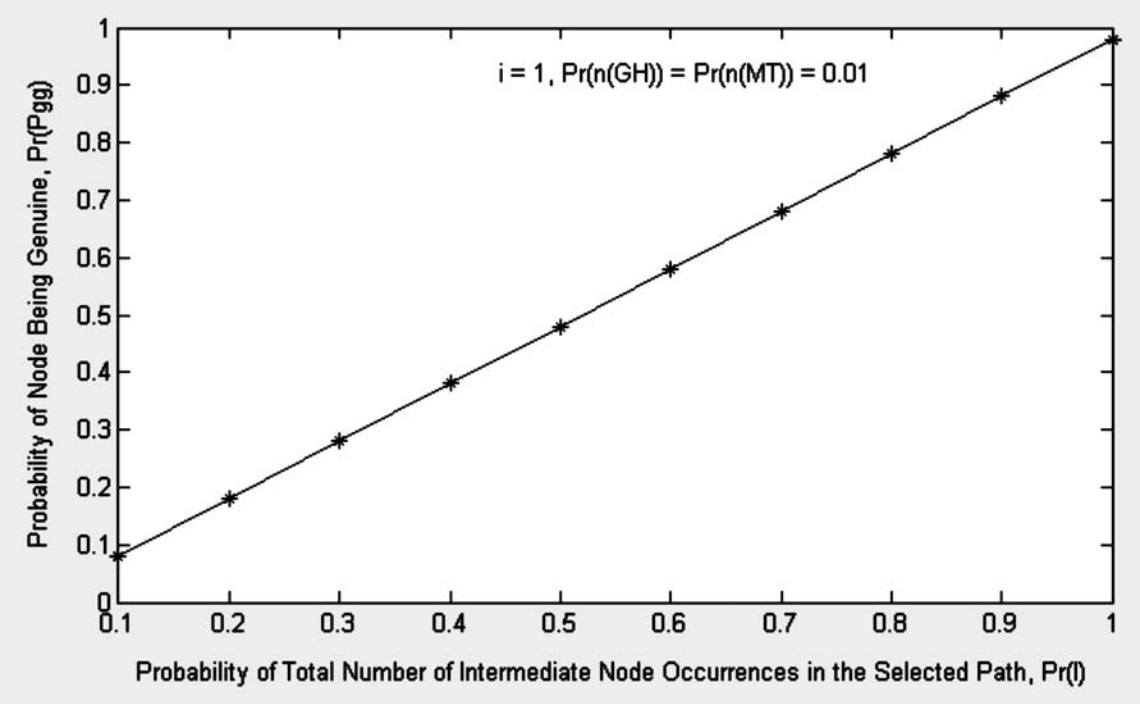

Figure 3: Graph of Pr(I) vs Pr(P_{gg})

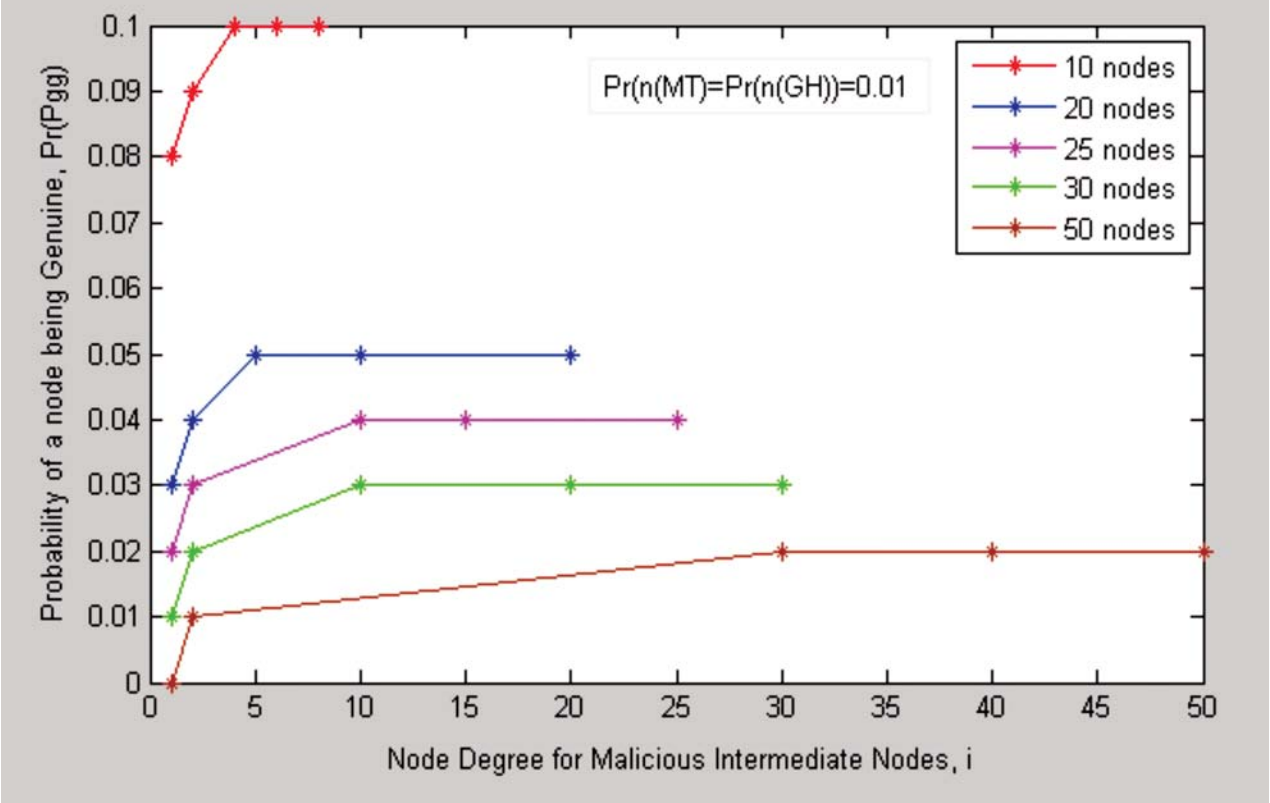

Figure 4: Graph of *i* vs Pr(P_{gg})

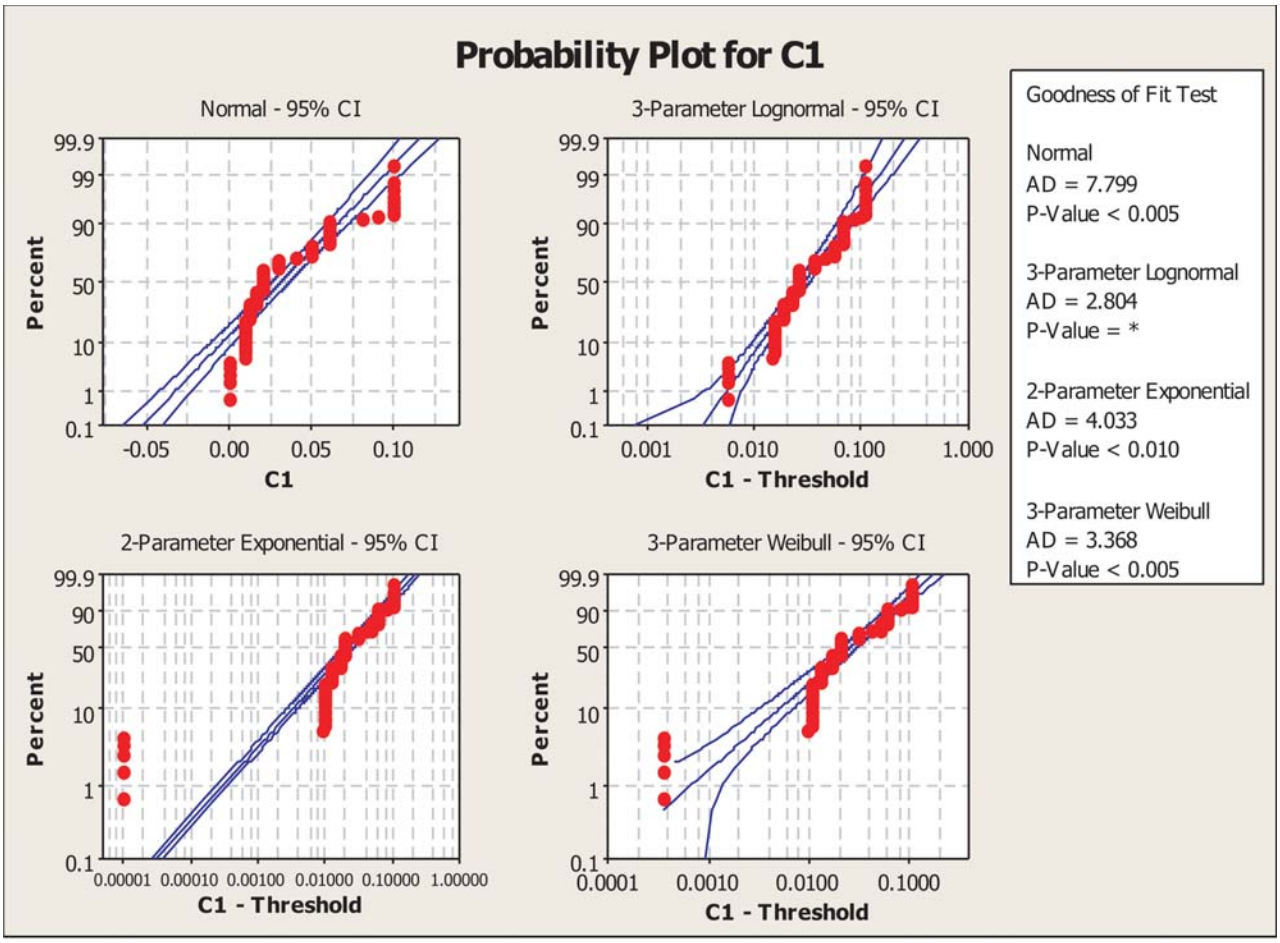

Figure 5: Approaches to different distributions

The distribution is exactly inverse in nature, which becomes an analogy for the link failure property in MANETs. This fact illustrates that, whenever there will be a link failure in the network, the link comes down with a negative value. This feature makes the distribution as inverse. Therefore in MANETs, especially the military and other defense networks, mitigating malicious nodes launching network layer attacks becomes a serious concern as it is going to majorly affect the routing and packet forwarding process. To keep the packet forwarding process also in a stabilized manner, the proposed solution proves to be the best and thereby promises to increase the throughput parameter of the network.

4. CONCLUSION

The work described in this paper contributes for the development of a new compressed semi-Markov model for three node behavior states. From this node behavior model it is finally deduced that the increase in misbehavior probability will definitely reduce the packet forwarding probability or in other terms the node being in the genuine state. The solution provided to mitigate such problem is to isolate a malicious node exhibiting misbehavior in the form of network layer attacks. It is found that the probability of node being genuine linearly increases with the increase in number of intermediate nodes between source and destination pair. As the probability of a node being genuine increases, the misbehaviors decreases which will in turn enhances the routing capabilities in forwarding packets without dropping or losses. This thereby upgrades the performance of the network by increasing the throughput, as probability of packet forwarding capacity will increase. Further the model can be extended and made concrete in nature proving the best of solution to mitigate misbehaviors in MANETs.

5. ACKNOWLEDGMENT

My sincere thanks to our now Principal Dr. K N Subramanya and Dr. N. S Narahari , HoD, IEM Dept., RVCE for their support and advise rendered for this work.

REFERENCES

[1] Fei Xing and Wenye Wang, Modeling and Analysis of Connectivity in Mobile Ad Hoc Networks with Misbehaving Nodes, In proceedings of IEEE ICC 2006, pp.1879-1884

[2] Baruch Awerbuch et al., An On-Demand Secure Routing Protocol Resilient to Byzantine Failures, In proceedings of the ACM Workshop on wireless Security, ACM Press, 2002, pp. 21-30.

[3] Inwhee Joe, SCTP with an Improved Cookie Mechanism for Mobile Ad Hoc Networks, In proceedings of IEEE GLOBECOM, Vol. 7, Dec 2003, pp. 3678-3682.

[4] Imad Aad, JP. Hubaux and E W Knightly, Denial of Service Resilience in Ad Hoc Networks, In proceedings of ACM Moicom, 2004, pp. 202-215.

[5] Hao Yang et al., Security in Mobile Ad Hoc Networks:Challenges and Solutions, IEEE Wireless Commnications, Feb 2004, pp. 38-47.

[6] Xiang-Yang Li et al., Tolerant Deployment and Topology Control in Wireless Networks, In proceedings of ACM MOBIHOC, Jan 2003, pp. 117-128.

[7] Kejun Liu, Jing Deng, P.K. Varshney and K. Balakrishnan, "An Acknowledgement-Based Approach for the Detection of Routing Misbehavior in MANETs, IEEE Transactions on Mobile Computing, Vol. 6, No. 5, MAY 2007, pp. 536-550.

[8] A.H. Azni and R. Ahmad et al., Correlated Node Behavior Model based on Semi Markov Process for MANETS, International Journal of Computer Science Issues, Vol. 9, Issue 1, No. 1, JAN 2012, pp. 50-59.

[9] A.H. Dehghan, Mobile Ad Hoc Networks Flexibility in Dynamic Denial of Service Attacks, International Journal of Advanced Research in Computer Science and Software Engineering, Vol.2, Issue 2, FEB 2012.

[10] Andr'e K''onig, Daniel Seither, R. Steinmetz and M. Hollick, An Analytical Model of Routing, Misbehavior, and Countermeasures in Mobile Ad Hoc Networks, In proceedings of IEEE Global communications conference (GLOBECOMM-2009), DEC 2009.

[11] Ravindran, Phillips and Solberg, Operations Research, Principles and Practice, Second Edition, Wiley-India Edition, 2007.

[12] Shuaib Khan, G.R Pasha, Ahmed Hesham Pasha, Theoretical Analysis of Inverse Weibull Distribution, WSEAS Transactions on Communications, Issue 2, Volume 7, February 2008, pp. 30-38.

[13] Shakhakarmi Niraj, Dhadesugoor R. Vaman, distributed position localization and tracking (dplt) of malicious nodes in cluster based mobile ad hoc networks (manet), Issue 11, Volume 9, November 2010, 708-719.

[14] Arun Kumar Singh, Neelam Srivastava, J. B. Singh, A Novel Strategy for High Throughput in Ad Hoc Networks using Potential transmission Count (PTC) Metric, Issue 8, Volume 10, August 2011, 223-232.