International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 25, No. 2, April, 2020, pp. 199-206
Journal homepage: http://iieta.org/journals/isi

Channel-Based Encrypted Binary Arithmetic Coding in Wireless Sensor Networks

Balaji Subramanian[1], Harold Robinson Yesudhas[2*], Golden Julie Enoch[3]

[1] Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli 627003, India
[2] School of Information Technology and Engineering, Vellore Institute of Technology, Vellore 623014, India
[3] Department of Computer Science and Engineering, Anna University Regional Campus, Tirunelveli 627007, India

Corresponding Author Email: haroldrobinson.y@vit.ac.in

https://doi.org/10.18280/isi.250207

Received: 22 November 2019
Accepted: 27 January 2020

Keywords:
crypto signature, hash function, code conversion, efficiency

ABSTRACT

The proposed methodology is used for encrypted Joined Compression data attribution which plays a significant responsibility for guaranteed data dependability. Though, the size of the attribution plans to augment at a superior speed as it is delivered from the one end to another end and is executed by a lot of midway nodes. Due to energy and bandwidth boundaries of networks, like growing of attribution size sluggish behind the network and reduces the energy of particular nodes. The proposed Channel-based Binary Encoding Technique is constructed the secured data transmission in Wireless Sensor Networks. A split encoding and decoding procedure discover the syntax components in the regions. As a result, compression of data attribution is a necessary constraint. Related methods like probabilistic node mark methodologies include tall inaccuracy ratios in provenance-recovery. In this paper, the proposed method has the problem and proposes a distributed proposed methodology that achieves a compression ratio higher than that of existing techniques.

1. INTRODUCTION

The source and channel codes are normally divided separately. Thus it appears rational to glance for codes that merge coding to decrease difficulty and interruption [1]. Throughout years, a lot of techniques have developed to attain this goal. For this, arithmetic codes are measured to a great extent for the reason that of its good compression effectiveness [2]. The proposed compression technique has inserted normal symbols as an outlawed Symbol into the coding period to sense errors in recipient. Every time to translate this not at all encoded symbol, it imitates amount of a mistake [3]. In the previous system has used tree search algorithms by the side of with FS to accurate error after detect them. This Paper proposed a MAP inference to recover sound infected series of arithmetic codes [4]. Data compression proposes to minimize the quantity of information consequently that it needs a smaller amount of storage space and a smaller amount of bandwidth of the message controls [5]. Data compression has freshly in progress to be used to diminish the power utilization in numerous wireless systems such as WSNs because wireless broadcast of a bit can necessitate over 1100 times extra power than a particular 32-bit calculation [6]. Several compression methods experience from a trouble that is to describe the redundancy grounds by the source data could be encoded in [7]. It happens at what time a compression method has the choice, at assured steps throughout the encoding procedure; to encode the remaining symbols in many ways of codeword for the particular symbol might be delivered to the decoder and can be decoded properly [8]. In such a situation, the evasion performance of several methods is to encode the particular symbol with the straight codeword and, perhaps, it reduces the complexity [9].

Several methods endure and its alternatives, some alternatives of the Prediction propose a switching compression technique [10], and proposed an algorithm for the production of the remaining codes [11]. The Bit Recycling (BR) method has been utilized to decrease the redundancy [12]. It decreases that kind of repetition by connecting in an assured method so that it is not constantly necessary to choose the direct codeword, but as an alternative, all the suitable codeword are received into description with a quantity of accord involving the encoder method and the decoder method [13]. An additional method to recovering the coding is throughout mathematical mapping. A method of mathematical function through with a logarithmic sphere, the system is unsuccessful to concentrate on the connection among the unique domain [14]. These processes need huge amounts of remembrance and compound performance, with no understandable development in coding effectiveness [15]. Each time a character is coded; two different log tables to notify the log values of PMPS and PLPS should be converting [16]. In addition, a dynamic procedure for understanding the converse log table with the value is necessary to limit the period [17].

Arithmetic coding (AC) is at present accepted in numerous global source coding standards like H.264 and JEPG 2000 as it can give most favourable entropy related coding [18]. Nevertheless, it is extremely responsive to channel noise and is not easy to coordinate while mistakes happen [19]. To trounce this inadequacy, conveniently 2 techniques are accounted in the review to offer mistake exposure ability for Arithmetic Coding, i.e. the prohibited symbol process has been the proposed method called Continuous error detection (CED) for consistent transmission and the marker symbol approach [20]. The error identification is the ability in Arithmetic coding is accomplished by chronological decoding methods to consecutively eliminate the incorrect decoding ways [21]. The implemented joint based channel coding for breadth first and depth first decoding techniques with the pretence parameter was implemented by binary searching related on an empty area. The mistaken decoding areas are unused by the prohibited symbol technique [22]. The greatest application measure for context-related arithmetic coding was accessible with the harmonization indicators. The error-durable Arithmetic Coding appended with a conventional code is performed by repeated decoding technique [23]. The error identification ability is evaluated by the conduction of images larger than an implemented path [24]. A narrative MAP decoding method related to the prohibited symbol, with an elevated litheness in changing the coding rate [25]. It improves the performance of the usual divide technique based on conventional code for error correction capability. The general communication metric is more enhanced when it is successively appended with channel codes by implementing repeated decoding technique [26]. A chronological MAP inference for the CABAC coder was considered, which utilizes an enhanced sequential decoding mechanism to regulate the tradeoffs among complication and competence [27]. To improve the execution effectiveness, arithmetic coding by the prohibited representation could be replicated as a limited state mechanism producing a jagged length lattice code, the unused detachment and the hypothetical mistake alteration performance of that were examined [28]. They proposed an enhanced SISO repeated decoding technique for mistake-removing Arithmetic coding [29].

Arithmetic coding is a structure of unfixed-length mathematical encoding utilized in lossless data compression [30]. Usually, a sequence of letters for example the characters "welcome there" are symbolized with a predetermined amount of bits for every symbol, the same as in the ASCII symbols [31]. There is a succession of characters changed to arithmetic encoding, commonly utilized symbols would be accumulated through smaller amount of bits that happening symbols will be accumulated with supplementary bits, ensuing in smaller quantity bits used in total. Arithmetic coding differs from erstwhile forms of mathematical encoding such as Huffman coding in that moderately than unscrambling the contribution into constituent symbols and substituting each with a cipher, arithmetic coding transmits the complete communication into a solitary quantity [32].

Arithmetic coding endows with a valuable system for eradicating severance in the encoding of information. Arithmetic codes allocate one codeword to every potential data group [33]. The code words demonstrate half-open sub periods of the half-open component period [0; 1), and are articulated by stipulating an adequate amount of bits to discriminate the sub period consequent to the authentic data group starting from each and every erstwhile potential sub periods [34] The most important improvements of arithmetic coding for numerical data solidity are its optimality and its intrinsic severance of coding and representation. The foremost convenience of arithmetic coding is within utmost solidity in concurrence through an innovation representation, or whilst the possibility of solitary occurrence is to a great extent well-built than 1/2. The shortcomings of arithmetic coding are with the intention of it sprints unhurriedly, it is reasonably intricate to execute and in addition to it does not fabricate prefix codes [35].

Arithmetic coding is a well-liked and resourceful lossless compression method to facilitate a progression of resource symbols to a period of integers between the value of 0 and the value of 1 [36]. The encoder fabricates a secret code flow of bits that exceptionally symbolizes the period; the decoder subsequently facilitates the secret code flow to the inventive resource progression. In arithmetic coding, a complete resource progression is associated to a solitary secret code flow. Consequently, a distinct inaccuracy in an arithmetic secret code flow frequently reasons fault inundation at the decoder, reproduction the decoded secret code flow ineffective [37]. Complete resynchronization happens after the decoder preserve accurately establish the original b bits of the secret code flow. In this case the complete innovative resource progression imitated accurately [38]. Prejudiced resynchronization occurs when the decoder only concludes the present period after b bits of the secret code flow [39].

A customized development to arithmetic coding is the largely measurement lengthwise contained by the assortment [0, 1) distributed to every symbol is conserved, but the conventional hypothesis so as to a solitary immediate period is developed for every symbol is disconnected [40]. An explanation recognized to mutually the encoder and decoder is developed to illustrate everywhere the periods are "split" preceding to encoding every innovative representation [41]. The continual splitting has the outcome of together scuttling the periods and shifting their durations, by this means permitting both encryption and compression designate acquired concurrently [42]. When gaps in an arithmetic coder are divided, the exactitude necessitated to recognize a location surrounded by one of the innovative sub periods shaped by the split is simply slightly augmented comparative to conventional arithmetic coding [43]. The splitting generates encryption, the level of that is an occupation of the explicit characteristics of the input and the encoded progression [44].

The explicit contribution of the paper is

i. Channel-based Encrypted Binary Arithmetic Coding technique is used for Wireless Sensor Networks to afford the secured data transmission.
ii. The base station is responsible for providing security for the sensor nodes to deliver the data packets.
iii. The enhanced arithmetic coding is constructed to provide the code conversion within the codes as the message pool.
iv. A split encoding and decoding procedure is implemented to discover the syntax elements in the region of consistent probability allocation strategy.
v. The performance evaluation has been done using the simulator for the proposed technique.

The remaining contents of this paper is constructed as the Section 2 provides the proposed technique with procedures and algorithms, Section 3 evaluates the detailed performance for the proposed technique and to conclude the paper with appropriate clarification and future guidelines.

2. PROPOSED SYSTEM

2.1 System architecture

In common, every stage of the encoding method, excluding for the extremely last, is the equivalent; the encoder has principally:

- The subsequent representation that requires to be encoded
- The present period

- The possibility the reproduction assigns to every one of the different symbols.

The encoder separates the present into sub- periods, every representative a small part of the present period comparative to the possibility of that character in the present circumstance. Either period corresponds to the definite symbol or the period used in the subsequently stage.

4 – Character representation:

- The period for IMPARTIAL probable [0, 0.6)
- The period for OPTIMISTIC probable [0.6, 0.8)
- The period for PESSIMISTIC probable [0.8, 0.9)
- The period for FINISH probable [0.9, 1).

When every secret message has been encoded, the resultant period explicitly recognizes the succession of representations that formed it. Everyone who has the similar finishing period and representation that is mortal used can rebuild the representation succession that should have penetrated the encoder to consequence in that finishing period. It is not required to broadcast the concluding period, nevertheless; it is simply required to broadcast one tiny proportion with the intention of lies inside that period. In particular, it is simply required to broadcast sufficient number of the tiny proportion so that every fraction that begins with individual numbers plunge into the ending period. One benefit of arithmetic coding more than erstwhile comparable techniques of data compression is the expediency of alteration. Alteration is the altering of the possibility boards whereas dispensation of the information. The decoded information equivalent to the innovative information providing the regularity table in decoding is substituted in the equivalent technique and in the equivalent stage like encoding. The management is, frequently, related on a permutation of representations happening throughout the cryptography progression. Adaptive arithmetic coding extensively progresses the compression ratio with immobile procedures.

2.2 Encryption process

The proposed method has three properties:

1. Probability assessment is achieved by way of a finite-state mechanism with a table-based conversion process between 64 probability states.
2. The procedure of interval subdivision is cut down by a pre-quantization of the period range and a successive table look-up action.
3. A split encoding and decoding find a way around for syntax elements or parts having an in the region of consistent probability allocation has been recognized and explained in Figure 1.

Steps involved in the process

Step 1: Binary Arithmetic Coding begin with a Current Interval [Low, High] initialized as [0,1]

Step 2: For Every Symbol, the Arithmetic Coding has classified into Step 3 and Step 4.

Step 3: The Current Interval can be subdivided into subintervals; every possible alphabet symbol is in 1 subinterval. The Symbol's size is directly propositional to the probability of the next symbol.

Step 4: The subinterval with the symbol that actually occurs next to the symbol and make it the new modified current interval.

Step 5: To select all bits to discriminate the modified present interval from all other probable absolute intervals.

Figure 2 demonstrates the Encoder transition full diagram with the states 0, 1, 2, 3, and 4. Each state is communicated with the adjacent states with the binary values of 0 and 1.

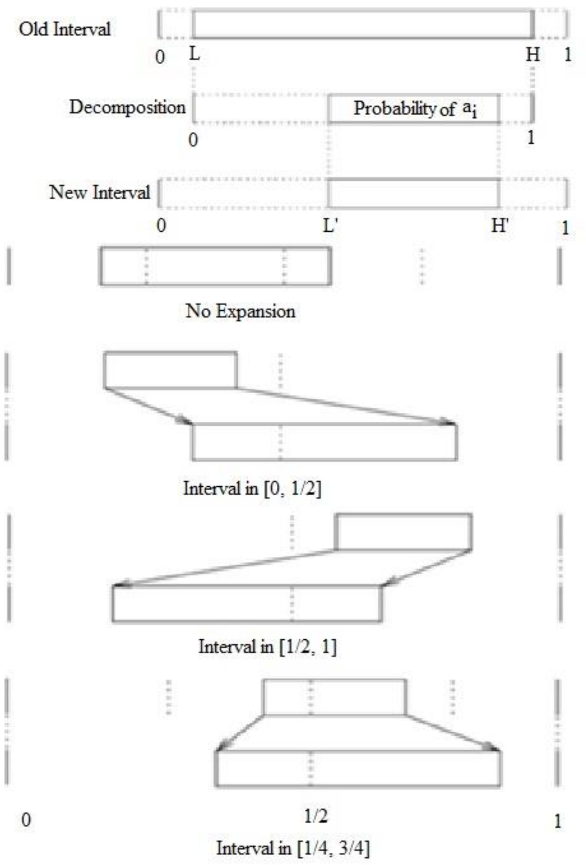

Figure 1. Subdivision of the interval

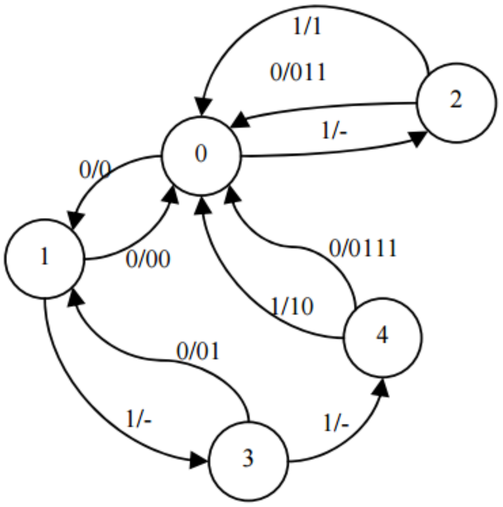

Figure 2. Encoder transition full diagram

2.3 Encryption scheme using binary arithmetic coding

The total amount of bits is helped to encode every character differs regarding to the possibility allocated to the particular character. The minimum possibility characters help a high amount of bit; high probability characters utilize smaller number of bits. The most important thought in Arithmetic coding is to allocate every character an interval. Beginning with the interval [0...1), every interval is separated in a number of subintervals, that its sizes are relative to the present possibility of the equivalent characters.

Wireless network is a compilation of portable stations structuring a provisional network exclusive of the assist of some distributed controller. Interior intimidation owing to developments in the node performance with the purpose of intention for the routing preservation segment of the routing protocol applies a pre-emptive handoff loom to carry on dependable associations by utilizing strait position data. With the same data, paths can be reprocessed while they befall accessible yet again, somewhat being unused. Security parameters are able to direct to anxious announcement in the network. The novel representation can be implemented that established the intolerable component of the nodes and eradicated them. Furthermore, it endows with secure routing system of membership messages among source node and destination node by appending data concerning sender and defends the communication substance by calculating hash function that avoids black hole attacks but also improves the reliability of information.

2.4 Channel-Based Encrypted Binary Arithmetic Coding (CEBAC)

Arithmetic coding demonstrates the message with the basic characters that identifies how to utilize the whole characters in the message pool as one of the main elements. Figure 3 illustrates the sub-interval from the coded formats with the time period is needed for the adjacent character and the output is the first character input value.

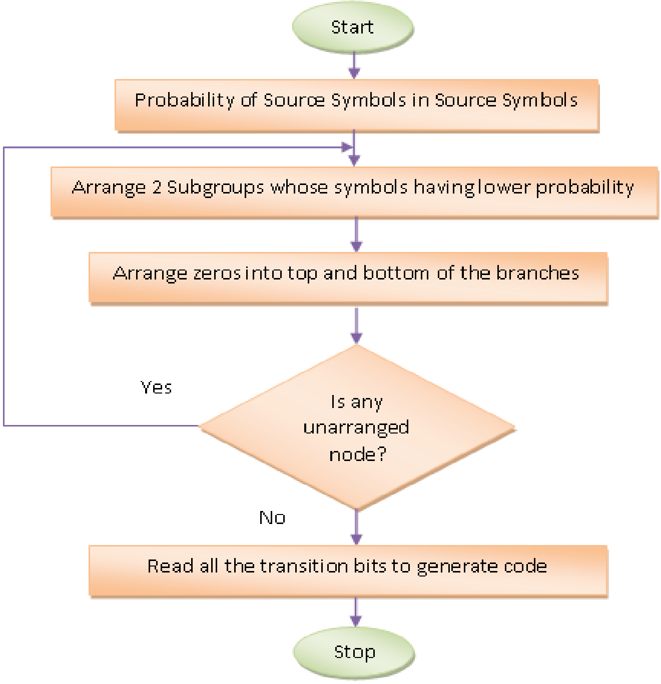
Start
Probability of Source Symbols in Source Symbols
Arrange 2 Subgroups whose symbols having lower probability
Arrange zeros into top and bottom of the branches
Yes
Is any unarranged node?
No
Read all the transition bits to generate code
Stop

Figure 3. Encryption scheme using binary arithmetic coding

Step 1: Read all the sequence of source symbol in to buffer in the form of bits.
Step 2: Discover the centre symbol in the symbol of unique sequence.
Step 3: Split the unique sequence into two same sizes of sub-sequences.
Step 4: Encode the two sub-sequences with their individual probability components and then get 2 secret word sequences.
Step 5: merge the 2 secret word sequences into one word sequence.

```
Input: Msg->Message, K->Key
Encrypt ()
begin
Int1 []=ASCII(Msg)
Split Int1 into Char1 & Char2
a1=IntegerConv (Char1)
a2=IntegerConv (Char2)
str= CreatMat (a1,a2)
split str into str1,str2
Int2 []=ASCII(str1)
Int2 []=ASCII(str2)
BinConv (Int2)
DeciConv(cipher)
 Div(Decimal) Until <2
If <1val >2
Then sub by 1
Else conv(Binary)
Return Cipher
CreateMat (a1, a2)
begin
FormMatrix (k)
s1=Mat [a1, a2]
s2=Mat [a2, a1]
Return s1 & s2
```

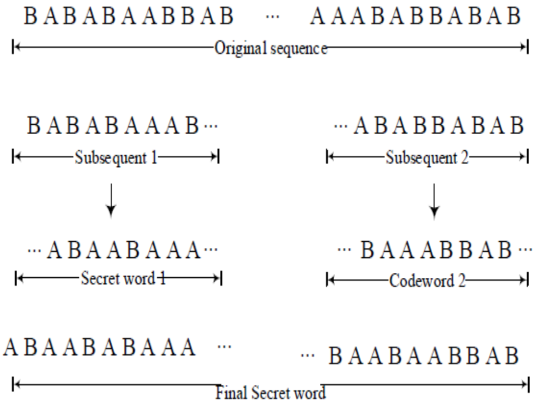

Figure 4. Encoded arithmetic coding

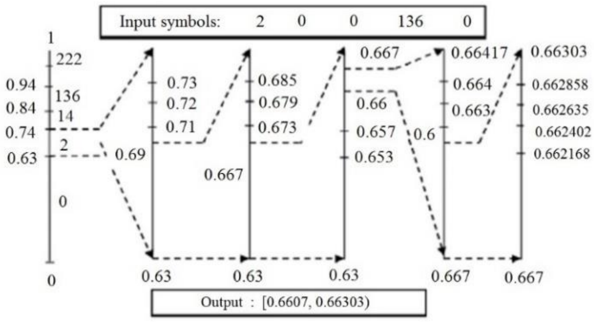

Figure 5. Input and output symbols

The input symbols can be classified into several binary encoded arithmetic coding levels and generate the output 0.6607 and 0.66303. Figure 4 demonstrates the Encoded Arithmetic coding that the original sequence is divided into the Subsequent 1 and 2, the subsequent 1 is converted into Secret word 1, subsequent 2 is converted into the codeword 2. The secret word 1 and codeword 2 is combined to produce the Final secret word. This technique is called as the Encoded Arithmetic Coding.

Figure 5 demonstrates the Input and Output Symbols. The values within 0 and 1 are used to segregate the input and output symbols. Figure 6 illustrates the Topology generation for providing the secured routing in WSNs that the Base station is communicated to the sensor nodes. The communication range is analyzed, based on the communication range the topology is constructed for further processing.

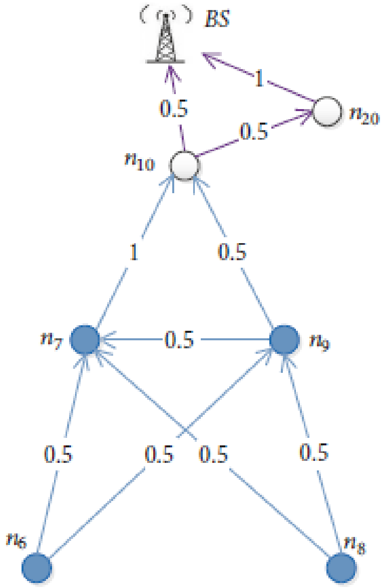

Figure 6. Topology generation in WSNs

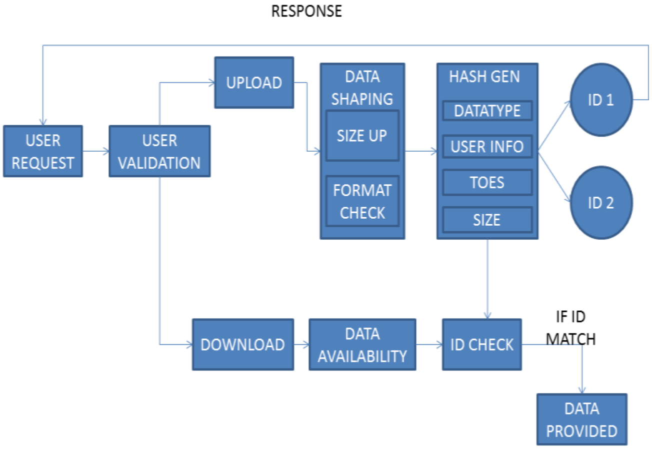

Figure 7. Request generation

The user request is validated and uploaded to provide the data shaping with the format check and the hash key. It is further constructed for implementing the ID checking. If the ID is matched, then the data is provided for further processing through the sensor nodes and it is demonstrated in Figure 7.

The analyzer consists of the IP packet frequently communicated list to save every IP packet frequency which takes the decision for blocking the data packets in the network. The threshold value provides the HTTP request to analyze the IP address within the specified time. The time period is computed in Eq. (1) as

$$\Delta P = p_2(IP_R) - p_1(IP_S) \qquad (1)$$

The activity of the user is recorded within the specified amount of time for which the IP address for communicating to the web browsers. The user activity is computed in Eq. (2).

$$User_{Act}(p_1) = user(IP_c(p_1), REQ) \qquad (2)$$

The data availability is checked with the client request through the IP packet having the address, user details to form the current time with ID details and the seeking permission is granted by the owner with the respective data ID and the process which is illustrated in Figure 8.

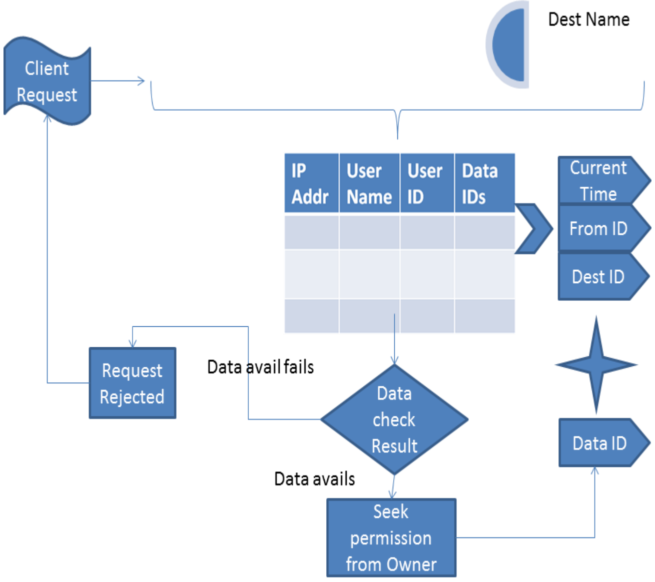

Figure 8. Data availability

3. PERFORMANCE EVALUATION

The performance evaluation is conducted using the simulation through the NS2 simulator. The performance parameters for analyzing the proposed technique are the code conversion and the IP packets are delivered for providing the secured transmission in WSNs. The proposed CEBAC technique is compared with the related methods of MTPKM [11], SIPTAN [13] and XRMAC [40]. Table 1 illustrates the Efficiency of CEBAC and the performance can be calculated based on key length and Hacking Time.

The index of the matrix plays a one of the major role in encryption and decryption. They are taken as row and column. While decrypting, instead of decrypting every term in the cipher, it can just find out the terms to identify the message.

Table 1. Efficiency of CEBAC

Text Length	Secret word		Efficiency CEBAC
	AC	CEBAC	
100	100	107	93.46
200	200	207	96.62
300	300	307	97.72
400	400	407	98.28
500	500	507	98.62
600	600	607	98.85
700	700	707	99.01
800	800	807	99.13
900	900	907	99.23
1000	1000	1007	99.30
1100	1100	1107	99.37

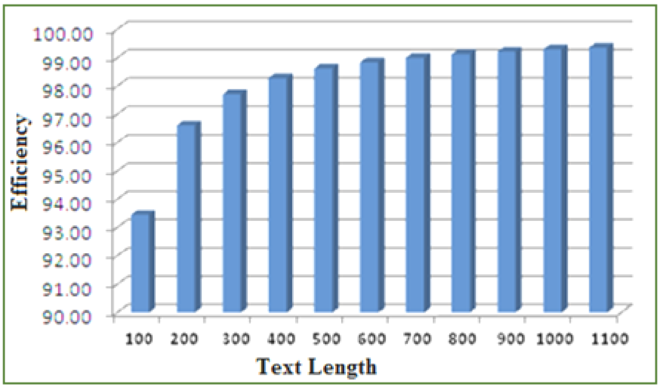

Figure 9. Efficiency with the text length

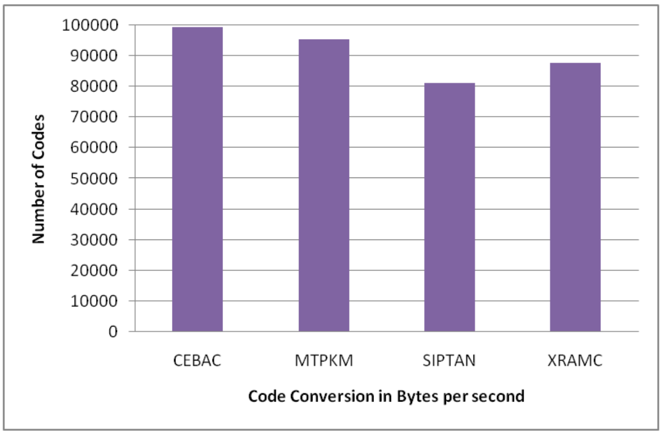

Figure 10. Code conversion

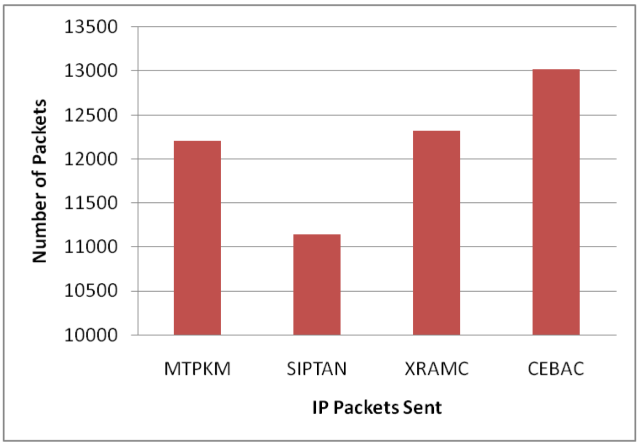

Figure 11. IP packets sent

The Efficiency has improved based on the Text Length of the Security of transferring Secret word from the source node to the destination node in terms of Encryption and Decryption techniques of Cryptograph with Arithmetic code conversion and it is demonstrated in Figure 9.

Figure 10 demonstrates that the code conversion in average within the total amount of codes for providing the secured data transmission. The proposed technique is compared with the relevant techniques to implement the code conversion process and the simulation results demonstrates that the proposed technique has the increased amount of code conversion compared with the related techniques.

Figure 11 demonstrates that the total amount of secured IP packets is delivered for reliable and secured data transmission in WSNs through the sensor nodes. The simulation results proved that the proposed methodology has more amount of IP packets are delivered through the data transmission. The complexity of the code conversion procedure is recorded as the $O(\log N_{co}) + 5$, where N_{co} is called as the cipher conversion value. The efficiency is the important metric for providing the reliable data transmission through the network topology. The sensor nodes are communicated frequently with the base station for data transmission within the communication range. Using that we can refer the matrix to obtain a new symbol. Then the derived index is reversed that is take row as column and column as row. Again we refer the matrix with the new index; another new symbol can be obtained. Now combine the obtained two symbols that collectively form composite symbols.

4. CONCLUSIONS

The system CEBAC implements the cryptographic functions and the text through the secret message counter which is enthusiastically modernized at the normal period by the server. Then the message uses emulate and opposite transformation as an alternative of using simple arithmetic calculation which increases the efficiency and increased the cipher text. The system CEBAC can use the cryptographic techniques of the text not only by the key, but also by the random symbols in the matrix that increases the security than previous system. It doesn’t take more time to encrypt & decrypt the data even it is large. Message is compressed after the encryption to toughen the cryptographic protection. Along with the encrypted value hash value is used to provide integrity. The performance evaluation proved that the proposed CEBAC technique has achieved highest amount of efficiency in spite of code conversion.

In future, to append supplementary cryptographic parameters like digital key, digital fingerprint, to develop a strong security scheme that can’t be persuaded.

REFERENCES

[1] Jahani, A., Khanli, L.M., Hagh, M.T., Badamchizadeh, M.A. (2019). EE-CTA: Energy efficient, concurrent and topology-aware virtual network embedding as a multi-objective optimization problem. Computer Standards & Interfaces, 66: 103351. https://doi.org/10.1016/j.csi.2019.04.010

[2] Lim, H.S., Moon, Y.S., Bertino, E. (2010). Provenance-based trustworthiness assessment in sensor networks. In Proceedings of the Seventh International Workshop on Data Management for Sensor Networks, pp. 2-7. http://dx.doi.org/10.1145/1858158.1858162

[3] Sultana, S., Ghinita, G., Bertino, E., Shehab, M. (2014). A lightweight secure scheme for detecting provenance forgery and packet drop attacks in wireless sensor networks. IEEE Transactions on Dependable and Secure Computing, 12(3): 256-269. http://dx.doi.org/10.1109/TDSC.2013.44

[4] Xu, Y., Wang, J., Wu, Q., Anpalagan, A., Yao, Y.D. (2012). Opportunistic spectrum access in unknown dynamic environment: A game-theoretic stochastic learning solution. IEEE Transactions on Wireless Communications, 11(4): 1380-1391.

http://dx.doi.org/10.1109/TWC.2012.020812.110025

[5] Kim, H., Wen, J.T., Villasenor, J.D. (2007). Secure arithmetic coding. IEEE Transactions on Signal Processing, 55(5): 2263-2272. http://dx.doi.org/10.1109/TSP.2007.892710

[6] Alam, S.I., Fahmy, S. (2014). A practical approach for provenance transmission in wireless sensor networks. Ad Hoc Networks, 16: 28-45. http://dx.doi.org/10.1016/j.adhoc.2013.12.001

[7] Harold Robinson, Y., Balaji, S., Golden Julie, E. (2019). PSOBLAP: Particle swarm optimization-based bandwidth and link availability prediction algorithm for multipath routing in mobile ad hoc networks. Wireless Personal Communications, 106(4): 2261-2289. http://dx.doi.org/10.1007/s11277-018-5941-9

[8] Hussain, S.R., Wang, C., Sultana, S., Bertino, E. (2014). Secure data provenance compression using arithmetic coding in wireless sensor networks. In Proceedings of the 2014 IEEE International Performance Computing and Communications Conference (IPCCC), Austin, TX, USA, pp. 1-10. http://dx.doi.org/10.1109/PCCC.2014.7017068

[9] Madden, S., Franklin, M.J., Hellerstein, J.M., Hong, W. (2002). TAG: a tiny aggregation service for ad-hoc sensor networks. ACMSIGOPS Operating Systems Review, 36(SI): 131-146. http://dx.doi.org/10.1145/844128.844142

[10] Wang, C., Bertino, E. (2017). Sensor network provenance compression using dynamic bayesian networks. ACM Transactions on Sensor Networks, 13(1): 5. http://dx.doi.org/10.1145/2997653

[11] Harold Robinson, Y., Golden Julie, E. (2019). MTPKM: Multipart trust based public key management technique to reduce security vulnerability in mobile Ad-Hoc networks. Wireless Personal Communications, 109: 739-760. https://doi.org/10.1007/s11277-019-06588-4

[12] Zhou, Q., Wong, K., Liao, X., Hu, Y. (2011). On the security of multiple Huffman table based encryption. Journal of Visual Communication and Image Representation, 22(1): 85-92. http://dx.doi.org/10.1016/j.jvcir.2010.10.007

[13] Balaji, S., Rajaram, M. (2016). SIPTAN: Securing inimitable and plundering track for Ad Hoc network. Wireless Personal Communications, 90: 679-699. http://dx.doi.org/10.1007/s11277-016-3187-y

[14] Katti, R.S., Srinivasan, S.K., Vosoughi, A. (2011). On the security of randomized arithmetic codes against ciphertext-only attacks. IEEE Transactions on Information Forensics and Security, 6(1): 19-27. http://dx.doi.org/10.1109/TIFS.2010.2096809

[15] Balaji, S., Golden Julie, E., Harold Robinson, Y. (2019). Development of fuzzy based energy efficient cluster routing protocol to increase the lifetime of wireless sensor networks. Mobile Networks & Applications, 24(2): 394-406. https://doi.org/10.1007/s11036-017-0913-y

[16] Wen, J.T., Kim, H., Villasenor, J.D. (2006). Binary arithmetic coding with key-based interval splitting. IEEE Signal Process. Lett., 13(2): 69-72. http://dx.doi.org/10.1109/LSP.2005.861589

[17] Zhou, J.T., Au, O.C., Wong, P.H.W. (2009). Adaptive chosen-cipher text attack on secure arithmetic coding. IEEE Transactions on Signal Processing, 57(5): 1825-1838. http://dx.doi.org/10.1109/TSP.2009.2013901

[18] Ayyasamy, A., Venkatachalapathy, K. (2015). Context aware adaptive fuzzy based QoS routing scheme for streaming services over MANETs. Wireless Networks, 21(2): 421-430. http://dx.doi.org/10.1007/s11276-014-0801-3

[19] Balaji, S., Golden Julie, E., Harold Robinson, Y., Kumar, R., Thong, P.H., Son, L.H. (2019). Design of a security-aware routing scheme in mobile ad-hoc network using repeated game model. Computer Standards & Interfaces, 66: 03358. http://dx.doi.org/10.1016/j.csi.2019.103358

[20] Kavitha, V., Balaji, S. (2011). ESAC based channel aware routing using route handoff. International Journal on Computer Science and Engineering (IJCSE), 3(3): 1260-1269.

[21] Zhu, Z., Zhang, W., Wong, K., Yu, H. (2011). A chaos-based symmetric image encryption scheme using a bit-level permutation. Information Sciences, 181(6): 1171-1186. http://dx.doi.org/10.1016/j.ins.2010.11.009

[22] Hao, X.C., Gong, Q.Q., Hou, S., Liu, B. (2014). Joint channel allocation and power control optimal algorithm based on non-cooperative game in wireless sensor networks. Wireless Personal Communication, 78: 1047-1061. http://dx.doi.org/10.1007/s11277-014-1800-5

[23] Miao, X.N., Xu, G. (2013). Cooperative differential game model based on trade-off between energy and delay for wireless sensor networks. Annals of Operations Research, 206: 297-310. http://dx.doi.org/10.1007/s10479-013-1354-z

[24] Kusyk, J., Cem, S.S., Umit Uyar, M., Urrea, E., Gundry, S. (2011). Self-organization of nodes in mobile ad hoc networks using evolutionary games and genetic algorithm. Journal of Advanced Research, 2(3): 253-264. http://dx.doi.org/10.1016/j.jare.2011.04.006

[25] Golden Julie, E., Tamil Selvi, S., Harold Robinson, Y. (2016). Performance analysis of energy efficient virtual back bone path based cluster routing protocol for WSN. Wireless Personal Communications, 91: 1171-1189. http://dx.doi.org/10.1007/s11277-016-3520-5

[26] Chen, X.Q., Jones, H.M., Jayalath, D. (2011). Channel aware routing in MANETS with route handoff. IEEE Transactions on Mobile Computing, 10(1): 108-120. http://dx.doi.org/10.1109/TMC.2010.144

[27] Bergen, H.A., Hogan, J.M. (1992). Data security in a fixed-model arithmetic coding compression algorithm. Computers & Security, 11(5): 445-461. http://dx.doi.org/10.1016/0167-4048(92)90011-F

[28] Harold Robinson, Y., Rajaram, M. (2016). A memory aided broadcast mechanism with fuzzy classification on a device-to-device mobile Ad Hoc network. Wireless Personal Communications, 90: 769-791. http://dx.doi.org/10.1007/s11277-016-3213-0

[29] Witten, I.H., Clearly, J.G. (1988). On the privacy offered by adaptive text compression. Computers & Security, 7(4): 397-408. https://doi.org/10.1016/0167-4048(88)90580-9

[30] Bergen, H.A., Hogan, J.M. (1993). A chosen plaintext attack on an adaptive arithmetic coding compression algorithm. Computers & Security, 12(2): 157-167. https://doi.org/10.1016/0167-4048(93)90099-Q

[31] Harold Robinson, Y., Rajaram, M. (2015). Energy-aware multipath routing scheme based on particle swarm optimization in mobile ad hoc networks. The Scientific World Journal, 2015: 1-9. https://doi.org/10.1155/2015/284276

[32] Senturk, I.F., Akkaya, K., Yilmaz, S. (2014). Relay placement for restoring connectivity in partitioned wireless sensor networks under limited information. Ad Hoc Networks, 13(Part B), 487-503. http://dx.doi.org/10.1016/j.adhoc.2013.09.005

[33] Harold Robinson, Y., Balaji, S., Golden Julie, E. (2019). FPSOEE: Fuzzy-enabled particle swarm optimization-based energy-efficient algorithm in mobile ad-hoc networks. Journal of Intelligent & Fuzzy Systems, IOS Press, 36(4): 3541-3553. http://dx.doi.org/10.3233/JIFS-181472

[34] Shamshirband, S., Patel, A., Anuar, N.B., Kiah, M.L.M., Abraham, A. (2014). Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks. Engineering Application on Artificial Intelligent, 32: 228–241. http://dx.doi.org/10.1016/j.engappai.2014.02.001

[35] Duan, J., Gao, D., Yang, D., Foh, C.H., and Chen, H.H. (2014). An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications. IEEE Journal of Internet of Things, 1(1): 58-69. http://dx.doi.org/10.1109/JIOT.2014.2314132

[36] Harold Robinson, Y., Balaji, S., Golden Julie, E. (2019). Design of a buffer enabled ad hoc on-demand multipath distance vector routing protocol for improving throughput in Mobile Ad hoc Networks. Wireless Personal Communications, 106(4): 2053-2078. https://doi.org/10.1007/s11277-018-5925-9

[37] Li, Z., Shen, H. (2012). Game-theoretic analysis of cooperation incentive strategies in Mobile Ad Hoc Networks. IEEE Transactions on Mobile Computing, 11(8): 78-86. http://dx.doi.org/10.1109/TMC.2011.151

[38] Safi, Q.G.K., Luo, S., Wei, C., Pan, L., Yan, G. (2018). Cloud-based security and privacy-aware information dissemination over ubiquitous VANETs. Computer Standards & Interfaces, 56: 107-115. http://dx.doi.org/10.1016/j.csi.2017.09.009

[39] Harold Robinson, Y., Golden Julie, E., Balaji, S., Ayyasamy, A. (2016). Energy aware clustering scheme in wireless sensor network using neuro-fuzzy approach. Wireless Personal Communications, 95: 703-721. http://dx.doi.org/10.1007/s11277-016-3793-8

[40] Rajaram, M., Balaji, S., Jeeva, R. (2013). XRMAC-an extended RMAC scheme to evade hacking by dynamic sizing. 2013 Fifth International Conference on Advanced Computing (ICoAC), Chennai, India. http://dx.doi.org/10.1109/ICoAC.2013.6921944

[41] Ahmad, B., Jian, W., Ali, Z.A., Tanvir, S., Sadiq Ali Khan, M. (2019). Hybrid anomaly detection by using clustering for wireless sensor network. Wireless Personal Communications, 106: 1841-1853. https://doi.org/10.1007/s11277-018-5721-6

[42] Kavitha, V., Balaji, S., Jeeva, R. (2011). RMAC a new encryption scheme for arithmetic coding to evade CCA attacks. 2011 Third International Conference on Advanced Computing, Chennai, India. http://dx.doi.org/10.1109/ICoAC.2011.6165170

[43] Wang, C., Hussain, S.R., Bertino, E. (2016). Dictionary based secure provenance compression for wireless sensor networks. IEEE Transactions on Parallel and Distributed Systems, 27(2): 405-418. http://dx.doi.org/10.1109/TPDS.2015.2402156

[44] Bae, S.H., Howe, B. (2015). Gossipmap: A distributed community detection algorithm for billion-edge directed graphs. Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis, SC'15, ACM, New York, NY, USA, pp. 1-12. https://doi.org/10.1145/2807591.2807668

NOMENCLATURE

ΔP	Time period threshold value
IP_R	IP address for the Receiver
IP_S	IP address for the Sender
p_1, p_2	time period
$User_{Act}$	user activity
$user$	particular user
IP_c	IP count
REQ	Request