Journal of Computer Science 10 (8): 1397-1402, 2014
ISSN: 1549-3636

doi:10.3844/jcssp.2014.1397.1402 Published Online 10 (8) 2014 (http://www.thescipub.com/jcs.toc)

DENIAL OF SERVICE ATTACK IN DISTRIBUTED WIRELESS NETWORK BY DISTRIBUTED JAMMER NETWORK: A BIRTH-DEATH RANDOM PROCESS ANALYSIS

[1]R. Dhanasekaran and [2]G. Singaravel

[1]Department of DCE, K.S. Rangasamy Institute of Technology, Tiruchengode Namakkal, Tamilnadu, India
[2]Department of IT, K.S.R College of Engineering, Tiruchengode Namakkal, Tamilnadu, India

Received 2014-01-06; Received 2014-02-05; Accepted 2014-03-07

ABSTRACT

Large number of low power, tiny radio jammers are constituting a Distributed Jammer Network (DJN) is used nowadays to cause a Denial of Service (DoS) attack on a Distributed Wireless Network (DWN). Using NANO technologies, it is possible to build huge number of tiny jammers in millions, if not more. The Denial of Service (DoS) attacks in Distributed Wireless Network (DWN) using Distributed Jammer Network (DJN) considering each of them as separate Poisson Random Process. In an integrated approach, in this study, we advocate the more natural birth-death random process route to study the impact of Distributed Jammer Network (DJN) on the connectivity of Distributed Wireless Network (DWN). We express that the Distributed Jammer Network (DJN) can root a phase transition in the performance of the target network. We use Birth-Death Random Process (BDRP) route for this phase transition to evaluate the collision of Distributed Jammer Network (DJN) on the connectivity and global percolation of the target network. This study confirms the global percolation of Distributed Wireless Network (DWN) is definite when the Distributed Jammer Network (DJN) is not more significant.

Key words: DWN, DJN, Birth-Death Random Process, BDRP, Network Architecture, DoS Attacks

1. INTRODUCTION

A manifestation of the development of radio technology is the transition from huge vacuum tube radios to micro nanotube radios. This in its wake has ushered in radical changes in the design and use of radio devices. Distributed Jammer Network (DJN) consists of a huge number of tiny low powered Jammers distributed inside a target network, with the purpose of jamming the target Distributed Wireless Network (DWN) (Huang *et al*., 2011). Recent advances in Micro-Electro Mechanical System (MEMS) and NANO technologies (Otis *et al*., 2004; Weldon *et al*., 2008) make it possible to build sufficient number of NANO jammers that the Distributed Jammer Network (DJN) takes the form of a dust cloud in the air, called jamming dust of micro sensors (Kahn *et al*., 1999).

Miniaturization of jammers is possible, compared to wireless sensors, due to the fact that jammers emit only noise signals without requiring complex modulations, filtering, scaling and other signal processing functions. Distributed Jammer Network (DJN) has many applications in the defense scenario of a country. New devices such as nanotube radio may find their application in the jamming dust. Distributed Jammer Network (DJN) forms a mirror image to the Distributed Wireless Network (DWN). Distributed jammer network can be deployed to form a low power air-born jamming dust, to disrupt the communication capabilities of an adversary, which is more advantages because the naked eye cannot even see the nanotube jammers, with much reduced effect on self-interface. The advantage of self-interface free jamming has been amply and purposefully seen in the second Iraq war as reported in the Washington post.

Corresponding Author: R. Dhanasekaran, Department of DCE, K.S. Rangasamy Institute of Technology

Civilian applications of distributed jammer network include the silencing of cell phones using jammers in restaurant, theatres and conversion halls in many countries where it is legal. Although owning or using jammers is illegal in USA. In Italy, jammers are reportedly used in examinations centre to avoid undesirable activities. Second nature of religious services is preserved in temples and churches using jammers. Deploying a low-power distributed jammer network in the place of high-power jammers is clearly preferable due to the health concerns.

Distributed Jammer Network is different from traditional jammers (Richa *et al*., 2010) used by the military, which are traditionally located outside the target distributed wireless network and produce inference by beaming high-power radio signal over long distances using directional antenna (Huang *et al*., 2011). As a network with large number of tiny nodes, Distributed Jammer Network (DJN) in a huge network perspective has a prominent effect on any Distributed Wireless Network (DWN). Distributed Jammer Network (DJN) has simple redundancy, hard to detect ability, self-interference free capabilities and low power consumption. Given that the total power consumption is constant, the gain of using a large number of jammers has been brought out in (Huang *et al*., 2011).

The wide usage of the wireless medium leaves it vulnerable to intentional interference attacks, typically referred to as jamming. This intentional interference with wireless mediums can be used to introduce the Denial of Service (DoS) attacks on wireless networks. Typically, jamming has been addressed under an external threat model (Pelechrinis *et al*., 2011). The open nature of the wireless networks, it has multiple security threats. Anyone with a transceiver can eavesdrop on wireless transmissions, inject spurious message or jam legitimate ones. While eavesdropping and message injection can be prevented using cryptographic methods, jamming attacks are much harder to counter (Proano and Lazos, 2012).

1.1. General Discussion and Related Work

Wireless networks have been used in many applications, such as home automation, military surveillances and entity tracking systems. The wireless nodes have low computational capabilities and are highly resource constrained. Routing protocols of wireless networks are prone to various routing attack, such as black hole, rushing and Denial of Service (DoS) attacks (Ramachandran and Shanmugan, 2011). There is an improved risk of security attacks, to defeat concealed attacks there is a necessity to authenticate both access points and wireless stations (Moorthy and Sathiyabama, 2012). Flooding is one of the types of Denial of Service (DoS) attack in mobile ad-hoc network. This kind of attack consumes battery power, storage space and bandwidth. Flooding the excessive number of packets ma degrade the performance of the network (Madhavi and Duraiswamy, 2013).

Previous works on jamming concentrates on military applications (Huang *et al*., 2011). Radio interference attacks are a serious threat to the operations of a wireless network. Jamming attacks, it is important to understand the different threat models. The counter measures that may be employed to defend against jamming attacks. Our work takes, Denial of Service (DoS) attacks in Distributed Wireless Network (DWN) by Distributed Jammer Network (DJN) as a Birth-Death Random Process X (a) where ‘a’ is the area of analysis and ‘n’ is the number of linked nodes. The Birth-Death Random Process (BDRP) confirms that the global percolation in Distributed Wireless Network (DWN).

This study is arranged as follows: (a). Materials and Methods are in section-2. (b). The Mathematical basis of Birth-Death Random Process (BDRP) is in section-3. (c). Results are in section-4. (d). Conclusion and future work are in section-5 and References follow in section-6.

2. MATERIALS AND METHODS

2.1. Random Process

The theory of probability attempts to quantity the chance of occurrence of an event of a random experiment. In a context where the discussion cannot be restricted to one random variable, we are confronted with a family of random variables.

A stochastic process (also called a random process) $\{X(t), t\varepsilon T\}$ is a family of random variables, each of which is a function of time. The set of all values X(t) of the process constitute its state space. If at any particular point of time t_3 is $X(t) = 3$, the process is said to be at state x, at time t. The set of all time points constitute the time space of the process.

A random process with a discrete state space and continuous time space is called a discrete random process. Birth-death random process is a discrete random process where discrete state space represents the number of connected transmitter nodes in the area ‘a’ of interest (called birth) and death denotes the demise the link in the area ‘a’ with respect to DWN/DJN environment.

If n is the number active linkages in an area ‘a’ and if $n \rightarrow \infty$, as $a \rightarrow \infty$ then there exists the global connectivity for the Distributed Wireless Network (DWN) in-spite of the Distributed Jammer Network (DJN).

3. MATHEMATICAL BASIS

3.1. Birth-Death Random Process

Birth-Death Random Process (BDRP) is a discrete random process satisfying the birth-death postulates (Veerarajan, 2004; Abramowitz *et al*., 2012; Bruce and Westwig, 2010) if $P_n(a) = P\{X(a) = n\}$ = probability that the active links of Distributed Wireless Network (DWN) in an area 'a' is n, in a birth-death random process satisfies the difference-differential Equation:

$$P'_n = \lambda_{n-1}P_{n-1} - (\lambda_n + \mu_n) P_n + \mu_{n+1} P_{n+1} \text{ for } n \geq 1 \qquad (3.1.1)$$

(where,′ is derivative w.r.t 'a') and:

$$P'_0 = -\lambda_0 P_0 + \mu_1 P_1 \text{ for } n \geq 0 \qquad (3.1.2)$$

where, λ_n, μ_n are the mean birth/death rates when n active nodes are in the Distributed Wireless Network (DWN).

Figure 1 shows, when a birth occurs, the process goes from state n to n+1. When a death occurs, the process goes from state n to n-1. The process specified by birth rates λ_n where n = 0…∞ and death rates μ_n where n = 1…∞.

Solving (3.1.1) and (3.1.2) we get $P_n(a)$ [n≥0] which gives P{X(a) = n} , the probability distribution of X(a).
If P′n is small and λn = λ and µn = µ then (3.1.1) gives:

$$\mu P_{n+2} - (\lambda + \mu) P_{n+1} + \lambda P_n = 0 \qquad (3.1.3)$$

And this is a second order difference equation with constant coefficients with the general solution [C1 and C2 are arbitrary constants]:

$$P_n = C_1{}^{m_1 a} + C_2{}^{m_2 a} \qquad (3.1.4)$$

where, m_1, m_2 are the roots of:

$$\mu m^2 - (\lambda + \mu) m + \lambda = 0 \qquad (3.1.5)$$

Given by:

$$m1, m2 = \frac{1}{2\mu}\left[(\lambda + \mu) \pm (\lambda - \mu)\right] = 1, \frac{\lambda}{\mu} \qquad (3.1.6)$$

where, λ = µ:

$$P_n = (C_1 + C_2 a) e^a \qquad (3.1.7)$$

3.2. Linear Birth-Death Process

If we assume a linear birth-death random process by taking $\lambda_n = n\lambda$ and $\mu_n = n\mu$, birth-death Random Process equations are for n≥1:

$$P'_n(a) = (n-1)\lambda P_{n-1}(a) - n(\lambda + \mu) P_n(a) + (n+1)\mu P_{n+1}(a) \qquad (3.2.1)$$

And:

$$P'_m(a) = \mu P_1(a) \qquad (3.2.2)$$

It can be shown (Veerarajan, 2004), that the simple birth-death random process:

$$P_n(a) = \{1 - \alpha(a)\}\{1 - \beta(a)\}\{\beta(a)\}^{n-1} \text{ for } n \geq 1 \qquad (3.2.3)$$

With:

$$P_0(a) = \alpha(a) \qquad (3.2.4)$$

Also the mean and variance of popular size in a linear birth-death process X(a) are given by:

$$E\{x(a)\} = e^{(\lambda-\mu)a} \qquad (3.2.5)$$

And:

$$\mathrm{Var}\{X(a)\} = \left[\frac{\lambda + \mu}{\lambda - \mu}\right] e^{(\lambda-\mu)a}\left\{e^{(\lambda-\mu)a} - 1\right\} \qquad (3.2.6)$$

Again, when no jammers are present the process is a pure link process with the difference-differential system (for the linear case) as:

$$P'_n(a) = (n-1)\lambda P_{n-1}(a) - n\lambda P_n(a) \qquad (3.2.7)$$

For n≥1 and with the solutions:

$$P_n(a) = e^{-\lambda a}\left(1 - e^{-\lambda a}\right)^{n-1}; n \geq 1 \qquad (3.2.8)$$

Also for the simple birth process {X(a)}:

$$E\{X(a)\} = e^{\lambda a} \qquad (3.2.9)$$

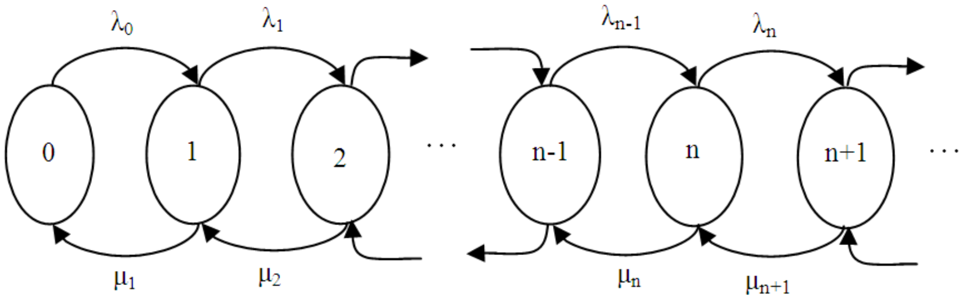

Fig. 1. Birth-death rates for n active nodes

And:

$$\mathrm{Var}\{X(a)\} = e^{\lambda a} \tag{3.2.10}$$

4. RESULTS

4.1. Birth-Death Random Process Analysis

The random process X(a) denotes the number of active links in the DWN with $P_n(a) = P\ \{X(a) = n\}$, the probability distribution of X(a), where 'a' is the area under consideration where n active links are present.

When λ_n and μ_n are the birth and death rates, the probability distribution of X(t) are governed by the difference differential system given by (3.1.1) and (3.1.2). We propose to give the general solution of this system for several special cases.

If P'_n is small ($P'_n = \frac{dp_n}{da}$ can be considered as a probabilistic measure of the rate of change of 'n' w.r.t 'a' and when P'_n is small, we can interpret it as that the DJN effect is not significant).

We get the difference Equation:

$$\lambda_{n-1}P_{n-1} - (\lambda_n + \mu_n)\ P_n + \mu_{n+1}P_{n+1} = 0\ (n \geq 1) \tag{4.1.1}$$

And:

$$P'_0 = -\lambda_0 P_0 + \mu_1 P_1 \tag{4.1.2}$$

The general solution of (3.1.1) is:

$$P_n(a) = Ae^{m_1 a} + B^{m_2 a} \tag{4.1.3}$$

where, m_1, m_2 are the roots of:

$$\mu_{n+2}m^2 - (\lambda_{n+1} + \mu_{n+1})\ m + \lambda_n = 0 \tag{4.1.4}$$

$$m = \frac{1}{2^{\mu}{}_{n+2}}\left[\frac{(\lambda_{n+1} + \mu_{n+1})}{\pm\sqrt{(\lambda_{n+1} + \mu_{n+1})^2 - n(\lambda_n \mu_{n+2})}}\right] \tag{4.1.5}$$

and when the discriminate is positive.

In the special case $\lambda_n = \lambda$, $\mu_n = \mu$ for all n, (4.1.5) gives:

$$m = \frac{1}{2\mu}\left[(\lambda + \mu) \pm (\lambda - \mu)\right] = \frac{\lambda}{\mu} = 1 \tag{4.1.6}$$

With:

$$P_n = Ae^{\frac{\lambda}{\mu}a} + Be^a$$

And:

$\bar{X}(a) = \sum_0^\infty n\ P_n \rightarrow \infty$ in general as $a \rightarrow \infty$

Hence global percolation of DWN is definite when the DJN effect is not more significant.

4.2. Linear Model When $\lambda_n = n\lambda$, $\mu_n = n\mu$

In this case the random process results are:

$$E\{X(a)\} = {}^{e(\lambda-\mu)a} \tag{4.2.1}$$

$$\mathrm{Var}\ \{X(a)\} = \left[\frac{\lambda + \mu}{\lambda - \mu}\right] e^{(\lambda+\mu)a}\left\{e^{(\lambda+\mu)a} - 1\right\} \tag{4.2.2}$$

Case 1: $\lambda > \mu$,

Then (4.2.1) gives that as a → ∞, E{X(a)} → ∞. Hence whenever the jamming rate is less than linking rate global percolation of the DWN is definite.

Case 2: $\lambda = \mu$,

Then E{x(a)} = 1 irrespective of the value of a. Hence for equal jamming and linking rates global percolation of the DWN is impossible.

Also:

$$\left.\begin{matrix}\text{Lt}\\ \lambda-\mu\end{matrix}\right\}\text{Var}\{X(a)\}=\left.\begin{matrix}\text{Lt}\\ \lambda-\mu\end{matrix}\right\}(\lambda+\mu)\left[\frac{e^{(\lambda-\mu)a}}{\lambda-\mu}-1\right]=2a\mu \;=\; 2a\lambda$$

Indicating large variance as a → ∞ and is interpreted as hugely dispersed link less isolated Distributed Wireless Network (DWN) nodes.

Case 3: $\mu > \lambda$:

$$E(x) = e^{-(\lambda-\mu)a} \rightarrow 0 \text{ as } a \rightarrow \infty$$

Hence the Distributed Wireless Network (DWN) dies out crashing due to superior jamming effect of the Distributed Jammer Network (DJN). Jamming of communications in enemy territory is done due to a powerful Distributed Jammer Network (DJN) let loose on their Distributed Wireless Network (DWN).

4.3. Model with λ = μ for Any Value of n. General Case.

The difference differential Equation is:

$$P'_n = +\lambda P_{n-1} - (\lambda+\mu)P_n + \mu P_{n+1}; \quad n \geq 1 \tag{4.3.1}$$

Laplace transforms solution (Widder, 2010).

Let:

$$LP_n = L_n(S) \tag{4.3.2}$$

Then:

$$LP'_n = SL_n\left[\text{Where } P_n(0)=0\right] \text{ When } n \geq 1 \tag{4.3.3}$$

On taking LT, (4.3.1) gives:

$$(S+\lambda+\mu)L_n = \lambda L_{n-1} + \mu L_{n+1} \tag{4.3.4}$$

$$\mu L_{n+2} - (S+\lambda+\mu)L_{n+1} + \lambda L_n = 0 \tag{4.3.5}$$

This is a second order difference equation with constant coefficients, with auxiliary Equation:

$$\mu m^2 - (S+\lambda+\mu)m + \lambda = 0 \tag{4.3.6}$$

With:

$$m = \frac{1}{\mu}[S+\lambda+\mu'],\frac{\mu''}{\mu} \tag{4.3.7}$$

With general solution:

$$L_n = Ae^{\frac{S}{\mu}} + B^{\frac{\mu''}{\mu}} \tag{4.3.8}$$

where, A, B, μ, μ” are constants.

Taking Inverse Laplace Transforms (ILT):

$$P_n = A\delta(a+\frac{1}{\mu}) + Be^{\frac{\mu''}{\mu}}\delta(a) \tag{4.3.9}$$

where, δ is the direct delta function. Using (4.3.4) one can compete E{X(a)} for this model, numerically or by simulation.

5. CONCLUSION

The Denial of Service (DoS) attack in Distributed Wireless Network (DWN) by Distributed Jammer Network (DJN) as a birth-death discrete random process X(a) where ‘a’ is the area of analysis, where E{X(a)} is the mean number of linked nodes of Distributed Wireless Network (DWN) when λ_n and μ_n are the mean linking/jamming rates per unit area when n linked nodes are in the area ‘a’.

The difference differential equation for $P_n(a)$ = P{X(a) = n} has been analyzed with E{X(a)} and Var {X(a)} for various case of λ_n, μ_n values and interpreted. The quantified results of this Birth-Death Random Process (BDRP) mathematical model, confirms the theoretical hypothesis that the global percolation of Distributed Wireless Network (DWN) is definite when the Distributed Jammer Network (DJN) effect is not more significant.

In future, analyze this study using, the topology employed in the network, medium used for data access and data transfer rate (time) rather than linked nodes (n) and area (a) that is in our approach.

6. REFERENCES

Abramowitz, M. and I.A. Stegun, 2012. Hand Book of Mathematical Functions: With Formulas, Graphs and Mathematical Tables. 1st Edn., Courier Dover Publications, New York, ISBN-10: 0486612724, pp: 1046

Bruce, R.K. and E.A. Westwig, 2010. Mathematical Physics: Applied Mathematics for Scientists and Engineers. 2nd Edn., John Wiley and Sons, ISBN-10: 3527406727, pp: 689.

Huang, H., N. Ahmed and P. Karthik, 2011. On a new type of denial of service attack in wireless networks: The distributed jammer network. IEEE Trans. Wireless Commun., 10: 2316-2324. DOI: 10.1109/TWC.2011.052311.101613

Kahn, J.M., R.H. Katz and K.S.J. Pister, 1999. Mobile networking for smart dust. Proc. ACM Mobi Com, University of California.

Madhavi, S. and K. Duraiswamy, 2013. Flooding attack aware secure AODV. J. Comput. Sci., 9: 105-113. DOI: 10.3844/jcssp.2013

Moorthy, M. and S. Sathiyabama, 2012. Effective authentication technique for distributed denial of service attacks in wireless local area networks. J. Comput. Sci., 8: 828-834. DOI: 10.3844/jcssp.2012

Otis, B.P, Y.H. Chee, R. Lu, N.M. Pletcher and J.M. Rabaey, 2004. An ultra-low power MEMS-based two-channel transceiver for wireless sensor networks. Proceedings of the Symposium on Digest of Technical Papers VLSI Circuits, Jun. 17-19, IEEE Xplore Press, pp: 20-23. DOI: 10.1109/VLSIC.2004.1346487

Pelechrinis, K., M. Iliofotou and V.S. Krishnamurthy, 2011. Denial of service attacks in wireless networks: The case of Jammers. IEEE Commun. Surveys Tutorials, 13: 245-257. DOI: 10.1109/SURV.2011.041110.00022

Proano, A. and L. Lazos, 2012. Packet-hiding methods for preventing selective jamming attacks. IEEE Trans. Dependable Secure Comput., 9: 101-114 . DOI: 10.1109/TDSC.2011.41

Ramachandran, S. and V. Shanmugan, 2011. Impact of sybil and wormhole attacks in location based geographic multicast routing protocol for wireless sensor networks. J. Comput. Sci., 7: 973-979. DOI: 10.3844/jcssp.2011.

Richa, A., C. Scheideler, S. Schmid and J. Zhang, 2010. A jamming-resistant MAC protocol for multi-hop wireless networks. Proceedings of the 24th International Conference on Distributed Computing, Sept. 13-15, Springer-Verlag Berlin Heidelberg, Cambridge, USA., pp: 179-193. DOI: 10.1007/978-3-642-15763-9_17

Veerarajan, T., 2004. Probability, Statistics and Random Process. 1st Edn., Tata McGraw Hill, ISBN-10: 0070494827, pp: 693.

Weldon, J., K. Jensen and A. Zettl, 2008. Nanomechanical radio transmitter. Physica Status Solidi, 245: 2323-2325. DOI: 10.1002/pssb.200879639

Widder, D.V., 2010. The Laplace Transform. 1st Edn., Dover Publications.