



Chaotic African Buffalo Optimization Based Efficient Key Mechanism in Categorized Sensor Networks

J.R.Arunkumar

Abstract: In recent days, Wireless Sensor Network (WSN) can be used to monitor the circumstances of various movable objects and several processes such as friendly forces monitoring, biological attack detection, fire detection and so on its applications are extended. To make all these applications reliable and secure, it is necessary to use cryptographic processes. The security of the whole network is depending on the strength of a generated key, the algorithm decides the size of the key handling and processing. In this research, a secure efficient key management scheme is proposed with the help of Chaotic African Buffalo Optimization (CABO) for wireless sensor networks. The evaluation of this method is made with the objective to improve the security strength and reduce the cost of resource. The traditional methods called genetic algorithm and an evolutionary algorithm named as Particle Swarm Optimization (PSO) is compared to verify the proposed scheme.

Keywords: Key Generation, Particle Swarm Optimization, Chaotic African Buffalo Optimization, Genetic algorithm.

I. INTRODUCTION

In sensor network, the key management is one of the core securities protocols for several real time applications. Normally, many researches were focused on some constrained resource such as limited battery power and processing capabilities. Apart from these constraints' security is one of the main factors that decides the data transmission between nodes. Data transmission from one node to another is depends upon the electronic security. For any legal transmission of information, it is necessary to encrypt the data. For this process the cryptography is used to convert the original information into unreadable format and while retrieving the data this encrypted data is again converted into original messages. Some of the security issues in sensor nodes are stated as, the radio links are insecure and sensor nodes are not temper resistant (i.e., attacker obtains all security information). Cryptographic methodology and cryptographic key are the two factors deciding cryptography. The algorithm decides the encryption and decryption process with the key as a parameter used by the function. The total security strength is made by the algorithm with several objectives named as key freshness, key authentication and key integrity. The mathematical process depends upon the selection of algorithm, to provide authentication and confidentiality.

The discrete logarithmic problem stated by Stinson (2005) is implemented with two prime numbers. Likewise, other key generation methods include the derivation of a key from another key, these processes are made by deriving the key from its password. Many traditional schemes focused on key pre-distribution schemes to make robustness in design reduce the memory requirement. In existing methods, the Diffie-Hellman (Rescorla 1999) method are used for two layered key management and dynamic key update protocol. These processes never suit sensors with large key sizes. The limitations of these process are unable to access the large keys, increases overload, security is less and induce key escrow problem.

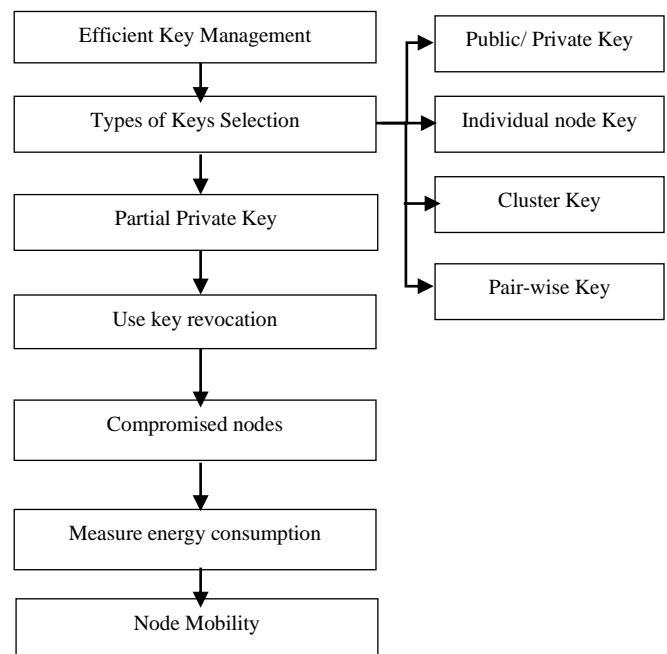


Figure 1 Key management flow diagram

The evolutionary algorithm (EA) considered in this research is Chaotic African Buffalo Optimization (CABO), it is an optimization technique established on intelligence of African buffalos and its movement. It is effective for tracking and identification of green pastures. The solution search is based on the sound made by each buffalo. The previous implementation of CABO made in travelling sales man problem. Mainly this optimization is selected for solving several problems because of its faster speed.

Revised Manuscript Received on February 05, 2020.

* Correspondence Author

Dr.J.R.Arunkumar, Assistant professor in faculty of Computing and Software Engineering, Institute of Technology, Arbaminch University, Ethiopia

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>)



Chaotic African Buffalo Optimization Based Efficient Key Mechanism in Categorized Sensor Networks

This section discussed about some main problems and traditional key management scheme. For further implementation and improvement in key management is the main objective of this work. Hence, a detail review and background study are made in Section 2. Section 3 provides the exact problem which is identified from the survey. Section 4 states research methodology that contains traditional genetic algorithm, particle swarm optimization and the proposed Chaotic African buffalo optimization for improving key management. To verify the experimental results, section 5 provides detail comparison among all methods. Finally, the conclusion is made in section 6 with the future directions.

II. LITERATURE SURVEY

In real time data processing environments, the sensor network occupies more processing units and security issues. Lee et al., (2004) presented a key management scheme that satisfies both operational and security requirements of distributed sensor networks. They have made a data aggregation for energy efficiency and watchdog mechanism for intrusion monitoring as an additional feature. They designed this scheme for applying in variety of sensor network protocols.

In order to achieve security in sensor networks, the messages must encrypt among sensor nodes. For encryption the keys must processed by communicating nodes. Due to several resource constraints, achieving such key agreement in networks is nontrivial. Some of the traditional pre-distribution of secret keys for all pairs of nodes is not suitable because the memory is large if the network is large. The assumption is made for random key pre-distribution schemes because there is no deployment knowledge is available. To solve these factors, Du et al., (2004) presented a key management scheme by deployment knowledge. They arranged the performance metrics such as connectivity, memory usage, and network resilience.

Sarkar and Mandal (2012) proposed a Public Key Cryptography (PKC) using swarm as solitary has been carried for wireless communication, it is tested with the with the deterministic approach. Hussein et al., (2010) observed that encryption based on chaotic map that has been derived from a simplified model of Swarm Intelligence (SI). They have been proposed along with the analysis of the possibility of using SI in the field of image cryptography. To increase the robustness of the system the Swarm Intelligence Chaotic Map (SICM) is used.

Sl.No	Citation	Methodology	Advantages	Role and applications
1	Chen and Chen (2014)	Secure routing solution based on LEACH protocol	It improved the survivability of node more efficiently in a harsh sensor network environment	System security is integrated into sensor node. Clusters are changed dynamically and periodically according to node mobility.
2	Celozzi et al., (2013)	Enhanced variant of the LEAP+ protocol	Decreases the key setup time by reducing the number of packets exchanged	To improve the security of communications and implement in hardware to verify the number of security threats
3	Wan et al., (2015)	Public-Key-Based Data Integrity Protection	Reduced the signing cost, PKDIP can even be more efficient than hash-function-based schemes.	It introduces the "Montgomery Modular Multiplication (MontMM)" technique to current public-key-based signing algorithm for wireless Image Sensors
4	Rahman and Sampalli (2015)	Efficient Pairwise and Group Key Management Protocol	It is efficient in terms of computation, communication and energy overhead.	It is designed to support both pairwise and group-wise key management
5	Latiff et al., (2016)	Hybrid algorithm based on Backtracking Search Optimization Algorithm (BSA) and K-Means	It is able to deliver more data to the base station and extends the network lifetime.	Heuristic algorithm is required to produce good clustering in sensor networks.

TABLE I: COMPARISON OF KEY MANAGEMENT SCHEMES

Sreelaja and Pai (2008) made a Ant Colony Key Generation Algorithm (AKGA) based key generation to perform encryption of data in cellular network. Sreelaja and Vijayalakshmi presented an encryption method of plaintext using a stream cipher method with single AKGA. The keys generation for encryption is made by swarm intelligence approach. In order to reduce the number of keys, an Ant Colony Optimization Key Generation Algorithm (AKGA) is used. Khan et al., (2013) made a Data Encryption Standard (DES) by Ant-Crypto and Binary Ant Colony Optimization (BACO). They made two metrics such as the ratio of the optimum keys in all solution and the number of success bits that are matched with the original key. Zhu et al., (2006) described a hierarchical key management method called as Lightweight Extensible Authentication Protocol (LEAP) to meet the different security requirements. They establishment

is of four types of keys for each sensor node, such as individual key, group key, cluster key and pair key.

The editorial work done by Chinwe et al., (2018), discussed about the African Buffalo Optimization (ABO) algorithm which is a search mechanism consuming an appropriate chaotic function. In the class of bio-inspired algorithm the ABO algorithm is meta-heuristic algorithm which is derived from the Swarm Intelligence Methodology. This algorithm inspired by scavenging and shielding the taxonomy of the African buffaloes who are sheltered in the East Africa and sub-Saharan of South. As like the literature in N-P hard problems similar to Travelling Sales Man problem the in the world of meta-heuristics, the ABO algorithm had been established expressively enhanced performance.



The chaotic logistic chart alleviated the flaws in the standard ABO algorithm by the reviews referred from the proposed work and then it evolved to a nonlinear guideline function termed as the Chaotic improved African Buffalo Optimization (CABO) and weighed against the typical standard algorithms such as the PSO, chaotic PSO and ABO algorithms. The performance of the CABO scored 92% of the performance ratio in comparison between the three algorithms. This research has been concluded with two results of annotations. That is, the best strategy for the ABO algorithm is stated as the logistic map. Additionally, In the real-world optimization glitches it is suggested to apply the CABO algorithm for issues similarly as scheduling, supply chain management, and many more as well in security key management.

The study of Li et al., (2018), discuss about the proposed work of creating a location sensor for supervising and maintaining the worked possessions, and for understanding the data collection of real-time location and time accuracy of the intellectual workshop, by applying in the wireless sensor network. In this mechanism for verifying real-time accurateness, a three-dimensional adaptive fruit fly optimization algorithm is modelled which computes the location, and this procedure resolved and adapted the three-dimensional location in the smart workshop and presented the familiarized coefficient of inertial weight, engaged the benefits of the fruit fly optimization algorithm to a robust local search ability, enhanced the global optimization ability.

A congestion control algorithm on behalf of the multi-objective development algorithm is proposed to manage the parameter by Singh et al., (2018), termed PSOGSA for rate optimization and regulating arrival rate of data from every child node to the node. The energy of the node to its appropriate function would be measured in a multi-objective optimization function. The optimization method controls the onset level on the priority origin: child node energy and result obtainable bandwidth.

Cai et al., (2019), addressed the LEACH protocol, which is an arbitrary selecting way of cluster-head nodes of cycles, resulting in scattering of energy node and diminished lifetime of entire network. This article proposed the FTBA algorithm adding the global search capabilities and curve strategy. Then integrated the amended BA with LEACH, and has sturdier optimization capability compared to other optimization algorithms, which has the method (FTBA-TC-LEACH) excel than the LEACH and LEACH with Standard BA (SBA-LEACH). The FTBA-TC-LEACH boosted lifetime and decreased the energy consumption in WSN.

Kaur et al., (2020), discussed about the localization algorithm which is divided into two categories, namely range-based and range-free are cost-effective, but lack accuracy. The part of nature-inspired processing in improvising the precision of range-free procedures were examined. Interpretations portrayed after comprehensive literature survey of current exploration in this extent signifies the reputation of such sensor localization algorithm.

III. PROBLEM STATEMENT

The security issues are utilized for proposing the clustering routing protocol which are surveyed from the many sources. Here there is a need of key every time when a message or data is encrypted and that is specified as the

problem and at the receiving unit that key aids in getting back the normal form. At the time of encryption process there arises a problem that is clustering head selection and key updating. The clustering network can be enhanced by, numerous optimization algorithms. Meanwhile, one of the most important modes of protecting the clustering safety is that the key management. So, the algorithms which are carried traditionally as like Genetic algorithms (GA) is improvised to enhance and solve the discrete optimization problems presented in the network based on the fitness value. The evolutionary techniques are one of the alternative methods for traditional techniques, because traditional methods are in high nonlinearity and low autocorrelation. In this research, the security issues and network success rates are considered and analyzed. To solve these issues a new inspiration made from the behavior of African buffalo is considered.

IV. RESEARCH METHODOLOGY

A new optimization methodology which is presented and termed as the African Buffalo Optimization by Odili et al., (2016). One of the endangered wild species that cattle in Africa is the African buffalos, it is set to find the rainy weather forecasts in various parts of Africa as it is mostly in mobile tracking. The optimization mechanism is achieved with the aid of two basic sounds in the search of finding solution. They are effective, efficient, user-friendly and are implemented easily. The Location of every buffalo would be usually updated and ensured relatively to any of the particular buffalo's best previous location by the use of the ABO, to try solving the pre-mature convergence problem. The number of iterations does not improve the present location of the best buffalo's location, instead it re-initializes the entire herd (present location). The Search space is kept under tracking in the basis of best suitability and the other buffalo's experience is tapped. The key management which using the certain algorithmic steps are as follows,

Step1. The aim of the function of $f(x) \quad x = (x_1, x_2, \dots, x_n)^T$

Step2. Initialization: at the solution space randomly set the buffalos to the nodes;

Step3. Use the following equation and update the buffalo's fitness values

$$w_{.k+1} = w_{.k} + lp_1 (bg_{max.k} - m_{.k}) + lp_2 (bp_{max.k} - m_{.k})$$

Where $w_{.k}$ and $m_{.k}$ denotes the survey and exploitation navigates respectively of the k^{th} buffalo ($k=1, 2 \dots N$); lp_1 and lp_2 are learning factors; r_1 and r_2 are random numbers between $[0, 1]$.

The best suitability of the herd is bg_{max} and the individual buffalo's best is the bp_{max} .

Step4. Renew the site position of the buffalo k with reference to $bp_{max.k}$ and $bg_{max.k}$ utilizing

$$m_{k+1} = \lambda (w_{.k} + m_{.k})$$

Where ' λ ' is a unit of time.

Step5. Examine the renewal of bg_{max} regularly. Move to 6, if yes or else, move to

2



Step6. Go back to the algorithm step 3 if the stopping criteria is not yet met.

Step7. The best solution is resulted in the output.

There are categorizations in the model of the African buffalo optimization, the buffalo with “maaa” sound is specified as $(k=1,2,3,...n)$ and represented by $m_{.k}$, next the buffalo with the sound “waaa” is denoted as $w_{.k}$. The keying process is updated in the basis of the node to generate the initial key. In this the buffalo’s fitness is directly depended. In combination with the plaintext message a keystream is generated in the basis of the random or pseudorandom characters or an encrypted message is produced with an image. Regularly, an Arithmetic cipher text is created by adding, subtracting, XORing the character in the plaintext with the key stream character.

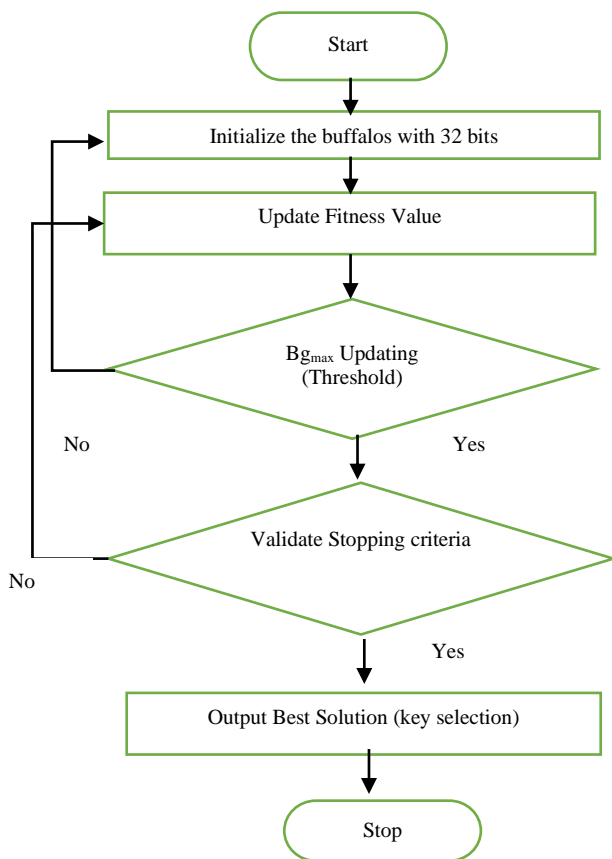


Figure.2 Key Generation using ABO

The initial process is selection of bits, here 32 bits is considered, each bit (buffalo) is validated by their fitness value. The bg_{max} is used here to measure the threshold value with respect to the African buffalo’s optimization. The key generation process using ABO is represented in a flow chart as shown in the figure 2. The mobility is noted by the sensor nodes with respect to the buffalo’s fitness value. The w_k represents the initial node bit length. A sample key obtained from the initial step based on iterations is shown in figure 3.

32bit length	0010 0101 0110 0100 1010 0111 0111 0001
--------------	---

Figure 3 Sample Key of 32-bit length

Key generation is the most important factor, hence, in this work ABO is used in the key generation process where key selection is depends upon the fitness function. Based on the iteration, the key has its highest fitness value. The selection value is selected with the threshold value to compare the process. The key must be selected as unique and non-repeating. The encryption is made with the selected key and are highly encrypted because of more randomness of key.

Types	Parameters		
GA	$\beta=2.0$	200 Nodes	$\rho=3.56$
PSO	$p_i=1.5$	150 Nodes	$t_{initial}=0.65$
ABO	$m.k=1.0$	150 Nodes	$Bg_{max}=0.61$

TABLE II: PARAMETER SETTING

The main advantages of ABO based on key generation is more accurate and the session key can be established directly between any two (buffalos) sensor nodes.

In GA the initial process is started with an initial population of 32 bits chromosomes which are generated randomly. This population is stored in an array, that contains maximum population, $initPop [MAX_POPULATION]$, in this process each cell consists of binary values 0 or 1. The maximum nodes considered here is 200, $MAX_POPULATION$. The size of chromosome cell is equivalent to the length of key intended to be generated.

The genetic algorithm flow is represented by initialization, threshold check, followed by iterative application of operators. For processing and selection, the following format is used, the size of array, final population meets $MAX_POPULATION$ limit. Parent selection, crossover and mutation is the basic process of GA. Finally, the fitness value is calculated for each chromosome.

For PSO process the algorithm parameters such as $Swarm_Size$, Max_Iter , $c1$, $c2$, w , V_MAX are considered. First step in PSO is initialization of swarm of particles, updating the global best position followed by initializing the velocity of particles. Each particle in swarm is initialized with a random seed velocity which is bounded by the intervals V_MAX and V_MIN . by updating the particles velocity the key generation I selected. Finally, the position is updated and find the best key.

$$x[i] = x[i] + v[i]$$

where, $x[i]$ is position of i^{th} particle and $v[i]$ is velocity of i^{th} particle. After updating the threshold value, the fitness function calculates the fitness of key stored at a particular location in key domain. The sequence of 0s and 1s provides the best randomness among all process.

A. Improvement in ABO

The basic control of ABO is maintained by the two equations Eqs.1 and 2 which refers to as location and democratic update equations, respectively, as earlier it was mentioned. Yet, the expectational memory capacity of the African Buffalos does not reason for those two equations.



Especially, based on the past experiences the herd may not explore the greener land or pastures and may identify a grazing land. So, the pre-mature convergence has the possibility reason of being the most observed.

optimization problems. Also, the λ in location update equation

Eq.2 is a simple random number generator, this implies that the search is aimless within the search space resulting in relatively inefficient solution and or premature convergence as the case may be. However, employing chaos and levy distribution properties could be a possible solution to these problems.

B. Chaotic Mapping Strategy

A system is said to be chaotic if it exhibits a kind of random deterministic behavior in a bounded but nonconverging search space. Many stochastic optimization problems are trapped in local optima. However, literature show that chaotic sequence or map could be used to deal with local optima problem. Some examples of such algorithms are GA, DE, PSO, FA, ACO, SA, imperialistic competitive algorithm, charged system search optimization, and big-bang big-crunch optimization, etc. as referenced therein. Basically, chaotic optimization is the use of chaotic sequence instead of random variables in an optimization algorithm. There are variations of one-dimensional chaotic maps including, logistic, iterative, sinusoidal, sin, circle, Chebyshev, intermittency, singer, sawtooth, pieces wise, tent, and Leibovitch. However, this study considers logistic map for ABO randomization. Eq. 3 represents the logistic function.

$$\mu_{m+1} = \beta \cdot \mu_m(1 - \mu_m)$$

C. The Proposed CABO

In this case, the learning terms of the democratic equation Eq. (1) is multiplied by a suitable chaotic sequence. This is to enhance exploration of the algorithm and guide against premature convergence. That is, given a chaotic map

$$\mu_{i+1} = f(\mu_i) \quad (8)$$

The democratic and exploitation equation have been modified as shown in Eqs. 9 and 10

$$m_{i+1} = m_i + l_1 \mu_i * ((b_{ogmax} - w_i) + l_2 \mu_i * (b_{opmax} \cdot i - w_i)) \quad (9)$$

$$w_{i+1} = \left(\frac{w_i + m_i}{\lambda} \right) + \mu \quad (10)$$

Where.* is element-wise multiplication of vectors. The step by step implementation is shown in Algorithm 2. The main property of chaos is that a slight variation in underlying population drastically yield unique outcome at each iteration. This characteristic enables the system to generate dynamic values at every iteration (search), which consequently enhance the quality of the solution within a shortest possible time. In this proposed CABO, an initial value of 0.01 and parameter value of 4 for the logistic map is used, as shown in Eqs.9 and 10. This enables the buffaloes (solutions) generate an efficient search mechanism that could escape local optima entrapment. The steps are illustrated in Algorithm 2. First, the Buffaloes are randomly initialized within the search space. Then, the chaotic sequence is generated. Next, the exploitation and democratic process is executed using chaotic map and chaotically enhanced

parameters (11, 12) respectively. These processes are carried out iteratively until the stopping criteria is reached. In other words, at each iteration, the fitness value of the new solution is evaluated to select the best solution. The maximum number of iterations is set to 100. Ten non-linear benchmark problems are utilized for the performance validation of the proposed CABO. The flow diagram of the proposed CABO is shown in fig. 1, the red color highlight captures modification of the basic ABO to CABO.

V. EXPERIMENTAL RESULTS

The performance of the proposed Chaotic African buffalo optimization algorithm is compared with the genetic algorithm and particle swarm optimization and the African buffalo optimization algorithm. The ratio of the optimum keys in all solution and the guessed key's bit are compared with the origin key. It is implemented in network simulator, to find the ratio of the optimum keys in all solution and the bits in guessed key that are matched with the original key, these are considered as the performance metrics.

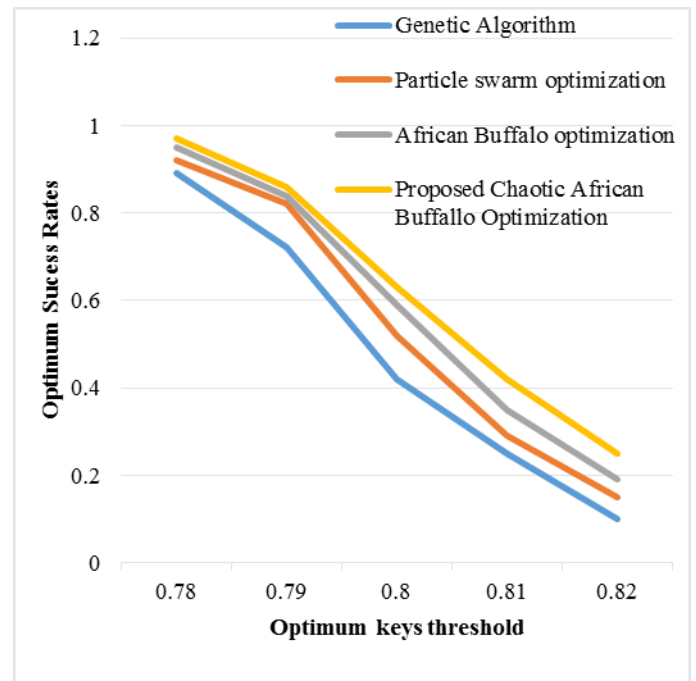


Fig 4 Comparison of GA, PSO, ABO and Proposed CABO based on optimum success rate

Implementation of the proposed work is done to find Public Key Cryptography with CABO, ABO, PSO and GA algorithm. A Quality cryptography is achieved through the key generation with great suitability of the proposed method. This graphical representation shows that the generated keys using the proposed CABO are more secure and unique for the data encryption.

The representation of fig 4 defines the comparison of traditional GA, PSO, ABO and proposed CABO methods with the optimum key generation. The success rate varied according to the iteration. If the threshold value is equal or near to unique then the original key is matched (i.e., Key is matched).



The number of success bits in the minimum threshold value is compared and deduced in the Fig 5 shown. When all the four optimization algorithms are equal in value, it is in minimum threshold value, if the success bits increased then the is in threshold varied state.

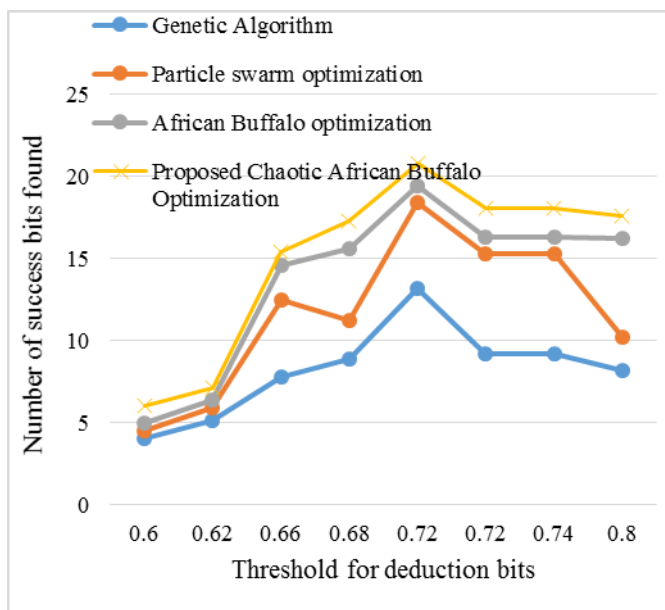


Fig 5 Comparison of GA, PSO, ABO and proposed CABO based on success bits

The experimental results shows that it has strong adaptability and the performance factor is improved based on the threshold value. If iteration is found then the bit selection is varied and gives the success bits. It helps in each encryption and decryption process. Finally, data confidentiality and data integrity is achieved due to chaotic optimal nature of buffalo’s strategy.

VI. CONCLUSION

Several researches only focused an energy as constrain, for security issues some standard algorithms are used to solve it by probability of node capturing. The chaotic African buffalo optimization based key management is proposed in this research to maintain the security level of all nodes by keeping a cluster head. The proposed CABO-KM provides effective selection and capturing the nodes activity. The dynamic changing of buffalo’s location directly links the nodes and their respective updating mechanism. The risk factor is reduced and the security level of data transmission is improved. Yet, still there is a need to improve network applicability by several factors such as key management, applying the proposed scheme in key management scheme, implementing it in secure routing that focus on multi path routing. In addition to that the security solutions are focused based on the management overhead.

REFERENCES

1. Celozzi, C., Gandino, F., & Rebaudengo, M. (2013, June). Improving Key Negotiation in Transitory Master Key Schemes for Wireless Sensor Networks. In International Conference on Sensor Systems and Software (pp. 1-16). Springer International Publishing.
2. Chen, L., & Chen, L. (2014). An improved secure routing protocol based on clustering for wireless sensor networks. In Mechatronics and

- Automatic Control Systems (pp. 995-1001). Springer International Publishing.
3. Du, W., Deng, J., Han, Y. S., Chen, S., & Varshney, P. K. (2004, March). A key management scheme for wireless sensor networks using deployment knowledge. In INFOCOM 2004. Twenty-third Annual Joint conference of the IEEE computer and communications societies (Vol. 1). IEEE.
4. Hussein, R. M., Ahmed, H. S., & El-Wahed, W. F. A. (2010, March). New encryption schema based on swarm intelligence chaotic map. In Informatics and Systems (INFOS), 2010 The 7th International Conference on (pp. 1-7). IEEE.
5. Khan, S., Ali, A., & Durrani, M. Y. (2013). Ant-Crypto, a Cryptographer for Data Encryption Standard. IJCSI International Journal of Computer Science Issues, 10(1).
6. Latiff, N. A., Malik, N. N. A., & Idoumghar, L. (2016, August). Hybrid Backtracking Search Optimization Algorithm and K-Means for Clustering in Wireless Sensor Networks. In Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), 2016 IEEE 14th Intl C (pp. 558-564). IEEE.
7. Lee, Y. H., Phadke, V., Deshmukh, A., & Lee, J. W. (2004, August). Key management in wireless sensor networks. In European Workshop on Security in Ad-hoc and Sensor Networks (pp. 190-204). Springer Berlin Heidelberg.
8. Odili, J. B., Nizam, M., & Kahar, M. (2016). African Buffalo Optimization. International Journal of Software Engineering & Computer Sciences (IJSECS), 2, 28-50.
9. Rahman, M., & Sampalli, S. (2015). An efficient pairwise and group key management protocol for wireless sensor network. Wireless Personal Communications, 84(3), 2035-2053.
10. Rescorla, E. (1999). Diffie-Hellman key agreement method.
11. Sarkar, A., & Mandal, J. (2012). Swarm intelligence based faster public-key cryptography in wireless communication (SIFPKC). Int. J. Comput. Sci. Eng. Technol.(IJCSET), 7, 267-273.
12. Sreelaja, N. K., & Pai, G. V. (2008, January). Swarm intelligence based key generation for text encryption in cellular networks. In Communication Systems Software and Middleware and Workshops, 2008. COMSWARE 2008. 3rd International Conference on (pp. 622-629). IEEE.
13. Sreelaja, N. K., & Vijayalakshmi Pai, G. A. (2011). Swarm intelligence based key generation for stream cipher. Security and Communication Networks, 4(2), 181-194.
14. Stinson, D. R. (2005). Cryptography: theory and practice. CRC press.
15. Wan, C., Zhang, J., & Huang, J. (2015). PKDIP: Efficient Public-Key-Based Data Integrity Protection for Wireless Image Sensors. Journal of Sensors, 2015.
16. Zhu, S., Setia, S., & Jajodia, S. (2006). LEAP+: Efficient security mechanisms for large-scale distributed sensor networks. ACM Transactions on Sensor Networks (TOSN), 2(4), 500-528.
17. Li, S., Zhang, C., & Qu, J. (2018). Location Optimization of Wireless Sensor Network in Intelligent Workshop Based on the Three-Dimensional Adaptive Fruit Fly Optimization Algorithm. International Journal of Online Engineering (iJOE), 14(11), 202-211.
18. Singh, K., Singh, K., & Aziz, A. (2018). Congestion control in wireless sensor networks by hybrid multi-objective optimization algorithm. Computer Networks, 138, 90-107.
19. Cai, X., Sun, Y., Cui, Z., Zhang, W., & Chen, J. (2019). Optimal LEACH Protocol with Improved Bat Algorithm in Wireless Sensor Networks. KSII Transactions on Internet & Information Systems, 13(5).
20. Kaur, A., Gupta, G. P., & Mittal, S. (2020). Impact of Nature-Inspired Algorithms on Localization Algorithms in Wireless Sensor Networks. In Nature-Inspired Computing Applications in Advanced Communication Networks (pp. 1-18). IGI Global.
21. Dr. M. SundarRajan, Dr. J. R. Arunkumar Dr. R. Anusuya (2020). Energy Efficient Cluster Head Selection in Adhoc On Demand Multipath Distance Vector Routing Protocol”. International Journal of Scientific & Technology Research (pp.4163-4172), 9(1).
22. Dr.J.R.Arunkumar, Dr.M.Sundarrajan, Dr.R.Anusuya, Mr. A.Kibread (2017) “African Buffalo Optimization based Efficient Key Management in Categorized Sensor Networks”, The 5th International Conference on the Advancement of Science and Technology ICAST, Proceedings.

23. Dr.J.R.Arunkumar, Dr.M.Sundarrajan, (2016). An Efficient Greedy Algorithm to Improve the Lifetime of the Wireless Sensor Network, CiiT International Journal of Networking and Communication Engineering Vol 8, No 10

AUTHORS PROFILE



Dr.J.R.Arunkumar, has excellent contribution in higher technical education in India and AbroadHe has B.E, M.Tech, and Ph.D. in the field of Computer Science and Engineering, Currently, He is working more than 7 years as an Assistant professor in faculty of Computing and Software Engineering, Institute of Technology, Arbaminch University, under the MOEFDRE, UNDP projects in Ethiopia. He published more than fifteen International and National journals like Scopus and UGC approved journals, He also obtained one patent for his work