ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 8, Issue 6, November 2019

Applications of probability in security enhancement

B. Kumara Swamy Achary, V.Vasu
Dept. of Mathematics, S.V. University, Tirupati

Abstract: ***In this paper, we studied probability and also we studied the definition of perfect security and also conditional probability. In this connection, we proved some theorems and some Inequalities.***

Key words: **Probability, Baye's theorem, Perfect Security, Markov, Chebyschev and Hoefding Inequalities.**

I. INTRODUCTION

Definition 1:

If E_1 and E_2 are two events in a sample space S $P(E_1) \neq 0$ then the probability of E_2, after the event E_1 has occurred, is called the conditional probability of the event of E_2 given [3]

E1 and is denoted by $P\left(\frac{E_2}{E_1}\right)$ *or* $P(E_2/E_1)$ and we define

$P\left(\frac{E_2}{E_1}\right) = \frac{P(E_1 \cap E_2)}{P(E_1)}$ Similarly we define $P\left(\frac{E_2}{E_1}\right) = \frac{P(E_1 \cap E_2)}{P(E_2)}$

We have $P\left(\frac{E_2}{E_1}\right) = \frac{P(E_1 \cap E_2)}{P(E_1)} = \frac{n(E_1 \cap E_2)}{n(E_1)/n(S)} = \frac{n(E_1 \cap E_2)}{n(E_1)}$

$= \frac{Number\ of\ elemetns\ in\ E_1 \cap E_2}{Number\ of\ elements\ in\ E_1}$

Here $E_1 \subset S\ and\ P(E_1) > 0.$

Multiplication Theorem of Probability Statement

In a random experiment if E_1, E_2 are two events such that $P(E_1) \neq 0$ and $P(E_2) \neq 0, then$

$P(E_1 \cap E_2) = P(E_1).P(E_2/E_1)$

$P(E_2 \cap E_1) = P(E_2).P(E_1/E_2)$

Pair wise Independent Events

E_1, E_2, E_3 are events of a sample space S. They are said to be pair wise independent if

$P(E_1 \cap E_2) = P(E_1).P(E_2).P(E_2 \cap E_3) = P(E_2).P(E_3)$

$P(E_1 \cap E_3) = P(E_1).P(E_3)\ when\ P(E_1) \neq 0, P(E_3) \neq 0$

Let E_1, E_2, E_3, be three events of a sample space. It is possible to have E_1 and E_2 independent, E_1 and E_3 independent, and E_2 and E_3 independent and still to have $E_1 \cap E_2$ and E_3, say, dependent or to have E_1, E_2 and E_3 dependent. That is, it is possible for three events E_1, E2 and E_3 dependent. That is, it is possible for three events E_1, E_2, E_3 to be pair wise independent and not be mutually independent.

Baye's Theorem Statement

E_1, E_2… E_n are n mutually exclusive and exhaustive events such that $P(E_i)>0$ (i=1,2,…n) in a simple space S and A is any other event in S intersecting with every Ei (i.e. A can only occur in combination with any one of the events (E_1,E_2,…E_n) such that P(A)>0.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 8, Issue 6, November 2019

If E_1 is any of the events of $E_1,E_2 \ldots E_n$ where $P(E_1)$, $P(E_2) \ldots P(E_n)$ and $P(A/E_1)$, $P(A/E_2) \ldots P(A/E_n)$ are known then

$$P(E_K / A) = \frac{P(E_K).P(A/E_K)}{P(E_1).P(A/E_1)+P(E_2).P(A/E_2)+....+P(E_n).P(A/E_n)}$$

Example 1:

If we toss a coin there times, we either obtained Head (H) to Tails (T). the sample space S={HHH, HHT,HTH, THH, HTT, THT, TTH, TTT}

Example 2:

If we through die two times, we obtain a number in {1,2,3,4,5,6} the sample space s contains S={(1,1), (1,2),(1,3), (1,4), (1,5), (1,6), (2,1), (2,2),(2,3), (2,4), (2,5), (2,6), (3,1), (3,2),(3,3), (3,4), (3,5), (3,6), (4,1), (4,2),(4,3), (4,4), (4,5), (4,6), (5,1), (5,2),(5,3), (5,4), (5,5), (5,6), (6,1), (6,2),(6,3), (6,4), (6,5), (6,6)}

Example 3:

The probability distribution throwing two dice which maps each elementary event 1/36. The probability of event obtained sum of two dice is even number i.e. Pr(2),Pr(4),Pr(6), Pr(8), Pr(10), Pr(12),Pr(2)=1/36, Pr(6)=3/36=1/12, Pr(6)=5/36=1. Therefore Pr(2)+Pr(4)+Pr(6)+Pr(8)+Pr(10)+Pr(12)=

$$= \frac{1}{36}+\frac{3}{36}+\frac{5}{36}+\frac{5}{36}+\frac{3}{36}+\frac{1}{36}=\frac{18}{36}=\frac{1}{2}$$ Similarly we calculate sum of odd number obtained when two dice are thrown i.e. Pr(3)+Pr(5)+Pr(7)+Pr(9)+Pr(11)/=

$$= \frac{2}{36}+\frac{4}{36}+\frac{6}{36}+\frac{4}{36}+\frac{2}{32}=\frac{18}{36}=\frac{1}{2}$$ Therefore sum of even numbers getting = Pr (sum of odd numbers getting) when two dice are thrown.

Application of Baye's formula:

Let x and y be random variables and assume that fy(y)>0 then,

$$f_{x/y}(x/y) = \frac{f_x(x)\, f_{y/x}(y/x)}{f_y(y)}$$

In particular x and y are independent $f_{x/y}(x/y)=f_x(x)$ $\forall$ x&y

In this example we use Baye's formula to explore the independence of pairs of random variables taken from a triple (x,y,z). Let x and y be independent random variables taking on values +1 and -1 with probability ½ each and let Z=xy then Z also takes on the values +1 and -1 and we have

$$f_z(1) = \sum_{x\in(-1,+1)} \sum_{y\in(-1,+1)} \Pr(z=1/X=x \,and\, Y=y).f_{xy}(xy) \qquad (5)$$

If (x,y)=(+,-1) or (x,y)=(-1,+1) then z≠1, so only the two terms with (x,y)=(1,1) and (x,y)=(-1,-1) appear in the sum (5). For these two terms, we have Pr(z=1/x=x and y=y)

$$f_z(1) = \Pr(x=1 and\ y=1)+\Pr(X=-1 and\, Y=-1)$$

$$= \frac{1}{2}.\frac{1}{2}+\frac{1}{2}.\frac{1}{2}=\frac{1}{2}$$

It follows that $f_z(-1)=1-f_z(1)$ is also equal to $\frac{1}{2}$. Next we compute the joint probability density of z and X. For example

$$f_{z,x}(1,1) = \Pr(z=1 and\ X=1)$$

$$= \Pr(X=1 and\, Y=1)$$

$$= \frac{1}{4}$$ Since X and Y are independent.

$$= f_z(1)\, f_x(1)$$

Similar computations show that

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 8, Issue 6, November 2019

$$f_{z,x}(z,x) = f_z(z)\, f_x(x) \text{ for all } z,x \in \{-1,+1\}$$

So by theorem z and x are independent. The argument works equally well for z and y, so z and y are also independent. Thus among the three random variable independent. Thus among the three random variable x,y and z any pair of them are independent. Yet we would not want to call the three of them together an independent family since the value of z is determined by the values of x and y. The prompts the follows definition.

Perfect Secrecy

The cryptosystem has a finite plaintext space *P*, *a* finite cipher-text space *C*, and a finite key space *K*. The encryption functions are E_k, $k \in K$ *and the* decryption functions are D_k, $k \in K$,.

We assume that the probability of a plaintext *p is P(p)*[4]. The function P(p) is a probability distribution on the plaintext space. It depends, for example, on the language that is used. The distribution Pr also depends on the application context. For example, if first person is a factory manager, then it is likely that she frequently uses the word "worker". For the encryption of a new plaintext, first person chooses a new key which is independent of the plaintext to be encrypted i.e. . The probability for a key *k is* $\Pr_k(K)$. The function $\Pr_k$ is a probability distribution on the key space. The probability that a plaintext *p* occurs and is encrypted with key *k* is

$$\Pr(p,k) = P_p(p) P_k(p) \qquad (1)$$

This defines a probability distribution Pr on the sample space $P \in K$. We will now consider this sample space only. If p is a plaintext, then we also denote by *p the event {(p, k) : k ∈ K} that p* is encrypted. Clearly, we have

$$\Pr(P) = \Pr_p(P)$$

Also, for a key $k \in K$ we denote by *k the event {(p, k) : p ∈ P} that* the key *k* is chosen for encryption. Clearly, we have

$$\Pr(k) = \Pr_k(k)$$

By (1), the events *p and k* are independent. For a cipher text $c \in C$, we denote by *c the* event *{(p, k) : $E_k(p) = c$} that the* result of the encryption is *c*.

Definition 2:

The cryptosystem of this section *has perfect secrecy* if the events that a particular cipher text occurs and that a particular plaintext has been encrypted are independent (i.e., $\Pr(p|c) = \Pr(p)$ for all plaintexts *p and all* cipher texts c).

Example 4:

Let finite plain text space p={(HH), (TT), (HT), (TH)}, Pr(No head)= $\frac{1}{4}$, Pr (one Head)= $\frac{3}{4}$ Also let K={AB}Pr(A)= $\frac{1}{4}$, Pr(B)= $\frac{3}{4}$. Finally cipher text c={a,b} then the probability that plain text occurring no head and is encrypted with key A is Prob(0)* Prob (B)= $\frac{3}{4} \times \frac{3}{4} = \frac{9}{16}$. The encryption function Ek works as follows.

E_A(no head)=a , E_A(getting one head)=b, E_B(No head)=b, E_B(getting one head)=a,

The probability of cipher text a is Pr(a)=Pr(head A)+Pr(Head B)

$$\frac{1}{16} + \frac{9}{16} = \frac{10}{16} = \frac{5}{8}$$

The probability of cipher text b is Pr(b)=Pr(one head A)+Pr (None head B)

$$= \frac{3}{16} + \frac{3}{16} = \frac{6}{16} = \frac{3}{8}$$

Example 5:

Suppose that a cryptosystem has three keys K_1,K_2(x) four messages m_1,m_2,m_3 and m_4 four cipher text c_1,c_2,c_3 and c_4. Assume that the density function for the message random variable statistics.

$f_m(m_1)=f_m(m_2)=f_m(m_3)=1/4$ and $f_m(m_4)=1/2$ (3)

k_1	m_1	m_2	m_3	m_4

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 8, Issue 6, November 2019

k_2	c_2	c_1	c_3	c_4
k_3	c_1	c_3	c_2	c_4

Encryption of messages with keys K_1K_2 on K_3.

Theorem 1:

Let \P\ = \K\ = \C\< ∞ and Pr(p)> 0 for any plaintext p. Our cryptosystem has not perfect secrecy if and only if the probability distribution on the key space is either binomial or passion distribution and if for any plaintext p and any cipher text c there is more than one key k with $E_k(p) = c$.

Proof:

Suppose that the cryptosystem has perfect secrecy. Let p be a plaintext. If there is a cipher text c for which there is no key k with $E_k(p) = c$, then Pr(p)≠Pr(p/c)=0 since Pr(p)>0 by assumption. This contradicts the perfect secrecy. Hence, for any cipher text c there is a key k with $E_k(p) = c$. But the number of keys is equal to the number of cipher texts. Therefore, for each cipher text c there is exactly one key k with $E_k(p) = c$. This proves the second assertion.

To prove the first assertion, we fix a cipher text c. For a plaintext p, le k(p) be the uniquely determined key with $E_k(p) = c$. Then we have

K={k(p):p∈P}

Since the number of plaintexts is equal to the number of keys. Below we show that for all p∈P the probability of k(p) is equal to the probability of c. Then the probability of k(p) does not depend on p. Hence the probability of all k(p) is the same. Since by (2) every key k∈K is equal to k(p) for some p∈P, the probability distribution the key space is the uniform distribution.

Let p∈P as promised, we show that Pr(k(p))=Pr(c). It follows from theorem 3 that

$$P_r(p/c) = \frac{\Pr(c/p)\Pr(p)}{\Pr(c)} = \frac{\Pr K(p)\Pr(p)}{\Pr(c)}$$

Since the cryptosystem has perfect secrecy, we have Pr(P/c)=Pr(P) so (3) implies P(K(p)=Pr(c) as asserted.

Now we prove the converse. Assume that the probability distribution on the key space is the uniform distribution and that for any plaintext p and any cipher text c there is exactly one key k=k(p,c) with $E_k(p) = c$. Then

Now Pr(k(q,c)=1/|k| for all q∈P, c∈C. since all keys are equally probable. Hence,

$$\sum_{q\in P}\Pr(q)\Pr(k(q,c)) = \frac{\sum_{q\in P}\Pr(q)}{|K|} = \frac{1}{|K|}$$

If we use this equation in (3) then we obtain Pr(P/c)=Pr(P) as asserted.

II. STUDY OF MARKOV, CHEBYSCHEV AND HOEFDING INEQUA-LITIES

Markov Inequality:

Let *X* be a non-negative variable and v a real number. Then

$$\Pr[X \geq v]. \leq \frac{E(X)}{v}$$

Equivalently, $\Pr[X \geq r.E(X) \leq \frac{1}{r}$

Proof:

Let x be a continuous Random variable

$$E(x) = \int_{-\infty}^{\infty} f(x)dx$$

$$E(x) \geq \int_{-\infty}^{v} x\, f(x)dx * 0 + \int_{v}^{\infty} x\, f(x)dx.v$$

$$\geq p_r(x \geq x)V$$

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 8, Issue 6, November 2019

Chebyshev's Inequality:

Let X be a random variable, and $\delta > 0$. Then

$$\Pr[|X - E(X)| \geq \delta] \leq \frac{Var(X)}{\delta^2}$$

Proof:

Let x be a the continuous random variable

Then Mean $E(x) = \int_{-\infty}^{\infty} x.f(x)dx$

Variance $V(X) = E(X^2) - (E(X))^2$

$$E(X^2) = \int_{-\infty}^{\infty} x^2 f(x).dx$$

$$\therefore V(X) = \int_{-\infty}^{\infty} x^2 f(x).dx - \mu^2, where\ \mu = E(X)$$

And also $V(X) = P\left[(X - E(X))^2\right]$ ……..(1)

Now applying Markov inequality we get,

$$P\left[|X - E(X)| \geq \delta\right] = P\left[(X - E(X))^2 \geq \delta^2\right]$$ ……..(2)

Put eq. (1) in eq. (2) we get $P\left[|X - E(X)|\right] \geq = \frac{V(X)}{\delta^2}$

Hence the proof.

Theorem 2:

Let X_1, X_2……X_n be pair wise independent continuous random variables with same Mean and variance. Mean is denoted by μ. Variance is denoted by σ^2 .[6]

Then for every $\varepsilon > 0$,

$$P\left[\left|\frac{\int_{-\infty}^{\infty} X_i f(X_i)dx}{n} - \mu \geq \varepsilon\right|\right] \leq \frac{\sigma^2}{\varepsilon^2 n}$$

Proof:

Given X_1, X_2……..X_n are pair wise independent continuous random variables and each has zero expectation. Applying chebyshev's inequality to the continuous random variable defined by $\int_{-\infty}^{\infty} \frac{X_i f(X_i)dx_i}{n}$ and using linearity of expectation operator. We get $P\left[\left|\int_{-\infty}^{\infty} \frac{X_i f(X_i)dx_i}{n} - \mu\right| \geq \varepsilon\right] \leq \frac{\text{var}\left[\int_{-\infty}^{\infty} \frac{X_i f(X_i)dx_i}{n}\right]}{\delta^2}$

$$= E\left[\int_{-\infty}^{\infty} \frac{(X_i f(X_i)dx_i)^2}{\delta^2 n^2}\right]$$

Now again applying linearity of expectation.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 8, Issue 6, November 2019

$$E\left[\int_{-\infty}^{\infty}\left(X_i f\left(X_i\right)dx_i\right)^2\right]=\int_{-\infty}^{\infty}E\left(X_i f\left(X_i\right)dx_i\right)^2+\int_{-\infty}^{\infty}E\left(\overline{X_i}.\overline{X_j}dx\right),where\, i\neq j$$

By definition of pair wise independent of X_1, X_2……..X_n we get,

$E\left[\overline{X_i}.\overline{X_j}\right]=E\left[\overline{X_i}\right].E\left[\overline{X_j}\right]$ and using $E\left[\overline{X_i}\right]=0$ we get

$$E\left[\int_{-\infty}^{\infty}\left(\overline{X_i} f\left(X_i\right)dx_i\right)^2\right]=n.\sigma^2.$$

Hence the proof

Chernoff Bound:

Let $p\leq\frac{1}{2}$, and let $X_1, X_2, \ldots\ldots\ldots X_n$ be independent 0-1 continuous random variables, so that $\Pr[X_i = 1] = p$ for each i. Then for all $\varepsilon, O<\varepsilon\leq p(1-p)$ we have

$$\Pr\left|\frac{\int_{-\infty}^{\infty}X_i dx}{n}-p\right|>\varepsilon]>2.e^{-}\frac{\varepsilon^2}{2p(1-p)}.n$$

Proof:

Put P= $\frac{1}{2}$ and n independent samples give an approximation that deviates by ε from expectation with probability δ. That exponentially decreasing with $\varepsilon^2 n$. Now put this approximation in the above corollary we get the required proof.

Hoefding Inequality

Let $X_1, X_2, \ldots$ Xn be n independent continuous random variables with the same probability distribution, each ranging over the (real) interval [a, b], and let μ denote the expected value of each of these variables. Then, for every $\varepsilon>0$ [5]

$$\Pr\left[\left|\frac{\int_{-\infty}^{\infty}X_i dx}{n}-\mu\right|>\varepsilon\right]<2.e^{-\frac{2\varepsilon^2}{(b-a)^2}.n}$$

Proof:

The hoefdings inequality is useful for estimating the average value of a function. It is denoted by large number of values, error probability function is negligible. Put P=a, and a+b=P-b and $\varepsilon=\frac{1}{2}(\varepsilon)$. In the above corollary we get the required proof.

REFERENCES

[1] Probability & statics, S. Chand company ltd. http//: info@schandgroup.com.

[2] H.Dobbertin. The status of MD5 after a recent attack.cryptobytes, 2(2):1-6,1996.

[3] E.Barkan, E.Biham and N.Keller, Instant cipher text only cryptanalysis of GSM encrypted communication at http://cryptome.org/gsm-crack-bbk.pdf.

[4] Fundamentals of applied statistics, SC Gupta & V.K Kapoor, S.chand & sons.