ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, 2023

The Importance of Cryptography in network security using fuzzy logic.

Dr. Ashutosh Pandey, Assistant Professor, Department of Mathematics.
D.P. VIPRA P.G.College Bilaspur (C.G.) Pin- 495001
Email Id- ashutoshpandey28jd@gmail.com Mo no 9754867695.
Mrs. Snehlata Mishra Assistant Professor, Department of Mathematics.
D.P. VIPRA P.G.College Bilaspur (C.G.) Pin- 495001
Mr. Tikamsingh Rajput, Assistant Professor, Department of Mathematics.
D.P. VIPRA P.G.College Bilaspur (C.G.) Pin- 495001
Mr. Nidhi Danekar Assistant Professor, Department of Mathematics.
D.P. VIPRA P.G.College Bilaspur (C.G.) Pin- 495001

Abstract – Network security and cryptography is a concept to protect network and data transmission over wireless network. Network security typically relies on layers of protection and consist of multiple components including networking monitoring and security software in addition to hardware and applications.

Keywords:- Fuzzy logic, Cryptography, Network security

Introduction:- Cryptography in computer network security is the process of protecting sensitive information from unauthorized access when it is at rest or in transit by rendering it. Cryptosystem is the application of number theory. The hard problem in number theory uses to develop cryptosystem. Basically cryptosystem is the system for providing the security to the information. Modern world is the world of information. Some of the information requires the security such as; banking transactions, government security information, medicine information, military information, police information, economic information, password, debit card, credit card etc. This information is very important for the individual thus its security is also very important relatively. We focused on the cryptosystem based on fuzzy set. The properties of the fuzzy set are reviewed and its application presented as a cryptosystem. this system is claimed under the security, efficiency and smart to use. This gives smart decision also.

Review of literature - The concept of fuzzy logic has been firstly by L. Zadeh [29] in 1965 which is used in almost all field of research and development where include high degree of uncertainty, complexity and nonlinearity. The pattern recognition, automatic control, decision making, data classification are few of them. The theory of fuzzy logic systems is inspired by the remarkable human capacity to reason with perception-based information.

Rule based fuzzy logic provides a formal methodology for linguistic rules resulting from reasoning and decision making with uncertain and imprecise information. In fuzzy behavior based navigation the problem is decomposed into simpler tasks (independent behaviors) and each behavior is composed of a set of fuzzy logic rule statements aimed at achieving a well-defined set of objectives.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, 2023

Generally, Fuzzy Logic used for modelling uncertain systems by enabling common sense reasoning in decision-making in the lack of complete and accurate information. It enables the arrival of a definite conclusion based on input information, which is unclear, uncertain, noisy and imprecise.

The mathematics has been starting to apply in cryptology since 1976, when Diffie and Hellman [2] proposed the principle of public key cryptography. They used discrete logarithm problem (DLP) for the key exchange protocol. This was the first concept of public or asymmetric key cryptography.In 1985, RSA cryptosystem is invented by Rivest, Shamir and Adleman [8]. . ElGamal [3] is invented this scheme. In the same year, Goodman and Mcauley [] introduced another improved public key cryptosystem, which is called as Trapdoor-Knapsack cryptosystem. Basically this system is based on the idea of fuzzy set and its application. The fuzzy tool box operation is used in this. In 2001, there was presented a fuzzy logic tool kit by Shalfield [16]. This was applied in the various cryptosystems for getting the third dimension of the cryptosystem which is called the smart to use. The fuzzy set is presented by the probabilistic approach in the year 2004, by Delman [1]. He proposed a cryptosystem based on Genetic Algorithm. In this system, fuzzy logic tool kit is applied. Hence this scheme proved the both parameters of security and efficiency. Other cryptosystems are XTR, Elliptic Curve, Hyper elliptic curve etc [1-28], which is left the impression for some time in the quick change world of security.

Generally, Fuzzy Logic used for modelling uncertain systems by enabling common sense reasoning in decision-making in the lack of complete and accurate information. It enables the arrival of a definite conclusion based on input information, which is unclear, uncertain, noisy and imprecise.

1. Fuzzy Network Systems:

Let N be a network. It can be defined as the function;

N : $y=f(x_1,x_2,.....x_n)$

Where x_i is the $_i$th independent variable;

i=1,2,3,…….,n

if $X=\{x_1,x_2,……x_n\}$ is defined by Fuzzy as,

$$A=\{\frac{\mu_A(x_1)}{x_1}+\frac{\mu_A(x_2)}{x_2}+\cdots\}$$

$$=\left\{\sum_{i=1}^{n}\frac{\mu_A(x_i)}{x_i}\right\}$$

This is the discrete representation, but for the infinite number of variables, the representation will be as follows:

$$A=\left\{\int\frac{\mu_A(x)}{x}\right\}$$

There is an uncertainty is considered. This uncertainty is refers to the probability theory. Thus the above representation transferred into the following:

X : x_1 x_2 . . . x_n

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, 2023

$P(X) : p(x_1)\ p(x_2)\ .\ .\ .\ p(x_n)$
$P :\ p_1\ \ p_2\ .\ .\ .\ p_n$

Hence, for the finite nos.,
$A=\left\{\frac{\mu_A(p_1)}{p_1}+.\ .\ .+\frac{\mu_A(p_n)}{p_n}\right\}$
Hence, for the infinite nos.,
$A=\left\{\int\frac{\mu_A(p)}{p}\right\}$

This is presented as the prerequisites for the proposed Network System.
The network N analyzes over the two parameters, Structure Optimization and Sequencing.

These two are the major challenges in any Network .Network consists a defined structure but its optimization is always in the centre of the Network's study. This paper presents a new technique based on fuzzy to fulfill this requirement of every network system.Next is, Sequencing , it is also a challenging task in the world of network.

But by the fuzzy logic , the ordering can be defined over the structure of the vertex and nodes,
Network Optimization : Let N be a network by the graph theory,
N=(V,E)
There are existing the finite sets of vertex and edge. Thus the objective is, to obtain the subsets of vertex and edge.
Let $V=\{V_1,V_2,\ .\ .\ .,V_n\}$
and $E=\{E_1,E_2,\ .\ .\ .,E_n\}$
Then the subset of V be
$V'=\{v_1,v_2,\ .\ .\ .,v_m\}$
And the subject of E be
$E'=\{e_1,e_2,\ .\ .,e_m\}$; $m<n$
By the fuzzification of V,
$A=(V,\ \mu_A(V))=\{(v_1,\ \mu_A(V_1)),\ .\ .\ ,\ (v_n,\ \mu_A(V_n))$
and by the fuzzification of E,
$B=(E,\mu_B(E))=\{(e_1,\ \mu_B(e_1),\ .\ .\ .,\ (e_m,\ \mu_B(e_m)\}$
There is the certainty in E and V , as the subset formation of it. Thus the probability distribution can be defined over V ? E
$P(V)=\{p(v_1),\ .\ .\ .,p(v_n)\}$
$P(V')=\{p(v_1),.\ .\ .,p(v_m)\}$
$P(E)=\{p(e_1),.\ .\ .,p(e_n)\}$
$P(E')=\{p(e_1),.\ .\ .,p(e_m)\}$
And its fuzzy representation is

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, 2023

A'=(p(V), $\mu_{A'}$(p(V)))={(p(v1), $\mu_{A'}$(p(v_1)), . . ., (p(v_n), $\mu_{A'}$(p(v_n)))}
B'=(p(E), $\mu_{B'}$(p(E)))={(p(e1), $\mu_{B'}$(p(e_1)), . . ., (p(e_n), $\mu_{B'}$(p(e_n)))}
By Fuzzy Bayesian Decision Method,

P={P(v_1), . . ,P(v_n)}, where $\sum_{i=1}^{n} P(v_i) = 1$

And

E={P(e_1), . . ,P(e_n)}, where $\sum_{i=1}^{n} P(e_i) = 1$

Suppose,
The optimum decision depends on the following set of actions;
C={a1,a2, . . ,an}
Then the expected utility associated with the followings:
E(u_y)=$\sum_{i=1}^{n} u_{yi}$P(v_i)
And
E(u_y)= $\sum_{i=1}^{n} u_{yi}$P(e_i)
Thus, the maximum expected utility can be defined by
E(u)=max E(u_y).
Finally, we propose a cryptosystem based on the above secure fuzzy network system.

2. Fuzzy Cryptosystem:

2.1. Key Generation:

2.1.1. The message = m.

2.1.2. *The Fuzzy Key Set =* $\{k_1,...,k_n\}$.

2.1.3. *The Fuzzy Key Subset =*

$\{k_1\}$

$\{k_1, k_2\}$

.

.

.

$\{k_1,..., k_{n-1}\}$

2.1.4. *The Fuzzy Key Operation:*

This is based on the fuzzy rule. Fuzzy algebraic properties can be applied to form the fuzzy structure for the cryptosystem.

In below, this is explained.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, 2023

$k_1 \cup k_2$

$or,$

$k_1 \cup k_2 \cup k_3$

$or,$

.

.

.

$or,$

$k_1 \cup ... \cup k_{n-1}$

or

$k_1 \cap k_2$

$or,$

$k_1 \cap k_2 \cap k_3$

$or,$

.

.

.

$or,$

$k_1 \cap ... \cap k_{n-1}$

$or,$

$1 - k_1 \cup k_2$

$or,$

$1 - k_1 \cup k_2 \cup k_3$

$or,$

.

.

.

$or,$

$1 - k_1 \cup ... \cup k_{n-1}$

or

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, 2023

or,

$1-k_1 \cap k_2$

or,

$1-k_1 \cap k_2 \cap k_3$

or,

.

.

.

or,

$1-k_1 \cap ... \cap k_{n-1}$

2.2. Encryption:

$ciphertext = (m)(k_1) * (k_2) \# ... @(k_n)$

Where,

$\{*, \#, @\} = FuzzyOperation.$

2.3. Decryption:

$Plaint\ ext = m =$

$Defuzzification[(k_1) * (k_2) \# ... @(k_n)]$

Where,

$\{*, \#, @\} = FuzzyOperation.$

3. Conclusion: Although there are several cryptosystems based on different mathematical problems, but this is the first cryptosystem based on the classification. The fuzzy class is unique, thus its security is also unique correspondingly. The existing algorithm for attacking cryptosystems cannot be applied to the proposed cryptosystem. Hence this cryptosystem becomes the securest and also practical to use by its own network system of fuzzy.

REFERENCES

1. B Delman, Genetic Algorithms in cryptography, Rochester Institute of Technology Publication, 2004.
2. W Diffie, M E Hellman, New directions in cryptography, IEEE Transactions on Information Theory, 22, 1976, 644-654.
3. T ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory, 31, 1985, 469-472.
4. R Goodman, A Mcauley, New Trapdoor-Knapsack public key, IEEE Transaction on Information Theory, 132 (6), 1985, 56 – 65.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, 2023

5. N Koblitz, Elliptic curve cryptosystems, Mathematics of Computation, 48, 1987, 203-209.
6. N Koblitz, Hyperelliptic cryptosystems, Journal of Cryptology, 1, 1989, 139-150.
7. A K Lenstra, Verheul E R, The XTR public key system, Advances in Cryptology — CRYPTO 2000, Lecture Notes in Computer Science, Springer-Verlag.
8. R L Rivest, A Shamir, L Adleman, A method for obtaining digital signatures and public key cryptosystems, Communication of the ACM, 21, 1978, 120-126.
9. T. Satoh, The canonical lift of an ordinary elliptic curve over a prime field and its point counting, Journal of the Ramanujan Mathematical Society, 15, 2000, 247-270.
10. T. Satoh and K. Araki, Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves, Commentarii Mathematici Universitatis Sancti Pauli, 47, 1998, 81-92.
11. T. Satoh, B. Skjernaa and Y. Taguchi, Fast computation of canonical lifts of elliptic curves and its application to point counting, Finite Fields and Their Applications, 9, 2003, 89-101.
12. O. Schirokauer, Discrete logarithms and local units, Philosophical Transactions of the Royal Society of London, Series A, 345, 1993, 409-423.
13. R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, Mathematics of Computation, 44, 1985, 483-494.
14. R. Schoof, Nonsingular plane cubic curves, Journal of Combinatorial Theory, Series A, 46, 1987, 183-211.
15. I. Semaev, Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p, Mathematics of Computation, 67, 1998, 353-356.
16. R Shalfield, Fuzzy Logic Toolkit, IPA, IK, 2001.
17. P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM Journal on Computing, 26, 1997, 1484-1509.
18. J. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, 1986.
19. J. Silverman, The xedni calculus and the elliptic curve discrete logarithm problem, Designs, Codes and Cryptography, 20, 2000, 5-40.
20. J. Silverman and J. Suzuki, Elliptic curve discrete logarithms and the index calculus, Advances in Cryptology — ASIACRYPT '98, Lecture Notes in Computer Science, Springer-Verlag, 1514, 1998, 110-125.
21. N. Smart, The discrete logarithm problem on elliptic curves of trace one, Journal of Cryptology, 12, 1999, 193-196.
22. D. R. Stinson, Cryptography: Theory and Practice, CRC Press, Boca Raton,

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, 2023

Florida, 1995.
23. E. Teske, Speeding up Pollard's rho method for computing discrete logarithms, Algorithmic Number Theory: Third International Symposium, Lecture Notes in Computer Science, Springer-Verlag, 1423, 1998, 541-554.
24. N. Thferiault, Index calculus attack for hyperelliptic curves of small genus, Advances in Cryptology — ASIACRYPT 2003, Lecture Notes in Computer Science, Springer-Verlag, 2894, 2003, 75-92.
25. C. Tobias, Design and analysis of cryptographic building blocks on non-abelian groups, Mitt.-Math.-Sem.-Giessen., Volume No. 253, 2004, 122.
26. E. Verheul, Evidence that XTR is more secure than supersingular elliptic curve cryptosystems, Advances in Cryptology — EUROCRYPT 2001, Lecture Notes in Computer Science, Springer-Verlag, 2045, 2001, 195210.
27. L. Washington, Elliptic Curves: Number Theory and Cryptography, CRC Press, 2003.
28. A. Yun, J.Kim, D. H. Lee, Cryptanalysis of a divisor class group based public key cryptosystem, Collection: Algorithmic number theory, LNCS, 3076, 2004, 442-450.
29. L. A. Zadeh, “Fuzzy sets”, Information and Control, Volume 8, issue 3, June 1965, pages 338-353.