ACSIJ Advances in Computer Science: an International Journal, Vol. 3, Issue 1, No.7 , January 2014
ISSN : 2322-5157
www.ACSIJ.org

ACSIJ
WWW.ACSIJ.ORG

Determining Threshold Value and Sharing Secret Updating Period in MANET

Maryam Zarezadeh[1], Mohammad Ali Doostari[2] and Hamid Haj Seyyed Javadi[3]

[1] Computer Engineering, Shahed University
Tehran, Iran
m.zarezadeh@shahed.ac.ir

[2] Computer Engineering, Shahed University
Tehran, Iran
doostari@shahed.ac.ir

[3] Mathematics and Computer Science, Shahed University
Tehran, Iran
h.s.javadi@shahed.ac.ir

Abstract

In this paper, an attack model is proposed to implement safe and efficient distributed certificate authority (CA) using secret sharing method in mobile ad hoc networks (MANETs). We assume that the attack process is based on a nonhomogeneous Poisson process. The proposed model is evaluated and an appropriate amount of threshold and updating period of sharing secret is suggested. In addition, threshold value effect on security of the network which uses the distributed CA is investigated. The results may be also useful in security improvement of networks that apply secret sharing scheme.

Keywords: *Ad Hoc Network, Nonhomogeneous Poisson Process, Certificate Authority, Public Key Infrastructure.*

1. Introduction

Public key infrastructure (PKI) is a basic and fundamental infrastructure for implementation of security services such as key generation and distribution in mobile ad hoc networks (MANETs). In conventional PKI, the centralized certificate authority (CA) is responsible for the distribution and management of public key certificate used for assigning public key to relevant user. But implementation of PKI in MANET faces several obstacles. Including in PKI, the conventional single-CA architecture suffers from single point of failure problem. Furthermore, due to the dynamic topology and mobile nature of nodes, setting a node as CA may cause a lot of communication overhead. The distributed CA method has been suggested for solving single point of failure problem [1]. In this method, using threshold secret sharing scheme, functionality of CA is distributed among several nodes. Then, for providing CA services, t nodes as CA servers cooperate, which t is called the threshold parameter of a secret sharing scheme. Therefore, the attacker cannot identify the secret key of CA until it detects the number of sharing secret less than t. Also, to cope with the efforts of attackers to know the secret value periodically update the shared secret is suggested.

Secret sharing method has many applications in key management. Li et al. [2] suggested new distributed key management scheme by combination of certificateless public key cryptography and threshold cryptography. In this scheme, for sharing master key of the network, n out of N nodes are chosen as shareholders. Zhu et al. [3], using threshold cryptography (n, t), presented mobile agent to exchange topology information and private key. When a new node requests to connect to network with size n, t nodes cooperate and authentication is done. This method can reduce network overhead and can improve the success rate of authentication. Zefreh et al. [4] proposed a distributed CA system based on secret sharing scheme. They have assumed that the network is divided into several clusters and each cluster head is in role of distributed CA. So, a valid certificate is produced by a quorum of cluster heads. Ge et al. [5] suggested the certificate authority based on the group of distributed server nodes. In this model, it is considered different types of nodes jointed to network and MANET is subject to frequent partitioning duo to dynamic nature of topology. Hence they classify nodes to three types: servers, high-end clients and low-end clients. In requesting procedure, high-end and low-end clients obtain a valid certification. They sent request to proxy server and proxy server forwards this request to other servers. If at least t servers exist in group server to combine at least t partial certificates, certificate is issued.

The aim of group key distribution protocol is to distribute a key used for encrypting the data. Therefore, based on generalized Chinese remainder theorem, Guo and Change [6] suggested a group key distribution built on the secret sharing scheme. Their protocol requires few computation operations while maintain at least security degree. Liu et al. [7] proposed similar group key distribution protocol. They

indicated Guo and Chang ' s protocol [6] have some security problems and suggested simpler protocol that confidentiality of group key is secure unconditionally. In registration phase, key generation center (KGC) shares a secret with each group member. Then, KGC establishes the session key of group using threshold secret sharing method and Chinese remainder theorem. Each group member use her/his secret shared with the KGC to recover the group key. Also, Gan et al. [8] proposed a threshold public key encryption scheme. In this scheme, on the base of dual pairing vector space and bilinear group, the decryption key is distributed between n nodes. For decrypting the cipher text, it is sent to t or more than t nodes and the plain text is obtained, t is the threshold value. For more researches on applications of secret sharing scheme in ad hoc networks, one can see [9-11].

As can be seen in aforementioned research works, many studies showed the role of secret sharing scheme in security of MANET. Then, determination of threshold value and updating period of sharing secret is important. However, few studies have focused on this issue. Dong et al. [12] have compared security of the partially and fully distributed CA based on the number of server nodes. But they did not show how to determine the threshold value. Haibing and Changlun [13] have suggested an attack model to determine threshold value and updating period of sharing secret.

The aim of the present paper is to determine the sufficient threshold value and sharing secret updating period to use effectively secret sharing scheme in MANETs. For this purpose, we propose an attack model by considering the attack process as a nonhomogeneous Poisson process (NHPP). The paper is organized as follows. Attacks on MANET and secret sharing scheme are studied in Section 2. Attack process is explored in Section 3. First, some researches on the attack processes in MANETs are discussed. Then, in the sequel, the suggested attack model in this paper is described and a sufficient amount for threshold and updating period of sharing secret is specified. In Section 4, the effect of threshold on security of distributed CA scheme is evaluated. The paper is concluded in Section 5.

2. Attacks

In this section, we review the attacks on MANET and secret sharing scheme.

2.1 Attacks on MANET

Many attacks in MANET have been investigated by researchers. According to [14], attacks on MANET can be classified as follows:

Passive/active: A passive attacker takes an action such as traffic eavesdropping for information gathering. But in this attack, no interference is occurred in network host performance. In active attack, adversary interferes through actions e.g. modulating, packet forwarding, injecting or replaying packets, and so on.

Insider/outsider: This is potentially serious security risk in all security application domains and adversary can cause with insider capability. Some researchers have suggested threshold protocols (e.g. m-out-of-n voting protocols) for resolving this problem in field of secret sharing and aggregating application protocols.

Static/adaptive: Setting a learning algorithm in each node can be considered as static. From a practical point of view, the network's ability to respond to environment, increases significantly attacker power. For example, make an informed selection as to which node to compromise next improves attack performance.

2.2. Attacks on secret sharing scheme in MANET

Since secret is shared between several users and each user can get only a single secret key, it is difficult to Brute-Force attack. It becomes more harder for the adversary to guess all the values of threshold t because value of t being variable for different partitions. But there is a chance of Brute-Force attack by obtaining partial information from a shared secret. A malicious user with help of his share of secret can get another shared secret. When the number of nodes that is compromised is more than or equal to threshold, the malicious node can reconstruct secret key. In other words security of the network has been failed; see [15]. Yi and Kravets [16] studied the following two active attacks on a distributed PKI:

(i) Routing Layer Attacks - Malicious nodes disrupt routing by announcing false routing information such as injecting incorrect routing packets or dropping packets. If the attacker blocks or reroutes all victim's packets, some routing layer attacks can be used to establish a denial-of-service (DOS) attack.

(ii) Directed Attacks on CA nodes - Once an attacker discovers identity or location of CA nodes may employ its resource in attacking only the CA nodes.

3. Proposed attack model

In this section, first, some researches on the attack processes in MANET are discussed. Then, the suggested attack model in this paper is described and a sufficient amount for threshold and updating period of sharing secret is specified.

Some researchers have studied and modeled the attack process. Jonsson and Olovsson [17] targeted a distributed computer system which consisted of a set of 24 SUN ELC diskless workstations connected to one file server. In

intrusion test is assumed that all attackers are system legal users with normal user privileges and physical access to all workstations except file server. They considered intrusion process into three phases: learning phase, standard attack and innovative attack phases. Many of data related to standard attack phase and statistical evidence showed the intrusion process could be described by an exponential distribution.

Kaaniche et al. [18] collected data from the honeypot platforms which deployed on the Internet. Then they did empirical analysis and statistical modeling of attack processes. Results showed the probability distribution corresponding to time between the occurrence of two consecutive attacks at a given platform can be described by a mixture distribution combining a Pareto distribution and an exponential distribution. The probability density function $g(t)$, is defined as follows:

$$g(t) = p_w \lambda e^{-\lambda t} + (1 - p_w)\frac{k}{(t+1)^{k+1}}, \quad t > 0 \qquad (1)$$

It should be noted that p_w is a probability, λ is the scale parameter of the exponential distribution and k is the shape parameter of the Pareto distribution.

It was found that the amount of p_w in (1) varies from 0.9885 to 0.9981 in all the platforms of honeypot; see [13]. Because p_w is the weight of exponential distribution in mixture distribution, Haibing and Changlun [13] concluded that the exponential distribution dominates mixture distribution. Also, these authors proposed an attack model based on Poisson process to determine threshold value and updating period of sharing secret. In the suggested model, since the attacks appear according to a Poisson process then the attacks occur at random instants of time with an average rate of λ attacks per second. Limitation of Poisson process to approximate the attack process is that its rate is constant and does not vary over time. On the other hand, it is well known that the security of MANETs is poor. In other words, the wireless communication medium is accessible to any entity with adequate resources and appropriate equipment. Hence, access to the channel cannot be restricted. According, attackers are able to eavesdrop on communication and inject bogus information [19]. This means that over time, node is more vulnerable to compromise and attack. So, by considering the rate of attack process as a function of time, modeling is closer to reality. Based on this, we suggest a new attack model in which this assumption is also considered. To describe the model, we need to present the following definition definition.

Definition: Let $N(t)$ be a non-negative random variable representing the number of events in the interval $[0, t)$. Then $N(t)$, $t \geq 0$ is called a counting process. The Poisson process model is a well known counting process model. A counting process is a Poisson process if for some small value *h* and all times *t*

(i) $N(0) = 0$.
(ii) Non-overlapping increments are independent
(iii) $P(N(t+h) - N(t) = 1) = \lambda h + o(h)$.
(iv) $P(N(t+h) - N(t) > 1) = o(h)$.

where, in little o notation, $\frac{o(h)}{h} = 0$ when $h \to 0$ Interarrival times of Poissson process have exponential distribution with rate λ and hence it is said this process has no memory. This means that $\{N(t), t \geq 0\}$ is Poisson process with mean $\Lambda(t) = \lambda t$ where $\Lambda(t) = E(N(t))$ is called the mean value function (m.v.f.). NHPP is a generalization of Poisson process with conditions (i)-(iv) except for that the rate is a function of t denoted by $\lambda(t)$, and is called intensity function. The m.v.f of the NHPP is written as $\Lambda(t) = \int_0^t \lambda(t')dt' = -\log(1 - F(t))$, where $F(t)$ is the distribution function of the time of the first event in the process. See [20] for a good review of stochastic processes.

We consider MANET as a closed system. When a network is based on threshold secret sharing scheme, a group of nodes have the pieces of secret. Then, for modeling of attacks, the inside attacks are only considered. Usually in such attacks, malicious nodes drop and refuse to forward request of generation or updating certificate, return a fake reply (e.g. an invalid partial certificate).

Let $\{N(t);\ t \geq 0\}$ be a counting process in which $N(t)$ denotes the number of attacks happened in the interval $[0, t)$. Thus $N(t) = 0$ means that no attack has occurred in the network up to time t Also, it implies that $N(t) - N(t_0) = N(t, t_0)$, $0 \leq t_0 \leq t$ denotes the number of attacks in interval $[0, t)$ .The probability that the network receives m attacks in interval $[0, t)$ is denoted by:

$$P_m(t_0, t) = P\{N(t_0, t) = m\}, \quad m = 0,1,2, \ldots \qquad (2)$$

According to our analysis $\{N(t);\ t \geq 0\}$ can be estimated by NHPP with m.v.f. $\Lambda(t)$. Then, the probability that m attacks appear during $[t_0, t)$ is obtained as

$$P_m(t_0, t) = \frac{[\Lambda(t - t_0)]^m}{m!} e^{-\Lambda(t - t_0)}, \quad t > t_0, \qquad m = 1, 2, .. \quad (3)$$

Particularly, if attacks in the time interval $[0, t)$ is considered, we can write

$$P_m(0, t) = \frac{[\Lambda(t)]^m}{m!} e^{-\Lambda(t)}, \quad t > 0, \qquad m = 0,1,2, \ldots \quad (4)$$

Due to network protection, all attackers cannot successfully compromise nodes. We assume that any node at each attack may be compromised with probability p. In the following, we calculate the probability distribution of the successful attack process.

Rule 1: Let $\{N(t);\ t \geq 0\}$ be a NHPP with m.v.f. $\Lambda(t)$ in which $N(t)$ denotes the number of attacks happened in the interval $[0, t)$. Assume the probability that the attackers compromise successfully a node at each attack is p and

hence the unsuccessful probability is $1-p$. Suppose that $\xi(t)$ is a random variable denoting the number of nodes that attackers compromise successfully in the interval $[0,t)$. Then $\{\xi(t); t \geq 0\}$ is a NHPP with m.v.f. $p\Lambda(t)$ and hence the probability that k nodes are compromised in the interval $[0,t)$ is

$$P_k(t) = P(\xi(t) = k) = \frac{[p\Lambda(t)]^k}{k!} e^{-p\Lambda(t)}, \qquad k = 0,1,.. \quad (5)$$

Hence $P_k(0) = 0$ for all $k = 0,1,..$, which means that no attack is happened at time $t = 0$ and the network is secure. The next rule provides the time of maximum compromise probability.

Rule 2: Consider the assumptions of Rule 1. Further, suppose that $\Lambda(t) = -\log(1 - F(t))$ in which $F(t)$ denotes the distribution function of the time to the first attack in the network. The probability that k nodes in the network have been compromised successfully reaches maximum at time t where

$$t = F^{-1}\left(1 - e^{-\frac{k}{p}}\right) \qquad (6)$$

Proof: Differentiating from equation (5), we can obtain the peak time as follows:

$$P_k'(t) = \frac{e^{-p\Lambda(t)}}{k!} p^k \Lambda(t)^{k-1} \lambda(t)\left(k - p\Lambda(t)\right)$$

Letting $P_k'(t) = 0$, the unique maximum value of equation (5) is obtained at time $t = F^{-1}\left(1 - e^{-\frac{k}{p}}\right)$.

Rule 3: Equation (6) will help us to determine the updating period T of sharing secret. Equation (6) states that when the system is under risk. According to equation (6) at time t attack to k nodes as shared secret holders reaches maximum. In this condition to maintain system security and prevent of disclosure of shred confidential should be secret value is updated in $T < t$.

Rule 4: From (6), it can be concluded that the threshold value of sharing secret, denoted by τ. From equation (6), $k = -p\ln(1 - F(t))$ is obtained. As mentioned until attacker compromise less than k nodes, cannot discover sharing secret. Therefore, for given attack stream and p, τ should be greater than k and we can write

$$\tau > k = -p\ln(1 - F(t) + 1 \qquad (7)$$

4. Evaluation of proposed model

In this section, we will discuss the influence of threshold value τ on the security performance of the distributed CA scheme based on the proposed model. An attacker which wants to attack the network must compromise no less than τ nodes to recover the sharing secret. The probability of compromising less than τ nodes in time interval $[0,t)$ is called the security of the network and is obtained, as follows

$$P_{sec} = P(\xi(t) < k) = \sum_{k=1}^{\tau-1} \frac{[p\Lambda(t)]^k}{k!} e^{-p\Lambda(t)} = \frac{\Gamma(\tau; p\Lambda(t))}{\Gamma(\tau)}, \qquad (8)$$

where $\Gamma(m;u) = \int_u^\infty x^{m-1}e^{-x}\,dx$ is the incomplete gamma function.

Representation (8) shows that the probability of network security does not depend on the number of nodes. Then, using P_{sec}, cannot be compared the security of partial with full distributed CA schemes.

Also, it can be seen that P_{sec} is increasing in τ and is decreasing in t and p, separately. Thus, if we select nodes that are less vulnerable to attacker compromise as nodes holding the pieces of shared secret in partial distributed scheme, the security of network is improved.

Using equations (5) and (6), it can be seen that

$$P_k(t) = \frac{k^k}{k!} e^{-k} \qquad (9)$$

That is, the maximum value of $P_k(t)$ depends only on k and is independent of m.v.f. and p, which is shown in figure 1 and figure 2. Figure 1 depicts the 3D plot of $P_5(t)$ in which $\Lambda(t) = t^2$. This plot shows the independency of maximum value of $P_5(t)$ from p.

Also, figure 2 draws $P_5(t)$ for $p = 0.2$ and m.v.f. $\Lambda(t) = t, t^2, 5t + 2t^2$. As we can see, the maximum value of $P_5(t)$ is independent of m.v.f.

.

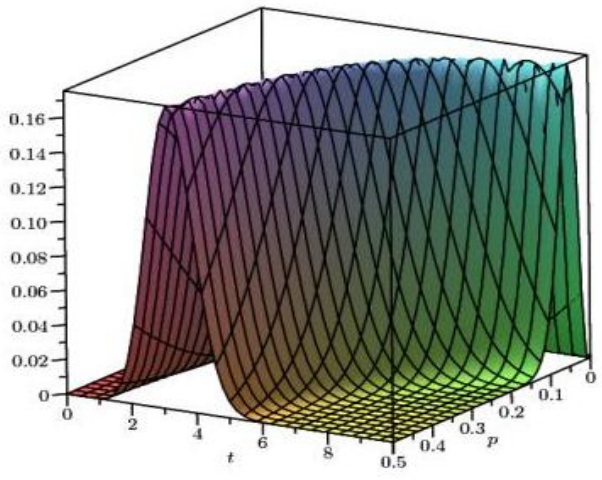

Fig. 1. The 3D plot $P_5(t)$ for $\Lambda(t) = t^2$.

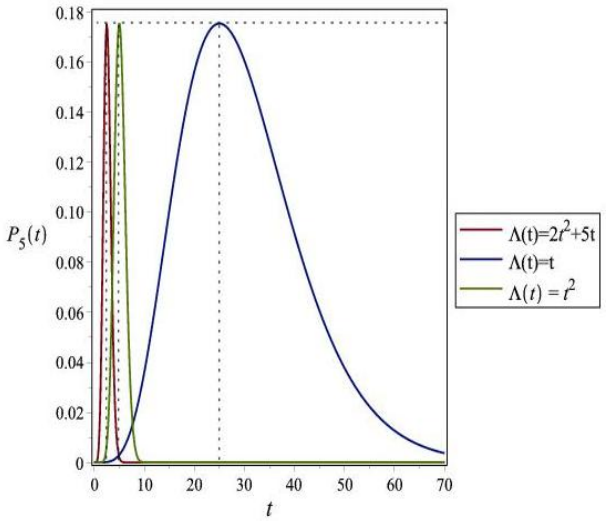

Fig. 2. The plot $P_5(t)$ for $\Lambda(t) = t, t^2, 5t + 2t^2$.

According to equation (9), the maximum value of $P_k(t)$ is decreasing in *k* and is shown in figure 3. In other words, increasing the number of secret holders, success of malicious node to obtain secret value decreases. So, attacker requires to further efforts in fully distributed CA in compared to the partially distributed CA that all nodes have a part of secret.

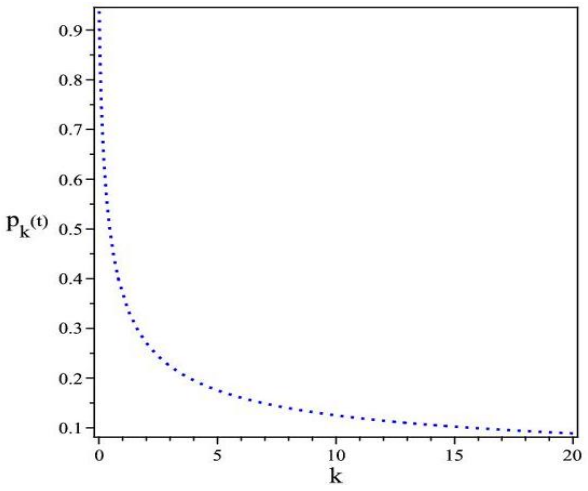

Fig. 3. Relationship between $P_k(t)$ and k.

5. Conclusion

In this paper, we have presented an attack model to determine the proper value of threshold and updating period of sharing secret for efficient implementation of distributed CA based on threshold secret sharing scheme in MANETs. In the proposed model, attack process has been estimated by NHPP. By considering the attack process as NHPP, the rate of the attack is not necessary fixed in time as Poisson process and can vary over time. The results of evaluating of suggested model have shown that the probability of network security is independent of the nodes number. Therefore, it cannot be compared the security of fully distributed and partially distributed CA schemes using the number of nodes.
According to our analysis, the maximum of probability that an attacker compromises the nodes of the network depends only on the number of nodes and is independent of the m.v.f. This means that if attack process is adopted based on NHPP, we have a unique maximum for any m.v.f. Also, the results of network security probability have shown this probability decreases when the probability that the attackers successfully compromise a node increases. Then, the nodes that have less risk of exposure and vulnerability have been selected as a part of the sharing secret holder in a partially distributed CA scheme and hence the security of MANETs can be improved.

References

[1] L. Zhou and Z. J. Haas, "Securing ad hoc networks", Network, IEEE, vol. 13, pp. 24-30, 1999.
[2] L. Liu, Z. Wang, W. Liu and Y. Wang, "A Certificateless key management scheme in mobile ad hoc networks", 7th International Conference on Wireless Communications, Networking and Mobile Computing, IEEE 2011, 1-4.
[3] L. Zhu, Y. Zhang, and L. Feng, "Distributed Key Management in Ad hoc Network based on Mobile Agent", in Intelligent Information Technology Application, 2008. IITA'08. Second International Symposium on, 2008, pp. 600-604.
[4] M. S. Zefreh, A. Fanian, S. M. Sajadieh, M. Berenjkoub, and P. Khadivi, "A distributed certificate authority and key establishment protocol for mobile ad hoc networks", in Advanced Communication Technology, 2008. ICACT 2008. 10th International Conference on, 2008, pp. 1157-1162.
[5] M. Ge, K.-Y. Lam, D. Gollmann, S. L. Chung, C. C. Chang, and J.-B. Li, "A robust certification service for highly dynamic MANET in emergency tasks", International Journal of Communication Systems, vol. 22, pp. 1177-1197, 2009.
[6] C. Guo and C. C. Chang, "An authenticated group key distribution protocol based on the generalized Chinese remainder theorem", International Journal of Communication Systems, 2012.
[7] Y. Liu, L. Harn, and C.-C. Chang, "An authenticated group key distribution mechanism using theory of numbers", International Journal of Communication Systems, 2013.
[8] Y. Gan, L. Wang, L. Wang, P. Pan, and Y. Yang, "Efficient threshold public key encryption with full security based on dual pairing vector spaces", International Journal of Communication Systems, 2013.
[9] S. Yi and R. Kravets, "Key management for heterogeneous ad hoc wireless networks", in Network Protocols, 2002. Proceedings. 10th IEEE International Conference on, 2002, pp. 202-203.

[10] J. Zhang and Y. Xu, "Privacy-preserving authentication protocols with efficient verification in VANETs", International Journal of Communication Systems, 2013.
[11] A. A. Moamen, H. S. Hamza, and I. A. Saroit, "Secure multicast routing protocols in mobile ad-hoc networks", International Journal of Communication Systems, 2013.
[12]Y. Dong, A.-F. Sui, S.-M. Yiu, V. O. K. Li, and L. C. K. Hui, "Providing distributed certificate authority service in cluster-based mobile ad hoc networks", Computer Communications, vol. 30, pp. 2442-2452, 2007.
[13] M. Haibing and Z. Changlun, "Security evaluation model for threshold cryptography applications in MANET", in Computer Engineering and Technology (ICCET), 2010 2nd International Conference on, pp. V4-209-V4-213.
[14] J. A. Clark, J. Murdoch, J. McDermid, S. Sen, H. Chivers, O. Worthington, and P. Rohatgi, "Threat modelling for mobile ad hoc and sensor networks", in Annual Conference of ITA, 2007, pp. 25-27.
[15] P. Choudhury, A. Banerjee, V. Satyanarayana, and G. Ghosh, "VSPACE: A New Secret Sharing Scheme Using Vector Space", in Computer Networks and Information Technologies: Springer, 2011, pp. 492-497.
[16] S. Yi and R. Kravets, "MOCA: Mobile certificate authority for wireless ad hoc networks", in 2nd Annual PKI Research Workshop Program (PKI 03), Gaithersburg, Maryland, 2003, pp. 3-8.
[17] E. Jonsson and T. Olovsson, "A quantitative model of the security intrusion process based on attacker behavior", Software Engineering, IEEE Transactions on, vol. 23, pp. 235-245, 1997.
[18] M. Kaaniche, Y. Deswarte, E. Alata, M. Dacier, and V. Nicomette, "Empirical analysis and statistical modeling of attack processes based on honeypots", International Conference on Dependable Systems and Networks, IEEE 2006; Philadelphia. USA.
[19] J. V. D. Merwe, D. Dawoud, and S. McDonald, "A survey on peer-to-peer key management for mobile ad hoc networks", ACM computing surveys (CSUR), vol. 39, p. 1, 2007.
[20] S. Ross, "Stochastic processes", 2nd edn, New York: Wiley, 2008.