IJCSN International Journal of Computer Science and Network, Volume 5, Issue 4, August 2016
ISSN (Online) : 2277-5420 www.IJCSN.org
Impact Factor: 1.02

Probabilistic Modeling and Estimation of Network Blocking Probability for Selfish Behavior Attack in Mobile Ad hoc Networks

[1]Kirti A. Adoni, [2]Anil S. Tavildar

[1] VIIT Research Scholar, VIIT Kondhwa
Pune, Maharashtra, India
akirti2008@gmail.com

[2] Emeritus Professor, MKSSS'sCummins college of Engineering
Pune, Maharashtra, India
astivaldar@gmail.com

Abstract - Data delivery in Mobile Adhoc Networks (MANETs) gets adversely affected by various malicious attacks. Detection of malicious presence, therefore, becomes important to improve MANET's performance. In this paper probabilistic models have been proposed to characterize random behavior of nodes for Selfish Behavior (SB) attacks. This attack makes nodes unavailable for data forwarding, resulting in increased blocking tendency of the network. Quantification of network blocking probabilities has been proposed. This can then be further used for making appropriate trustworthiness related decisions for nodes, leading to improvement in MANET's performance, using suitable routing protocols.

Keywords **-** probabilistic models, Selfish behavior attack, probability of blocking, MANETs

1. Introduction

Mobile Ad-hoc Networks (MANETs) comprise of mobile nodes. These nodes communicate with each other using wireless links without establishment of centralized network infrastructure. A MANET is a cooperative network, in which each node has responsibilities of forwarding and routing the packets. The nodes appear and disappear with respect to each other in the dynamic network topology. The dynamic nature of ad hoc networks is prone to many security challenges like non delivery of data, wrong delivery of data etc. The major challenge is in the area of protecting the networks against malicious attacks. The reliable dissemination of data between the nodes in MANETs greatly depends upon the degree of collaboration established among them. The reputation of the nodes present in the network is considered as a crucial aspect, for maintaining co-operation among mobile nodes. Some nodes in the network are not cooperative in nature, are termed as malicious nodes. Many nodes may exhibit a selfish behavior, not willing to forward packets for others and save its own resources. The selfish behavior of nodes is random in nature with respect to time and in number as well. Detecting these malicious nodes is essential to improve network performance. A common solution to handle this problem is to detect such malicious nodes in the network and avoid them. Most of the ad hoc routing protocols like DSDV, OLSR, AODV, DSR, DYMO etc. [1-6] are not designed originally to be secured against malicious attacks [7]; as they simply trust the neighbors implicitly. Modeling of malicious presence would help in determining the strategy for malicious node detection. Probabilistic modeling for Selfish Behavior (SB) attack has been considered in this paper and probability of blocking due to malicious presence has been estimated. This can be used to decide strategy of Malicious Node Detection towards improving network performance.

The paper is organized as follows; section 2 briefly reviews statistical modeling strategies used in literature. The proposed probabilistic models and estimation of blocking probability have been discussed in section 3. Estimation of total network blocking probability due to various malicious nodes has been discussed in section 4. Simulation Results are included in section 5, followed by conclusion and directions for future work.

2. Related Work

Many researchers [8 to 19] have proposed strategies for detection of malicious nodes using prior history of data forwarding or using collaborative Watchdog mechanisms. Some of the researchers [8, 9, 10, 13, 20 and 26] have proposed security enhancing algorithms/architectures for improving the data delivery by avoiding paths containing malicious nodes. However, only a few researchers [21, 22, 23, 24, and 25] have proposed mathematical or statistical models for characterizing malicious presence, which are briefly summarized in the following paragraph.

Amir Khusru Akhtar, G. Sahoo [21] have proposed mathematical heuristic model for detection of malicious nodes under different attacks. They have used Gaussian statistics for conditional probability of observed node either being malicious or non-malicious. J. Sengathir et al. [22] have proposed mathematical model for detection of nodes which behave selfishly under different conditions such as route discovery, route reply and data delivery, using conditional Laplace Transform. Various performance parameters of MANETs have been evaluated using

typical simulation scenario. Syed S. Rizvi et al.[23] have proposed mathematical model using Binomial statistics for different behavior of nodes, for transmission of its own packets and forwarding of packets received from neighboring nodes. Hernandez-Orallo et al.[24] have proposed mathematical model which computes time and cost for identifying selfish nodes with the help of watchdogs. Communication between two nodes has been modeled to be Poisson distributed. The continuous parameter Markov chain is used to model the network. S. Buchegger et al. [25] have proposed mathematical model for determining the reputation of every node based on Bayesian philosophy and the reputation has been calculated using Beta distribution.

Considerable research efforts have thus been directed towards algorithms / architectures using different mathematical or statistical models for detecting or dealing with malicious presence, with a view to improve the performance of the network. However, the basic random nature of various attacks for modeling the randomness does not seem to have received much of attention in the literature. In this paper, the probabilistic models for SB attack have been proposed. Further these models have been used to estimate the network blocking probabilities due to the malicious presence.

3. Proposed Probabilistic Model

3.1 Description of SB Attack

Rajaram and Palaniswami[27] have discussed various malicious attacks in Mobile Ad hoc Networks. In this paper, the Selfish Behavior (SB) attack has been modeled probabilistically. In case of SB attack, to prevent the detection as a malicious node, the nodes frequently change their behavior ON to OFF or OFF to ON. The malicious node switches ON/OFF randomly with a view to preserve its resources like battery power, memory etc. The nodes change states abruptly, they remain 'ON' only for sending their own data and become 'OFF', when data of other nodes is to be forwarded. Such type of behavior is commonly referred to as selfish behavior.

Suppose j^{th} node in the network is suspicious and considered to be selfish, then its ON-OFF behavior can be as shown in fig.(1)

Service is blocked during the small time interval τ such that

For k=1 $\tau_1 = t_2 - t_1$

For k=2 $\tau_{1+} \tau_2$ where $\tau_2 = t_4 - t_3$

And general equation will be for 'k' ON/OFF pulses, $\tau = \tau_1 + \tau_2 + \ldots\ldots\ldots + \tau_k$ where $\tau_k = t_{(2.k)} - t_{((2.k)-1)}$

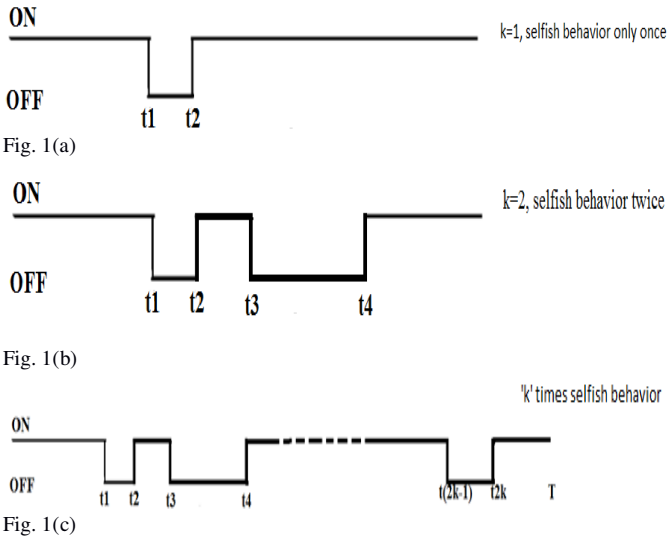

Fig. 1(a)

Fig. 1(b)

Fig. 1(c)

Fig.1 Illustration of typical Selfish Behavior attack

3.2 Proposed system Architecture for modeling

As shown in fig. (2) below the random behavior of malicious SB attack can be visualized in three separate levels, L_1, L_2 and L_3, due to three distinct parameters namely absolute time of ON/OFF switching of malicious nodes, the number of consecutive pulses of ON/OFF switching for malicious nodes and randomness in number of maliciously behaving nodes in the MANET, respectively.

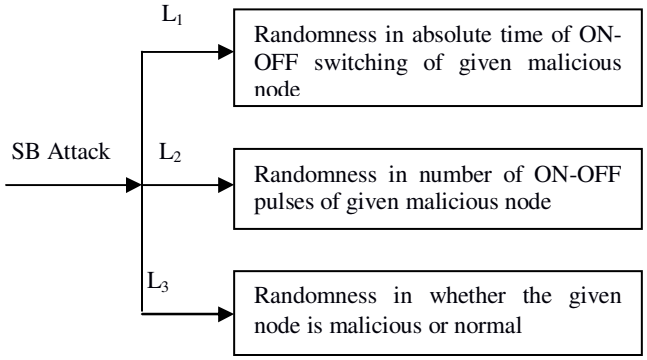

Fig.2 Three levels of SB attack

It can be readily seen that,

a. All $t_1, t_2 \ldots\ldots\ldots\ldots t_{(2.k)}$ corresponding to 'L_1' above can be considered as continuous random variables, between 0 to T
b. Number of ON/OFF pulses 'k' for given malicious node corresponding to 'L_2' above can be viewed is discrete random variable
c. Number of malicious nodes 'n' in the MANET corresponding to 'L_3' above can be treated as discrete random variable

3.3 Proposed Probability Models

In the ensuing analysis, the different probability models assumed have been as given below

1. The number of times, given malicious node switches ON/OFF i.e. random variable 'k' has been assumed to be a) Uniform and b) Poisson distributed.
2. Number of nodes 'n' which can be malicious in the network has been assumed to be binomially distributed.
3. The absolute time for ON/OFF switching t_1, $t2$…….$t_{(2.k)}$ have been assumed to be uniformly distributed over the available observation time.

It is further assumed that all random variables i.e. 'k', 'n' and various time occurrences are statistically independent variables. The joint probability density functions (pdfs) for timing distributions $f(t_1,t_2$…….$t_{(2.k)})$ have now been derived in the following.

3.4 Determination of Joint pdf for various ON-OFF occurrences

Case I: for k=1, [Refer fig. 1(a)]

Here t_1 is assumed to be uniformly distributed between (0, T) as per equation below

$$f(t_1) = \frac{1}{T} \qquad 0 < t_1 < T \tag{1}$$

The Joint pdfs of t_1 and t_2 together, using Bay's conditional probability rule, can be expressed as

$$f(t_1,t_2) = f(t_2/t_1).f(t_1) \tag{2}$$

Considering distribution 't_2' also uniform between (t_1,T)

$$f(t_2/t_1) = \frac{1}{(T-t_1)}$$

Combining the above two equations

$$f(t_1,t_2) = \frac{1}{T.(T-t_1)} \tag{3}$$

Case II for k=2, [Refer fig.1 (b)]

This means the particular malicious node behaves selfishly, two times during the measurement time 0 to T. Thus, in this case, there are four random time occurrences t_1, t_2, t_3 and t_4.

The Joint pdf, can be written as

$$f(t_1,t_2,t_3,t_4) = f(t_4/t_1,t_2,t_3).f(t_1,t_2,t_3)$$
$$f(t_1,t_2,t_3) = f(t_3/t_1,t_2).f(t_1,t_2)$$

Considering distribution 't_3' also uniform between (t_2, T)

$$f(t_3/t_1,t_2) = \frac{1}{(T-t_2)}$$

Combining with equation (3) above, $f(t_1, t_2, t_3)$ becomes

$$f(t_1,t_2,t_3) = \frac{1}{(T-t_2)}.\frac{1}{T.(T-t_1)} \tag{4}$$

Assuming 't_4' to be uniformly distributed between (t_3,T), $f(t_4/t_1,t_2,t_3)$ can be expressed as,

$$f(t_4/t_1,t_2,t_3) = \frac{1}{(T-t_3)} \tag{5}$$

Combining equations (4), (5), the joint pdf $f(t_1, t_2, t_3,t_4)$ can now be written as

$$f(t_1,t_2,t_3,t_4) = \frac{1}{T.(T-t_1).(T-t_2).(T-t_3)} \tag{6}$$

Case III: General value of 'k', [Refer fig. 1(c)]

For general case, when 'k' ON-OFF occurrences are observed, extending the above argument, the joint pdf of all random instances can be visualized as

$$f(t_1,t_2 \dots\dots, t_{(2.k)}) = \frac{1}{T.(T-t_1).(T-t_2)\dots\dots\left(T-t_{((2.k)-1)}\right)}$$

$$f(t_1,t_2 \dots\dots, t_{(2.k)}) = \frac{1}{T}\prod_{j=1}^{((2.k)-1)}\frac{1}{(T-t_j)} \tag{7}$$

Where symbol $\prod represents multiplication.$

3.5 Estimation of Blocking Probability

In the first step the probability of blocking due to individual node, P_{bj} has been estimated. When any given node 'j' behaves selfishly, 'k' times during the total observation time, 'T', the data forwarding due to malicious behavior gets prohibited for the duration τ, given by

$$\tau = (\tau_1 + \tau_2 + \tau_3 + \cdots \tau_k) = \sum_{i=1}^{k} \tau_i$$

where 'k' is also a discrete random variable. The probability of blocking due to the j^{th} node, making use of the concept of statistical averaging [28] can be expressed as

$$P_{bj} = \frac{E[\sum_{i=1}^{k} \tau_i, k]}{T}$$

$$P_{bj} = \frac{1}{T}.E\left(\sum_{i=1}^{k}\tau_i \Big/ k\right).P(k) \tag{8}$$

where P(k) represents probability of occurrences of 'k' pulses.
First it has been assumed that random variable 'k' is uniformly distributed, in the following.

3.5.1 Assuming 'k' to be uniformly distributed

In this case, maximum possible degradation in worst case scenario, has been considered as maximum of ten times ON/OFF pulses of malicious node during the measurement period (0-T) i.e. k_{max}=10

Therefore, for uniform distribution

$$P_k = 0.1 \qquad k = 1,2,\ldots\ldots\ldots 10$$
$$= 0 \qquad otherwise$$

Therefore, for k=1, the equation (8) will lead to

$$P_{bj} = \frac{E[\tau_1/k=1].P_{(k=1)}}{T}$$

$$P_{bj} = \frac{1}{T}.\int_o^T \int_{t_1}^T (t_2 - t_1) f(t_1,t_2) dt_2 dt_1 P_{(k=1)}$$

$$P_{bj} = \frac{1}{T}.\int_o^T \int_{t_1}^T (t_2 - t_1) \frac{1}{T.(T-t_1)} dt_2 dt_1 . P_{(k=1)} \qquad (9)$$

For k=2

$$P_{bj} = \frac{E[(\tau_1 + \tau_2)/k=2].P_{(k=2)}}{T}$$

$$P_{bj} = \frac{1}{T}\int_0^T \int_{t_1}^T \int_{t_2}^T \int_{t_3}^T (t_2 - t_1 + t_4 - t_3).f(t_1,t_2,t_3,t_4) dt_4 dt_3 dt_2 dt_1 . P_{(k=2)}$$

Using equation (6), the above gives us

$$P_{bj} = \frac{1}{T}\int_0^T \int_{t_1}^T \int_{t_2}^T \int_{t_3}^T (t_2 - t_1 + t_4 - t_3).\frac{dt_4 dt_3 dt_2 dt_1}{T.(T-t_1).(T-t_2).(T-t_3)}.P_{(k=2)} \qquad (10)$$

For general value of 'k', the probability of blocking due to j[th] node can now be written as

$$P_{bj} = \frac{E\left[\sum_{i=1}^k \tau_i/k=k\right].P_{(k=k)}}{T}$$

$$P_{bj} = \frac{1}{T}\int_0^T \int_{t_1}^T \ldots \int_{t_{((2.k)-1)}}^T \left(t_2 - t_1 + t_4 - t_3 + \cdots + t_{(2.k)} - t_{((2.k)-1)}\right).f\left(t_1,t_2,\ldots t_{(2.k)}\right).dt_{(2.k)} \ldots dt_1 . P_{(k=k)}$$

Using equation (7), the above leads to

$$P_{bj} = \frac{1}{T}\int_0^T \int_{t_1}^T \ldots \int_{t_{((2.k)-1)}}^T \left(t_2 - t_1 + \cdots + t_{(2.k)} - t_{((2.k)-1)}\right).\frac{1}{T}.\prod_{i=1}^{((2.k)-1)} \frac{1}{(T-t_i)} dt_{(2.k)} \ldots dt_1 . P_{(k=k)} \qquad (11)$$

In the following paragraph, random variable 'k' has been assumed to be Poisson distributed with similar analysis.

3.5.2 Assuming discrete random variable 'k' to be Poisson distributed

The OFF/ON switching of malicious node selfishly is due to random arrival of time instances $t_1, t_2 \ldots\ldots\ldots\ldots t_{2.k}$ at which the malicious node changes its state. Therefore such random arrivals $t_1, t_2 \ldots\ldots\ldots\ldots t_{2.k}$, could also be modeled as Poisson distributed, i.e. for every occurrence of a pulse, it counts two arrivals. For k=1, for one pulse of ON to OFF and OFF to ON switching two random time arrivals at t_1 and t_2 respectively. For k=2, two pulses, four random arrivals at t_1, t_2, t_3 and t_4. The probability of 'm' arrivals has been as Poisson distributed [29] given by

$$P_m = \frac{(\lambda.T)^m}{m!} e^{(-\lambda.T)} \qquad (12)$$

Where, m=(2.k) and k=1,2,……10, 'λ' represents parameter of the distribution indicating the average level of malicious activity assumed in the network and 'T' represents total measurement time. For the present analysis, low level activity corresponding to k=1, only one ON-OFF pulse on an average, i.e. m=2 and medium level activity representing k=2, two ON-OFF pulses on an average, i.e. m=4, for malicious node have been considered. Estimation of blocking Probability due to individual node j can now be evaluated as follows,

3.5.2 A. Low level of malicious activity

In this case parameter 'λ' has been assumed as (λ.T) =2, i.e. average value of two time occurrences and P_m is determined using equation (12)

For k=1

$$P_{bj} = \frac{1}{T}\int_0^T \int_{t_1}^T (t_2 - t_1).f(t_1,t_2) dt_2 dt_1 . P_{m=2}$$

$$P_{bj} = \frac{1}{T}\int_0^T \int_{t_1}^T (t_2 - t_1).\frac{1}{T.(T-t_1)} dt_2 dt_1 . P_{m=2} \qquad (13)$$

For k=2

$$P_{bj} = \frac{1}{T}\int_0^T \int_{t_1}^T \int_{t_2}^T \int_{t_3}^T (t_2 - t_1 + t_4 - t_3).f(t_1,t_2,t_3,t_4) dt_4 dt_3 dt_2 dt_1 . P_{m=4}$$

$$P_{bj} = \frac{1}{T}.\int_0^T \int_{t_1}^T \int_{t_2}^T \int_{t_3}^T (t_2 - t_1 + t_4 - t_3).\frac{dt_4 dt_3 dt_2 dt_1}{T.(T-t_1).(T-t_2).(T-t_3)}.P_{m=4} \qquad (14)$$

General equation for blocking probability with 'k' times ON-OFF switching, with average lower level of maliciousness can therefore be written as

$$P_{bj} = \frac{1}{T}\int_0^T \int_{t_1}^T \ldots \int_{t_{((2.k)-1)}}^T \left(t_2 - t_1 + .. + t_{(2.k)} - t_{((2.k)-1)}\right).\frac{1}{T}.\frac{1}{\prod_{i=1}^{((2.k)-1)}(T-t_i)}.dt_{(2.k)} .. dt_1 . P_{m=(2.k)} \qquad (15)$$

3.5.2 B. Medium level of malicious activity

Exactly similar analysis as above can be done, using on an average of two pulses of switching or four random time arrivals. Correspondingly ($\lambda.T$) =4 can be put in equation (12) and $P_{m=(2.k)}$ as per equation (12) to be used for evaluating probability of blocking as per equation (13), (14) and (15), for different values of 'k'.

4. Estimation of Total Network Probability

In this MANET network with total of 'N' nodes, of which 'n' (n<N) have been assumed to be malicious. Therefore, total network blocking probability, P_B, for the entire network, assuming 'n' to be statistically independent of 'k' and various random time arrivals, t_is, can be determined. The total time 't_b' for which data forwarding gets prohibited due to malicious presence can be expressed as

$$t_b = n.\left(\sum_{i=1}^{k} \Upsilon_i\right)$$

Therefore, probability of blocking in the network can now be written as [28]

$$P_B = \frac{E(n.\sum \Upsilon_i, k)}{N.T} \quad (16)$$

Assuming all variables t_i, 'k' and 'n' to be statistically independent, the above can be simplified as

$$P_B = \frac{E(n)}{N.T}.E\sum(\Upsilon_k/k).P(k)$$

For Uniform Distribution of 'k', the Total network blocking Probability can be calculated by following equation

$$P_B = \frac{E(n)}{N.T}\int_0^T \int_{t_1}^T \dots \int_{t_{((2.k)-1)}}^T \left(t_2 - t_1 + .. + t_{(2.k)} - t_{((2.k)-1)}\right).\frac{1}{T}.\frac{1}{\prod_{i=1}^{((2.k)-1)}(T-t_i)}.dt_{(2.k)}..dt_1.P(k) \quad (17)$$

Using Poisson distribution for 'k', the Total network blocking Probability can be calculated by following equation

$$P_B = \frac{E(n)}{N.T}\int_0^T \int_{t_1}^T \dots \int_{t_{((2.k)-1)}}^T \left(t_2 - t_1 + .. + t_{(2.k)} - t_{((2.k)-1)}\right).\frac{1}{T}.\frac{1}{\prod_{i=1}^{((2.k)-1)}(T-t_i)}.dt_{(2.k)}..dt_1.P_m \quad (18)$$

where P_m has to be determined using equation (12).

5. Simulation Results

The simulations have been carried out using MATLAB13. The total network blocking probability P_B, for entire network and individual blocking probability due to any suspicious malicious node 'j' i.e. P_{bj} have been evaluated. The worst case situation of maximum possible ON-OFF time occurrences for any node with selfish behavior attack has been considered to be twenty. P_{bj} (corresponding to maximum ON/OFF 'k'=10 pulses). For evaluation purposes, a typical network with 50 MANET nodes and total observation time of 100 seconds has been considered.

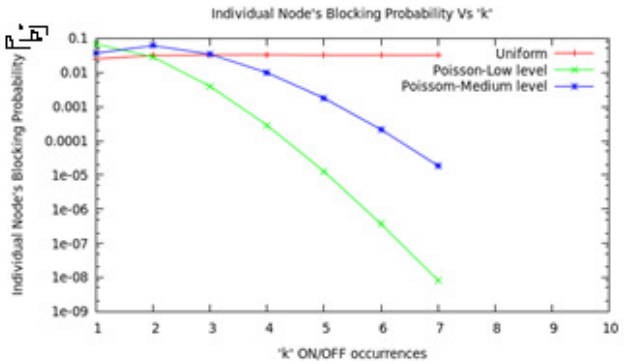

Fig.3 Individual node's Blocking Probability for various values of 'k' with Uniform and Poisson distribution

The fig.3 shows the probability of blocking due to any individual node 'j', P_{bj}, as a function of 'k', the number of ON/OFF pulses of the malicious node, using uniform and Poisson distributions for random variable 'k'. With uniform distribution probability of blocking appears to be almost same with marginal increase in P_{bj} as the number of ON/OFF pulses increase which is expected result. The probability of blocking seems to saturate beyond value of k=2 with uniform distribution. For Poisson distribution with low level malicious activity, the probability of blocking decreases rapidly as number of ON/OFF occurrences increases. This decrease in the probability of blocking can be attributed primarily due to rapid decrease of Poisson probability 'P_m' for higher values of 'k' with average of only one pulse for Poisson distribution. For Poisson distribution with medium level malicious activity, the probability of blocking decreases gradually as 'k' increases beyond two. This again can be attributed due to gradual decrease in Poisson probability 'P_m'. However the maximum value of probability of blocking has been estimated to be almost same for all the three cases

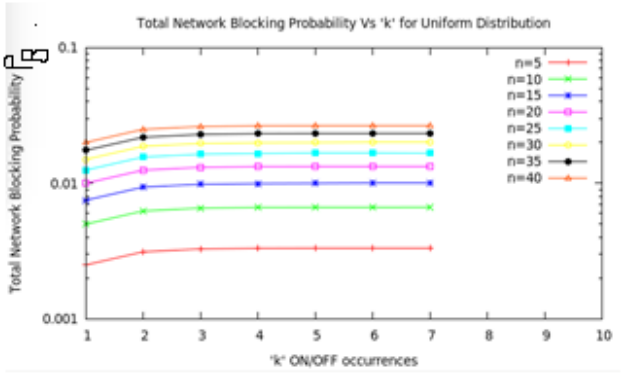

Fig.4 Total Network Blocking Probability for various values of 'k' with Uniform distribution

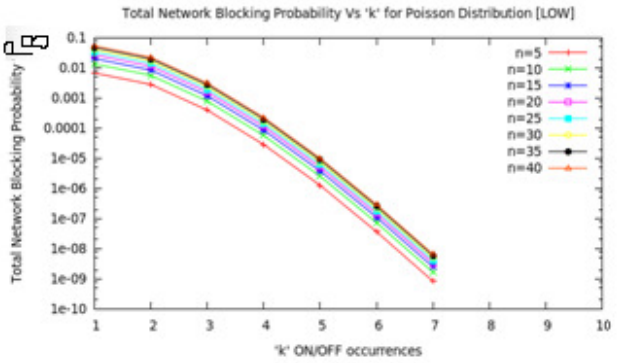

Fig.5 Total Network Blocking Probability for various values of 'k' with Poisson distribution with low level of maliciousness i.e. λ*T=2.

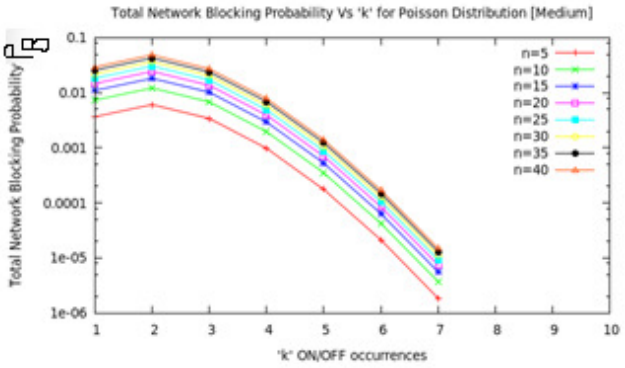

Fig.6 Total Network Blocking Probability for various values of 'k' with Poisson distribution with medium level of maliciousness i.e. λ*T=4

Figures (4), (5) and (6) show variation in total network blocking probability, P_B, with respect to number of ON-OFF pulses 'k' of malicious nodes for various values of number of malicious nodes n=5, 10,.....40, with uniform, Poisson with low level of maliciousness and Poisson with medium level of maliciousness, respectively. It can be readily seen from these figures that overall probability of blocking P_B increases with increase in number of malicious nodes in the network, which can be an expected result. Further it is seen that P_B value also gradually increases with 'k' for uniform distribution and almost becomes constant beyond k=2. For Poisson distributed 'k', P_B is maximum at k=1 for low level maliciousness and at k=2 for medium level maliciousness.

6. Conclusions and suggestions for future work

Maliciousness due to SB attack, has been modeled using uniformly distributed continuous time random variables, Poisson and uniformly distributed discrete values for ON-OFF pulses 'k' and binomially distributed number of malicious nodes 'n' of the network. Formulation for probability of network blocking for individual nodes P_{bj} and total network blocking probability, P_B, based on concept of statistical averaging have been proposed. MATLAB based simulations on typical MANET network of fifty nodes, indicate that blocking probability is maximum around k=2 and it saturates for higher values of 'k' for uniform distribution.

In the above analysis the basic occurrence of random time for ON-OFF switching of nodes has been assumed to be uniformly distributed in available time. However, any other continuous time distributions like, Gaussian, Lognormal, Exponential distribution etc. may also be used in modeling. The analysis can be carried out, using the similar approach. This could, however, substantially increase the computational effort in the modeling and analysis.

However, the above analysis is carried out using different uniform, uniform/Poisson and binomial distributions and results have been included in section5. Based on these results, it is suggested to use a strategy of gradually reducing the normalized dependability trust parameter for suspected malicious nodes from Trust=1 for k=0 to Trust=0.5 for k=1 and Trust=0 for k>=2, irrespective of whether 'k' is uniformly distributed or Poisson distributed. This strategy could then be used in enhancing network throughput using various Trust Aware Routing Framework (TARF) protocols.

References

[1] M. Abolhasan, T. Wysocki, E. Dutkiewicz, "A review of routing protocols for mobile ad hoc networks", Ad Hoc Networks, 1570-8705 2 (1) (2004) 1–22.

[2] Charles E. Perkins, Pravin Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers"

[3] T. Clausen, P. Jacquet, IETF RFC-3626: "Optimized Link State Routing Protocol OLSR", 2003.

[4] Charles E. Perkins, Elizabeth M. Royer, "Ad-hoc On-demand Distance Vector Routing"

[5] D. B. Johnson and D.A. Maltz, "Dynamic Sources Routing in Ad hoc Wireless Networks", Mobile Computing, 1996.

[6] I. ChakeresCenGen, C. Perkins WiChorus, "Dynamic MANET On-demand Routing draft-ietf-manet-dymo-17", 2009.

[7] LoayAbusalah, AshfaqKhokhar and Mohsen Guizani, "A Survey of Secure Mobile Ad Hoc Routing Protocols", *IEEE Communications Surveys and Tutorials*, vol.1, no.4, Fourth Quarter 2008.

[8] Jian Wang, Yanheng Liu, Yu Jiao, "Building a trusted route in a mobile ad hoc network considering Communication reliability and path length", *Journal of Network and Computer Applications*, 34(2011), pp.1138-1149.

[9]Candolin C, Kari H. "A security architecture for wireless ad hoc networks", In: Proceedings of International Conference on mobile computing and networking (MOBICOM'02): October 2002,1095-100.

[10]Pirzada AA, McDonald C., "Establishing trust in pure ad-hoc networks" In: Proceedings of Australian Conference on Computer Science, vol.56; January 2004, pp. 47-54.

[11]Anantvalee T., Wu J., "Reputation-based system for encouraging the cooperation of nodes in mobile ad-hoc networks", In: Proceedings of IEEE International Conference on the communication (ICC'07): June 2007, pp 3383-8.

[12]Peng SC, Jia WJ, Wang GJ, WU J, Guo MY, "Trusted Routing Based on Dynamic Trust Mechanism in Mobile Ad Hoc Networks.",*IEICE TRANSACTIONS on Information and Sysytems* E93-D 2010(3):510-7.

[13] AsmaAdnane , Christophe Bidan , Rafael Timóteo de Sousa Júnior, " Trust-based security for the OLSR routing protocol" , Computer Communications, 36 (2013) 1159–1171

[14] S. Buchegger, J-Y. Le Boudec, "Performance analysis of the confidant protocol : cooperation of nodes – fairness. Dynamic Ad-hoc networks" , Proceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), *IEEE,* 2002.
[15] P. Michiardi, R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks", in: IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security, 2002, pp. 107–121.
[16] K. Meka, M. Virendra, S. Upadhyaya, "Trust based routing decisions in mobile adhocNetworks", in:Workshop on Secure Knowledge Management (SKM), 2006.
[17]Hui Xia, ZhipingJia, Xin Li, Lei Ju,Edwin H.-M. Sha, "Trust prediction and trust-based source routing in mobile ad hoc networks", *Ad Hoc Networks*, 11 (2013) pp. 2096-2114.
[18]Ing-Ray Chen, JiaGuo, FenyoBao, Jin-Hee Cho, "Trust management in mobile ad hoc networks for bias minimization and application performance maximization", *Ad Hoc Networks* 19 (2014) pp. 59-74.
[19] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", In: Proceedings of international conference on mobile computing and networking(MOBICOM'00):August 2000, pp. 255-65.
[20] Zouridaki. C, Mark. B.L., Hejmo.M and Thomas.R.K., "A quantitative trust establishment framework for reliable data packet delivery in MANETs", Proceedings of the 3rd ACM workshop on security of adhoc and sensor networks, vol1, pp.1-10,(2005)
[21]Md. Amir Khusru Akhtar and Sahoo.G, "Mathematical Model for the detection of selfish Nodes in MANETs", *International Journal of Computer science and Informatics*, 2231-5292, vol 1(3), pp25-28(2011)
[22] J. SengathirR. And Manoharan, "Selfish Conscious Mathematical Model based on Reliable Conditional Survivability Co-efficient in MANET Routing", Proceedings of International Conference on Advances Information Technology and Mobile Communication (2013)
[23]Syed S. Rizvi and Khaled M. Elleithy, "A New Scheme for minimizing malicious behavior of mobile nodes in Mobile Ad Hoc Networks", *IJCSIS International Journal of Computer science and Information Security*, vol.3, no.1,(2009)
[24]Hernandez-Orallo, Manuel.D, Serraty, Juan-Carlos Cano, Calafate.T and Manzoni's, " Improving Selfish Node Detection in MANETs Using a collaborative Watchdog", *IEEE Communication Letters*, vol.16, no.5, (2012)
[25] Buchegger S., Boudec J.L., "A Robust reputation system for P2P and mobile ad hoc networks", In Proceedings 2nd Workshop on economics of Peer to Peer system(2004)
[26] Kirti A. Adoni, Mandar Karyakarte, Anil Tavildar, "Security Enhancement in OLSR protocol using Trust Aware Routing Framework" in proceedings of *ICEIT conference on Advances in Mobile Communications, Networking and Computing, April 2015, pp. 84-87.*
[27]A. Rajaram and Dr. S. Palaniswami, "Malicious node detection System for Mobile Ad hoc Networks", *IJCSIT International Journal of Computer Science and Information Technologies*, vol.1 (2), pp.77-85(2010)
[28] Cheny and Zhao Q. (2005) on the lifetime of wireless sensor networks, *IEEE Communications Letters, 9(11):976-978.*
[29] "Probability, Random Variables and Stochastic Processes" A Papoulis, S. Unnikrishnan Pillai, TMH, Fourth Edition

Mrs. Kirti Aniruddha Adoni is presently working as Assistant Professor at P.E.S. Modern College of Engineering, Shivajinagar, Pune, India 411005. She is a Research Student of Electronics and Telecommunication department, V.I.I.T. Research Centre, Kondhwa, Pune, India. She has completed her M.Tech (Microwave) from College of Engineering, Pune, Maharashtra, India in 2010. Her major fields of study are wireless networks, mobile ad-hoc networks

Dr. Anil S. Tavildar is working as Professor Emeritus in Electronics and Telecommunication Engineering at *MKSSS's Cummins college of Engineering*, Pune, India. He has obtained his B.E. (Electronics and Telecommunication Engineering) from University of Pune and PhD (Communication Engineering) from Indian Institute of Technology, Delhi in 1984. He has 28 years of industrial, research and development experience and 16 years of teaching experience. His research interests are in signal processing, wireless and mobile communication systems. Prof Tavildar is Senior Member, IEEE USA, Fellow Member of IETE, India, Founder Member ICIET and Life Member of ISTE, India.