International Journal of Industrial Engineering & Production Research (2019) 30: 165-172
DOI: 10.22068/ijiepr.30.2.165

RESEARCH PAPER

On the Network Reliability under Shock Models

Mohammadali Asadi[1] & Sareh Goli[2]*

Received 23 May 2017; Revised 10 February 2019; Accepted 8 May 2019; Published Online 20 June 2019

ABSTRACT
In the study of system reliability and survival analysis, the reliability function, the mean residual lifetime, and the hazard rate are important measures factors. Besides, they provide helpful tools to analyze the maintenance policies and burn-in of a system. This study considers a network containing n components with two states, up and down, showing whether an element is connected to other parts or not. It is supposed here that the system is subject to shocks that may cause component failure in which the number of crashes at each shock follows a truncated binomial distribution, and the process of shocks is associated with nonhomogeneous Poisson. The reliability function, the mean residual lifetime, and the hazard rate of this network are investigated under the shock model by experimenting them on a real system.

KEYWORDS *Network reliability, Shock model, T-Signature, Mean residual lifetime, Hazard rate.*

1. Introduction

Networks are one of the most important systems in industrial and software engineering. A network can be modelled by the triplet $N = (V, E, T)$, where set V stands for the nodes, and set E shows the links in the form of the relation between nodes, $T \subseteq E$ is a subset of E called vital-links. Let $|V| = m$ and $|E| = n$. In the following, the components of a network are subject to failure when the links are subject to failure and the nodes are assumed reliable. It is obvious that the failure of components may change the state of the network.

In Computer Networks, the nodes represent a variety of devices such as computers, servers, switches, routers, and etc. The edges are the information transmission lines containing telecommunication fibres, railways, copper cables, and wireless channels connecting these computers, and the shock may occur as a result of a sequence of attacks. Network security is one of the most important parts of this field, such that network engineers and administrators consider many measures and much money for keeping the networks safe. According to the CISCO annual security report [1], there are about 28 million network connections evaluated on the Internet every day in 2014-2015, and 50,000 network intrusions are detected every day. Attacks and network threats proliferate daily; therefore, modelling the network flows can be a useful method for better network analysis and visualization.

Over the past decade, several methods have been introduced to evaluate the reliability of a network, some of which are [2, 5, 6, 9, 10, 11, 12]; however, they often describe the reliability of a network as a function based on a defined signature such that the number of failure nodes at every shock is at most one; however, there are later models such as the model of Zarezadeh et al. (2016) designed over a kind of signature's notation called t-signature in which more than one node may break at every shock.

The present study considers a network through the former two-stated shock model to describe a counting-random-process network attacks model, and each can cause more than one node to break. Under this assumption, a new approach to the reliability function, the mean residual lifetime, and the hazard rate of the network is presented. The shock-model network can be extended for every network with every dataset; hence, our results are used to analyze the survival of a network simulation, dealing with shocks and, especially, attacks [7].

The aim of this paper is to obtain the reliability function, the mean residual lifetime, and the hazard rate of the network by using the t-signature method. In Section 1, it is supposed that each shock follows a truncated binomial

* **Corresponding author:** ***Sareh Goli***
s.goli@cc.iut.ac.ir

1. Department of Mathematical Sciences, Isfahan University of Technology, Isfahan 84156, Iran.
2. Department of Mathematical Sciences, Isfahan University of Technology, Isfahan 84156, Iran.

distribution and that the process of shocks is a nonhomogeneous Poisson process. In Section 2, the simulation of a real network with hybrid topology and a full attack scenario applied to the network are described. Finally, some analytical properties of the network are determined.

2. Network Reliability under Shock Models

Let the edges of a network have statistically independent and identically distributed (i.i.d.) lifetimes $X_1, X_2, \dots, X_n$ with a common continuous distribution function F, and the network has a lifetime T, which is a function of $X_1, X_2, \dots, X_n$. Prior to presenting the main results, some basic concepts that are useful in our derivation are briefly given.

Definition 1: (Samaniego, (1985)) Assume that $\pi = (e_{i_1}, e_{i_2}, \dots, e_{i_n})$ is a permutation of the network edge number. Suppose that all edges in this permutation are connected. This study moves along the permutation from left to right and turn the state of each edge from connected to disconnected state. Under the assumption that all permutations are equally the same, the signature vector of the network is defined as $s = (s_1, s_2, \dots, s_n)$, where

$$s_i = \frac{n_i}{n!}, \qquad i = 1, \dots, n,$$

and n_i is the number of permutations in which the failure of the i^{th} edge causes a change from the state of the network to a disconnected state. In other words, s_i is the probability that the lifetime of the network equals to the i^{th} ordered lifetimes among X_i's, i.e., $s_i = \Pr[T = X_{i:n}]$, where $X_{i:n}$ is the i^{th}-order statistic among the random variables (r.v.s) $X_1, X_2, \dots, X_n$.

Definition 2: (Zarezadeh et al. (2016)) Assume that $M \in \{1, 2, \dots, n\}$ is a discrete r.v. as the minimum number of edges whose breaks cause the network to disconnect. Under the assumption that all the ways of the order of edge breaks are equally the same, the *t*-signature vector of the network is defined as $s^\tau = (s_1^\tau, s_2^\tau, \dots s_n^\tau)$, where

$$s_i^\tau = \frac{n_i}{n^*}, \qquad i = 1, \dots, n,$$

and n_i is the number of ways of the order of edge breaks in which $M = i$, and n^* is the number of ways that the edges of the network break under the assumption that ties may occur as follows:

$$n^* = \sum_{j=1}^{n} \sum_{k=0}^{j} \binom{j}{k} (-1)^k (j-k)^n .$$

There is an efficient algorithm for computation n^* and signature vector [3].

Note that the signature vector and the t-signature vector defined in Definitions 1 and 2 depend on the structure of the network and do not depend on the real random mechanism of the edge failures.

The reliability function of the network lifetime, T, at time $t > 0$ is as follows:

$$R_T(t) = \Pr[T > t] = \sum_{i=1}^{n} s_i \Pr[X_{i:n} > t]. \quad (1)$$

In the following theorem, which is introduced by Gertsbakh and Shpungin [2], we obtain the reliability of the network under the assumption that all orders of breaks are equally the same.

Theorem 1: Assume that the component failures appear according to a renewal process $\{N(t), t \geq 0\}$ defined as a sequence of i.i.d. non-negative random variables $Y_1, Y_2, \dots$. The random variable $N(t)$ shows the number of links that are disconnected on the network at the interval $[0, t]$, and the breaks in process $\{N(t), t \geq 0\}$ appear at the instants

$$S_k = \sum_{i=1}^{k} Y_i, \qquad k = 1, 2, \dots .$$

Let all orders of breaks be equally the same, and the reliability function of the network lifetime can be represented as follows, and this is valid under any counting process:

$$R_T(t) = \Pr[T > t] = \sum_{i=1}^{n} \left[\sum_{k=i+1}^{n} s_k \right] \Pr[N(t) = i], \; t > 0.$$

Consider a network with lifetime T subject to shocks (attacks), where shocks appear according to a counting process, $N(t) \in \{1, 2, \dots, n\}$ denotes the number of links that disconnects at time t and the shocks appear according to a counting process by $\{\xi(t), t > 0\}$ with random time instants $\vartheta_1, \vartheta_2, \dots$ and random variable K_i, for $i = 1, \dots, n$, denoting the number of components that fail at the i^{th} attack and $K_0 := 0$.

Zarezadeh et al. (2016) demonstrated that the reliability function could be written as follows:

$$R_T(t) = \Pr[T > t] = \Pr[N(t) < M], \quad (2)$$

where $N(t) = \sum_{i=0}^{\xi(t)} K_i$, and we have

$$\Pr[N(t) \le x] = \sum_{k=0}^{+\infty} H_k(x) \Pr[\xi(t) = k],$$

where

$$H_k(x) = \Pr\left[\sum_{i=0}^{\xi(t)} K_i \le x \middle| \xi(t) = k\right].$$

From (2) and the last result, we have

$$\begin{aligned} \mathrm{R_T(t)} &= \Pr[T > t] = \Pr[N(t) < M] \\ &= \sum_{i=1}^{n} \Pr[M = i] \Pr[N(t) \le i-1] \\ &= \sum_{i=1}^{n} s_i^{\tau} \Pr[N(t) \le i-1]. \end{aligned} \quad (3)$$

Let $\bar{S}_j^{\tau} = \sum_{i=j+1}^{n} s_i^{\tau}$ and from (3), the following function is obtained as follows:

$$\begin{aligned} \mathrm{R_T(t)} &= \Pr[T > t] = \sum_{i=1}^{n} s_i^{\tau} \Pr[N(t) \le i-1] \\ &= \sum_{i=1}^{n} s_i^{\tau} \sum_{k=0}^{+\infty} H_k(i-1) \Pr[\xi(t) = k] \\ &= \sum_{k=0}^{+\infty} \beta_{k,n} \Pr[\xi(t) = k], \end{aligned} \quad (4)$$

where, for $k = 0, 1, \ldots$, we have

$$\begin{aligned} \beta_{k,n} &= \sum_{i=1}^{n} s_i^{\tau} H_k(i-1) \\ &= \sum_{j=0}^{n-1} \bar{S}_j^{\tau} \Pr[\sum_{i=0}^{k} K_i = j]. \end{aligned} \quad (5)$$

In order to study the aging behavior of a system, the mean residual lifetime (MRL) is a helpful tool. The MRL represents the expected value of the remaining lifetime $T - t$ under the condition that the system is working. Let T be a continuous random variable denoting the lifetime of the system with distribution function $F(t)$. The MRL of T is defined as follows:

$$M(t) = E(T - t | T \ge t) = \frac{\int_t^{+\infty} R_T(u)du}{R_T(t)},$$

provided that $R_T(t) > 0$.
The following theorem gives a form for the mean lifetime of a network system.

Theorem 2: Let T be a continuous random variable denoting the lifetime of a network with distribution function $F(t)$. The MRL of a network system is as follows:

$$M(t) = \frac{\sum_{k=0}^{+\infty} \beta_{k,n} \int_t^{+\infty} \Pr[\xi(u) = k]\, du}{\sum_{j=0}^{+\infty} \beta_{j,n} \Pr[\xi(t) = j]}. \quad (6)$$

Proof:

$$\begin{aligned} M(t) &= E(T - t | T \ge t) \\ &= \frac{\int_t^{+\infty} R_T(u)du}{R_T(t)} \\ &= \frac{\int_t^{+\infty} \sum_{k=0}^{+\infty} \beta_{k,n} \Pr[\xi(u) = k]\, du}{\sum_{j=0}^{+\infty} \beta_{j,n} \Pr[\xi(t) = j]} \\ &= \frac{\sum_{k=0}^{+\infty} \beta_{k,n} \int_t^{+\infty} \Pr[\xi(u) = k]\, du}{\sum_{j=0}^{+\infty} \beta_{j,n} \Pr[\xi(t) = j]}. \end{aligned}$$

In the sequel, it is assumed that the number of component failures at each shock follows a truncated binomial distribution. Let a shock cause, at least, a component to fail with probability p and the components fail independent of each other. Assuming that K_1 represents the number of failed components at the first shock. It is obvious that K_1 has truncated binomial distribution. Suppose that the number of failed components in the i^{th} shock, K_i, $i > 1$, depends only on $K_1, K_2, \ldots, K_{i-1}$. In other words, we have

$$\Pr[K_1 = k] = \binom{n}{k} \frac{p^k q^{n-k}}{1 - q^n}, \; k = 1, \ldots, n, \quad (7)$$

For $i \ge 2$,

$$\Pr[K_i = k \mid \sum_{j=1}^{i-1} K_j = w] = \binom{n-w}{k} \frac{p^k q^{n-w-k}}{1-q^{n-w}}, \quad k = 1, \dots, n-w, \ w < n, \tag{8}$$

where $q = 1 - p$.

Lemma 1: By using Assumptions (7) and (8), we have

$$\Pr[\sum_{i=1}^{k} K_i = j] = \binom{n}{j} \frac{\left(1-q^k\right)^j q^{k(n-j)}}{1-q^n}, \quad j = 1, \dots, n, \ k = 1, 2, \dots. \tag{9}$$

Proof: For $k = 1$, the result is true by Relation (7). Let the result be true for $k = m$, that is,

$$\Pr[\sum_{i=1}^{m} K_i = j] = \binom{n}{j} \frac{(1-q^m)^j q^{m(n-j)}}{1-q^n}.$$

Then, for $k = m + 1$, we get

$$\begin{aligned}
&\Pr\left[\sum_{i=1}^{m+1} K_i = j\right] \\
&= \sum_{k=0}^{j} \Pr\left[K_{m+1} = j-k \middle| \sum_{i=1}^{m} K_i = k\right] \\
&* \Pr\left[\sum_{i=1}^{m} K_i = k\right] \\
&= \sum_{k=0}^{j} \binom{n-k}{j-k} p^{j-k} q^{n-j} \Pr\left[\sum_{i=1}^{m} K_i = k\right] \\
&= \sum_{k=0}^{j} \binom{n-k}{j-k} p^{j-k} q^{n-j} \frac{\binom{n}{k}(1-q^m)^k q^{m(n-k)}}{1-q^n} \\
&= \binom{n}{j} \sum_{k=0}^{j} p^{j-k} q^{n-j} \frac{\frac{j!}{k!(j-k)!}\left(p^k \left(\sum_{i=1}^{m-1} q^i\right)^k\right) q^{m(n-k)}}{1-q^n} \\
&= \binom{n}{j} p^j q^{n(m+1)-j} \sum_{k=0}^{j} \frac{\binom{j}{k}\left(\sum_{i=1}^{m-1} q^i / q^m\right)^k}{1-q^n} \\
&= \binom{n}{j} \frac{p^j q^{n(m+1)-j} \left(\frac{\sum_{i=0}^{m} q^i}{q^m}\right)^j}{1-q^n} \\
&= \binom{n}{j} \frac{(1-q^{m+1})^j q^{(m+1)(n-j)}}{1-q^n}.
\end{aligned}$$

Theorem 3: Let T denote the lifetime of a network with a continuous distribution $F(t)$. The reliability of a network at time t is as follows:

$$P(T > t) = \sum_{k=0}^{+\infty} \beta_{k,n}^* \Pr[\xi(t) = k],$$

where $\beta_{0,n}^* = 1$ and, for $k = 1, 2, \dots$, we have

$$\begin{aligned}
\beta_{k,n}^* &= \sum_{j=0}^{n-1} \bar{S}_j^{\tau} \Pr[\sum_{i=0}^{k} W_i = j] \\
&= \sum_{j=0}^{n-1} \bar{S}_j^{\tau} \binom{n}{j} \frac{\left(1-q^k\right)^j q^{k(n-j)}}{1-q^n} \\
&= \sum_{i=1}^{n} s_i^{\tau} \sum_{j=0}^{i-1} \binom{n}{j} \frac{\left(1-q^k\right)^j q^{k(n-j)}}{1-q^n} \\
&= \sum_{m=1}^{n} \sum_{j=n-m}^{n-1} \bar{S}_j^{\tau} \binom{n}{j} \binom{j}{n-m} \frac{(-1)^{j-n+m} q^{km}}{1-q^n}.
\end{aligned}$$

3. Realistic Network

Networks are categorized by their topologies. There are many types of topologies with different reliability functions [3]. According to the reports of the Information Security Centre of Excellence (ISCX) at University of New Brunswick, it can be supposed that a realistic network contains the main structure and many substructures. For testing the results of the previous chapter, the intrusion detection dataset of this network is used [7].

The ISCX network consists of 21 interconnected Windows workstations. The systems' operators chosen as a different set of known attacks against the network would be possible. Indeed, the workstations of this network consist 17 Windows XP SP1, 2 Windows XP SP2, 1 Windows XP SP3, and 1 Windows 7.

To simplify the problem, we categorize the network into 4 sub-networks that connect with the main part by links. These sub-networks are called G_1, G_2, G_3, G_4. The fifth link, G_5, provides the means to conduct non-disruptive monitoring and maintenance of workstations and servers. Since the traffic is not captured, tasks such as loading applications and tuning service parameters are made possible.

The network has 3 servers, main server, secondary server, and additional servers. The main server is responsible for delivering the network's website, providing email services, and acting as the internal resolver considered to be

Ubuntu 10.04, and the secondary server is responsible for internal ASP.NET applications considered to be Windows Server 2003. The additional servers consist of servers that provide web, email, DNS, and Network Address Translation (NAT) services.

One of the advantages of this network is Internet access. The NAT server creates an access to the internet for the entire network, and the NAT server is Linux based with Ubuntu 10.04.

The topology of this network is a star with 5 substructures, which could have different topologies; however, all components of every substructure enjoy the same effective features; therefore, we can assume that every attack occurs in the whole of a sub-network with equal probability

The attack scenario is required to employ a description language that contains various attacks. In [7], for describing an attack scenario, ADeLe [4] was used; the full attack scenario was composed of 5 steps:

1. Information gathering and reconnaissance (passive and active),
2. Vulnerability identification and scanning,
3. Gaining access and compromising a system,
4. Maintaining access and creating backdoors,
5. Covering tracks.

The network analysis started at 00:01:06 on Friday June 11th and ran continuously for an exact duration of 7 days, ending on June 18th. See [13] to get the details and attack distribution.

ISCX Network Reliability

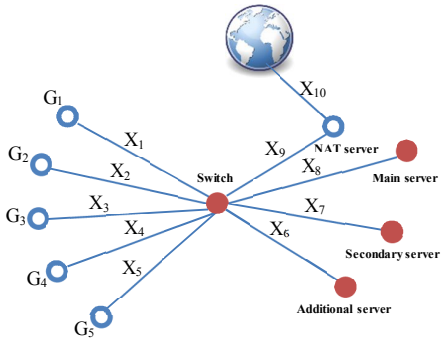

Fig. 1. The network graph

Assume that the network can be connected so long as the servers are working and, at least, one of them is connected; consequently, this is a $N=(V,E,T)$ where $|V|=11$, $|E|=10$, and $|T|=3$. Let $X_1, X_2, \ldots, X_{10}$ be the links' lifetimes that depend on attacks. As shown in Figure 1, the main devices (switch, servers) are shown by solid circles, and the X_6, X_7, X_8 are the main links.

Since each attack is followed by the attack scenario, every attack can break at most one link; therefore, signature vector in Definition 1 can be computed and Relation (1) is used to determine reliability function with this kind of scenario, where n_i, $i=1,\ldots,10$ is

Tab. 1. ISCX signature details

i	n_i	s_i
1	0	0
2	0	0
3	30240	0.008
4	90720	0.025
5	181440	0.050
6	302400	0.083
7	453600	0.125
8	635040	0.175
9	846720	0.233
10	1088640	0.300

From Table 1, $s=(0,0,0.008,0.025,0.050,0.083,0.125,0.175,0.233,0.3)$; therefore,

$$R_T(t)=\Pr[T>t]=\sum_{i=1}^{10} s_i \Pr[X_{i:10}>t].$$

In the real world, there are known attacks that can break more than one type of components. Hence, we can assume a new scenario in which every attack may result from the break of more than one component at the same time. n^* is the number of ways that the links disconnect in the network and n_i is the number of ways of the order of link breaks when $M=i$. Hence, we have

Tab. 2. ISCX t-signature details

i	n_i	s_i^τ
1	94,586	0.001
2	1,229,611	0.012
3	4,632,258	0.045
4	10,226,724	0.100
5	17,304,504	0.169
6	23,097,480	0.225
7	22,947,120	0.224
8	15,457,680	0.151
9	6,168,960	0.060
10	1,088,640	0.010

In addition, t-signature vector is $s^\tau=(0.001,0.012,0.045,0.1,0.169,0.225,0.224,0.151,0.06,0.01)$ where

$$n^* = \sum_{i=1}^{10} n_i = 102247563.$$

For $k = 0, 1, ...$, we get

$$\beta_{k,10}^* = \sum_{j=0}^{9} \bar{S}_j^{\tau} \Pr[\sum_{i=1}^{k} K_i = j].$$

where $\bar{S}^{\tau}$ is

Tab. 3. $\bar{S}^{\tau}$ for ISCX

i	0	1	2	3	4
$\bar{S}_i^{\tau}$	1.0	0.999	0.987	0.942	0.842
i	5	6	7	8	9
$\bar{S}_i^{\tau}$	0.672	0.446	0.2221	0.071	0.011

Thus, we can write

$$\beta_{k,10}^* = \frac{0.1\,q^k + 2.23q^{2k} + 4.93q^{3k}}{1-q^{10}} + \frac{-12.33q^{4k} + 1.15q^{5k} + 13.28q^{6k}}{1-q^{10}} + \frac{-11.90q^{7k} + 3.81q^{8k} - 0.21q^{9k} - 0.07q^{10k}}{1-q^{10}}.$$

In the following, it is assumed that the shocks appear as a NHPP. A counting process is named a NHPP if the reliability function of the k^{th} event is

$$\Pr[\xi(t) = k] = \frac{(\lambda t)^k}{k!} e^{-\lambda t}.$$

From Representation (4), the reliability function can be computed as follows:

$$\mathrm{R_T(t)} = \Pr[T > t] = \sum_{k=0}^{+\infty} \beta_{k,10}^* \Pr[\xi(t) = k]$$

$$= \sum_{k=0}^{+\infty} \beta_{k,10}^* \frac{(\lambda t)^k}{k!} . e^{-\lambda t}.$$

Various analysis types of the reliability function of the SICX network are given below in Figures 2, 3, and 4.

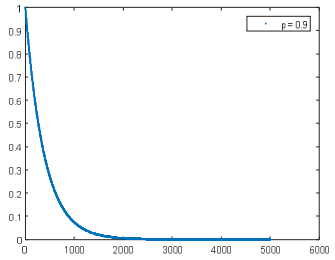

Fig. 2. The reliability function for p = 0.9 and λ=0.0271.

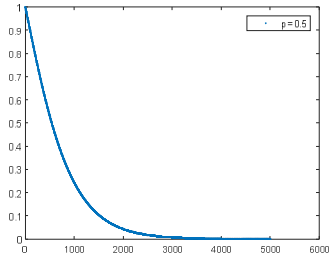

Fig. 3. The reliability function for p = 0.5 and λ=0.0271.

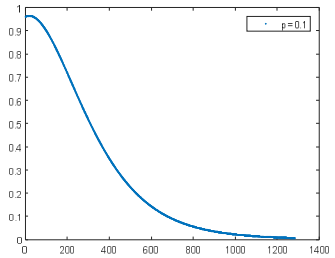

Fig. 4. The reliability function for p = 0.1 and λ=0.0271.

By (6), the MRL of a network can be described as follows:

$$M(t) = E(T - t | T \geq t)$$

$$= \frac{\sum_{k=0}^{+\infty} \beta_{k,10}^* \int_t^{+\infty} Pr[\xi(u) = k]\, du}{\sum_{j=0}^{+\infty} \beta_{j,10}^* Pr[\xi(t) = j]}$$

$$= \frac{\sum_{k=0}^{+\infty} \beta_{k,10}^* \int_t^{+\infty} \frac{(\lambda u)^k}{k!} . e^{-\lambda u}\, du}{\sum_{j=0}^{+\infty} \beta_{j,10}^* \frac{(\lambda t)^j}{j!} . e^{-\lambda t}}$$

$$= \frac{\sum_{k=0}^{+\infty} \beta_{k,10}^* \sum_{s=0}^{k} \frac{t^{k-s}\, \lambda^{(k-s)-1}}{(k-s)!}}{\sum_{j=0}^{+\infty} \beta_{j,10}^* \frac{(\lambda t)^j}{j!}}.$$

Further, analysis of the network's MRL for some values of p during time t outputs is shown in Figures 5, 6, and 7.

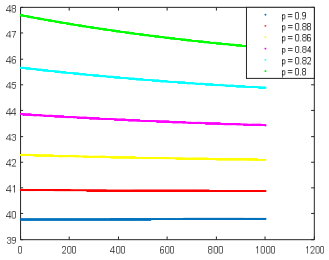

Fig. 5. The network's MRL for p = 0.9(blue), p = 0.88(red), p = 0.86(yellow), p = 0.84(pink), p = 0.82(azure), p = 0.8(green), and λ=0.0271.

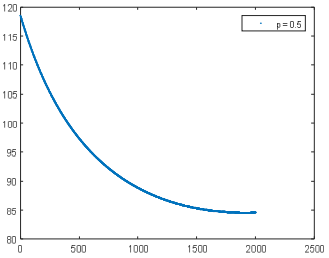

Fig. 6. The network's MRL for p = 0.5 and λ=0.0271.

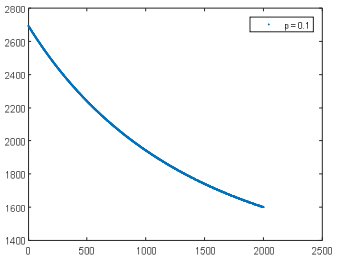

Fig. 7. The network's MRL for p = 0.1 and λ=0.0271.

Remark: The hazard rate of a continuous random variable T with density function f and distribution function F with f is defined by

$$h(t) = \lim_{\delta t \to 0} \frac{\Pr[T > t + \delta t \mid T \geq t]}{\delta t} = \frac{f(t)}{R(t)}.$$

The hazard rate of the network can be written as follows:

$$h_T(t) = \sum_{k=1}^{+\infty} p_{k,n}(t) h s_k(t), \qquad (10)$$

where $h_k(t) = \frac{(\Pr[\vartheta_k > t])'}{\Pr[\vartheta_k > t]}$ is the hazard rate of ϑ_k , $b_{k,n} = \beta_{k-1,n} - \beta_{k,n}$ and

$$p_{k,n}(t) = \frac{b_{k,n} \Pr[\vartheta_k > t]}{\sum_{j=1}^{+\infty} b_{j,n} \Pr[\vartheta_j > t]} .$$

Hence, from (10), we obtain

$$h_T(t) = \sum_{k=1}^{+\infty} p_{k,10}(t) h_k(t),$$

and

$$p_{k,10}(t) = \frac{b_{k,10} \Pr[\vartheta_k > t]}{\sum_{j=1}^{+\infty} b_{j,10} \Pr[\vartheta_j > t]}.$$

Acknowledgments
The authors would like to express our sincere thanks to Professor Ali Fanian, computer group at the Isfahan University of Technology, and ISCX research group for the helpful comments and providing data support, and the Isfahan University of Technology where the study was carried out.

References

[1] Annual Security Report of CISCO. www.cisco.com, (2014-2015).

[2] Gertsbakh, I. and Y. Shpungin: *Network Reliability and Resilience*. Berlin, Germany, Springer, (2011).

[3] Gertsbakh, I. and Y. Shpungin: *Models of Network Reliability: Analysis, Combinatorics, and Monte Carlo*. CRC press, (2009).

[4] Michel, C. and L. Mé: Adele: An Attack Description Language for Knowledge-Based Intrusion Detection. *In Trusted Information*, (2002), pp. 353-68.

[5] Navarro, J. and N. Balakrishnan, and F. Samaniego: Mixture Representations of Residual Lifetimes of Used Systems. *Journal of Applied Probability*, (2008), pp. 1097-1102.

[6] Samaniego, F. J.: *System Signatures and Their Applications in Reliability Engineering*. New York, NY, USA, Springer, (2007).

[7] Shiravi, A., H. Shiravi, M. Tavallaee, and A. Ghorbani: Toward Developing a Systematic Approach to Generate

Benchmark Datasets for Intrusion Detection. *Computers & Security*, Vol. 31, No. 3, (2012), pp. 74-357.

[8] Spizzichino, F. and J. Navarro: Signatures and Symmetry Properties of Coherent Systems. *In Recent Advances in System Reliability*, (2012), pp. 33-48.

[9] Triantafyllou, I. S. and M. V. Koutras: On the Signature of Coherent Systems and Applications. *Probability in the Engineering and Informational Sciences*, Vol. 22, No. 1, (2008), pp. 19-35.

[10] Zarezadeh, S. , S. Ashrafi, and M. Asadi: A Shock Model Based Approach to Network Reliability. *IEEE Transactions on Reliability*, Vol. 65, No. 2, (2016), pp. 992-1000.

[11] Zarezadeh, S. and M. Asadi: Network Reliability Modeling under Stochastic Process of Component Failures. *IEEE Transactions on Reliability*, Vol. 62, No. 4, (2013), pp. 917-922.

[12] Zarezadeh, S., M. Asadi, and N. Balakrishnan: Dynamic Network Reliability Modeling under Nonhomogeneous Poisson Processes. *European Journal of Operational Research*, Vol. 232, No. 3 , (2014), pp. 561-571.

[13] www.unb.ca/research/iscx/dataset/iscx-IDS-dataset-.html.