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

Ingénierie des Systèmes d'Information
Vol. 25, No. 5, October, 2020, pp. 619-627
Journal homepage: http://iieta.org/journals/isi

A Unique Data Identification System for Wireless Sensor Networks Based on Enhanced Arithmetic Coding

Balaji Subramanian[1], Harold Robinson Yesudhas[2*], Golden Julie Eanoch[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.250509

Received: 22 March 2020
Accepted: 3 June 2020

Keywords:
chosen-cipher text attack, arithmetic coding, wireless sensor networks, data communication

ABSTRACT

In wireless sensor networks, the data transmission provides the source of the data and the details of the forwarding data for the data packet through the based station, to save the energy and maximize the bandwidth while data transmission, the data packet is compressed at every node using the arithmetic coding technique. The encoding and decoding techniques are utilized for providing the secured data transmission. In this paper, the proposed Unique Data Identification System (UDIS) is used to generate the data communication model for user based validation technique. The proposed approach is capable of proxy interpretation for enhancing the server to get the solution for user authentication issues and processing the requests from the user. The performance evaluation is conducted using the network simulator to increase the performance in terms of user load and response time.

1. INTRODUCTION

Wireless sensor networks [1] contains the huge amount of low powered and randomly deployed nodes that are provided to gather the environmental information to detect the information through the base station (BS) with the wireless transmission [2]. The deployment of the amount of application like military monitoring and health based application [3]. The environmental and the huge amount of sensor types are utilized to produce the reliable communication [4]. The significant faults are reduced by removing the error information from the networks [5]. Figure 1 demonstrates the wireless sensor network that consists of 2 layers, layer 1 contains the group of sensor to produce the clustering and it is communicated to the layer 2 that consists of sensor nodes in a group these are connected with the base station to provide the secured and reliable data communication.

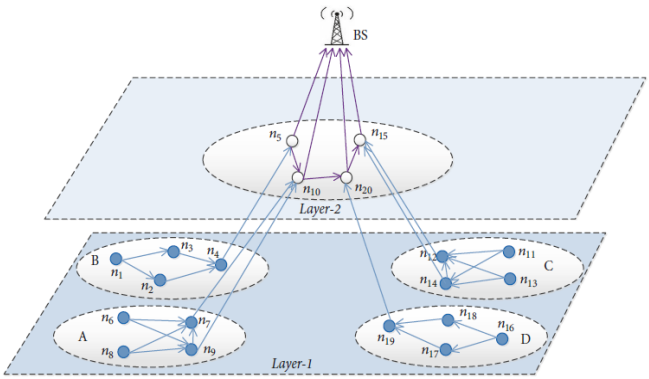

Figure 1. Wireless sensor network

For providing the multi-hop transmission in wireless sensor network, the data provenance of every data packet generates the data attainment and the information are communicated to the base station [6]. It creates the information about the state that the data initiated to generate the operations that guarantees the trustworthiness of the sensor nodes [7]. Whenever the hops are increased to provide the active transmission, then the volume of the data packet increases rapidly [8]. The network has the resource oriented data packet transmission for the computational resource utilization and the nodes are randomly deployed in the network to have the capability for manipulation the large amount of data communication [9]. Normally, the sensor nodes store the battery energy whenever the energy is restricted [10]. The data communication is the important parameter for energy utilization to have the efficient capacity of communicating the data packets [11].

A chosen-cipher text attack (CCA) is a type of attack representation for computation that assembles data by preferring a cipher text and acquiring its decryption below an unidentified key [12]. For an opponent has a possibility to penetrate more recognized cipher texts into the scheme and attain the consequential plaintexts [13]. Since the members of data the challenger can endeavour to improve the unseen secret key utilized for cryptography [14]. A quantity of protected techniques could be conquered below chosen-cipher text attack that is semantically protected below for active attack, but this type of semantic protection can be insignificantly overcome below a chosen-cipher text attack [15]. Untimely descriptions of RSA filling were susceptible to a complicated adaptive chosen-cipher text attack that exposed SSL session keys [16]. Chosen-cipher text attacks with insinuations for a number of self-synchronizing tributary ciphers [17]. Although a crypto scheme is susceptible to

chosen-cipher text attack, generators could be cautious to evade conditions wherein an opponent might be capable to decrypt chosen-ciphertext [18]. This can be additional complicated than it materializes, when partially-chosen-ciphertext can authorize delicate attacks [19]. Furthermore, various cryptosystems utilize the similar method to mark communication [20]. This authorizes attacks that has hashing is not used on the significance to be signed [21]. An improved advancement is to utilize a cryptosystem that is definitely protected below chosen-cipher text attack [22].

The packet is having the secured provenance procedure that each node on packet routing path is appended to the array of fixed length with the group of hah functions [23]. The randomized information structure that supports quick membership functions having the positive values to illustrate the size of the array [24]. The probabilistic cooperation of the sensor nodes having the provenance with a group of data packets are communicated through the same path [25]. Hence the packets need to retrieve to the base station so that the decoded message could be communicated [26]. The size of the transmitted packet is limited to one packet that the highest amount of error while decoding the packet is compared with the other methods of wireless sensor network topology data [27]. The arithmetic coding related technique allocates a probability with combined value for every node with the used path for data transmission [28]. This method generates the probability for the beginning node with coding based interval to be communicated with the other adjacent packets [29]. Every node ID is recorded to provide the interval based arithmetic coding functionality. The data packet can be transmitted to the network path with the probability of the wireless sensor networks [30].

The redundancy reduction method might not reduce the redundancy absolutely because it is based on Huffman codes that cannot include the capability to covenant with codeword of incomplete value and it is embarrassed to produce codeword of essential extents [31]. Furthermore, the enhanced coding has forced further loads to evade situations. Dissimilar Arithmetic coding needs the ability of influencing codeword of partial extents. Additionally, it has magnetized the investigators in the recent days because it is additional dominant and supple than Arithmetic Coding [32]. Accordingly, an innovative method named Arithmetic-Coding-built BR is implemented to determine the fault of HCBR by adjusting it to Arithmetic Coding. A hypothetical investigation demonstrates that ACBR accomplishes ideal while HCBR reaches ideal reprocessing simply in common precise cases. Consequently, considerably improved compression must be obtained by ACBR. The trouble is that it utilizes arbitrary-precision computations, this necessitate infinite sources [33]. Therefore, so as to profit from ACBR in observe, ACBR requires being modified so that it can execute finite-precision computations as an alternative of arbitrary-precision computations. This could construct it professionally appropriate on processors with predictable fixed-size registers.

Conventionally, channel coding is executed individually after basis coding to defend the squashed bits beside channel noise though in the raucous wireless message environment, this conventional method could not guide dependable communication [34]. Consequently, the combined source-channel coding method is a capable policy that endeavours at affording an enhanced communication routine than the conventional disconnect technique [35]. The combined method is understood by continuous decoding method, which permits the replacing of relative soft message within the source codes and the channel codes. Because various implied repentances might remain behind some source coding, it preserves to be engaged in the repeated decoding procedure to additional progress the general transmission routine [36].

Binary arithmetic coding occupies respective partitioning the collection (0, 1) in harmony with the comparative possibilities of occurrence of the two input symbols [37]. The overall length inside the collection (0, 1) distributed to every representation is conserved; however, the conventional hypothesis that a distinct adjacent period is used for every representation is eliminated [38]. An input identified to together the encoder and decoder is exploited to illustrate everywhere the periods are “split” earlier to encoding every innovative symbol [39].

Arithmetic coding recommends enormously elevated coding effectiveness; its diminutive or no safety measures as conventionally executed [40]. To develop a customized design that affords both encryption and compression. The categorization exploits an arithmetic coder wherein the largely duration surrounded by the collection [0, 1) developed to every symbol is conserved, but the conventional statement that a distinct adjacent period is exploited for every symbol is disconnected [41]. Furthermore, successions of transformations are practiced at the contribution and the production of the encoder [42]. The general scheme grants synchronized encryption and compression, through insignificant coding effectiveness penalty relative to a traditional arithmetic coder [43]. Intended for succession of sensible extent, the competence result for acquiring protection is insignificant [44]. The classification consists of an initial transformation movement used to the key progression, arithmetic coding by means of period splitting, and a next transformation movement used to the bits shaped by the coder [45]. An input progression is contribution to an input scheduler who in revolve affords key data to together transformation steps and to the period splitting arithmetic coder [46].

A procedure called renormalization maintains the restricted accuracy from flattering a boundary on the whole quantity of representations that must be encoded [47]. On every occasion, the assortment is abridged to the end where all significance in the assortment splits positive starting numbers and those numbers are delivered to the output [48]. For the numerous numbers of correctness the computer may hold, it is currently managing less than that, so the active numbers are transferred to the left side, and at the forward side, novel numbers are appended to enlarge the collection as extensively as feasible [49].

The major contribution of the paper is

- ✓ A key-based arithmetic coding technique is used to identify the chosen-cipher text attacks.
- ✓ The unique data identification system identifies the anomaly detection through the signature generator technique.
- ✓ The data communication has completed through UDIS system by identifying the invalidate requests.
- ✓ The secure data query processing is implemented by the encryption and the decryption techniques.

The remainder contents of paper are organized as section 2 constructs the proposed system using arithmetic coding technique and the unique data identification system, section 3

implements the performance evaluation and finally, section 4 describes the conclusion of the paper.

2. PROPOSED SYSTEM

Chosen-cipher text attacks that the attacker discovers the cipher text to decrypt previously may not employ the consequential plaintexts to update their option for additional ciphertext. In a generated chosen-cipher text attack, the assailant constructs their cipher text preferences adaptively on the consequence of preceding decryptions. An adaptive chosen-cipher text attack (abbreviated as CCA2) is a generated format of chosen-cipher text attack for an attacker delivers a number of cipher texts to be decrypted, and then uses the results of these decryptions to cipher texts. It is to be renowned from an unresponsive chosen-cipher text attack (CCA1). Figure 2 demonstrates the procedure for establishing the arithmetic coding with the probability technique for the particular message.

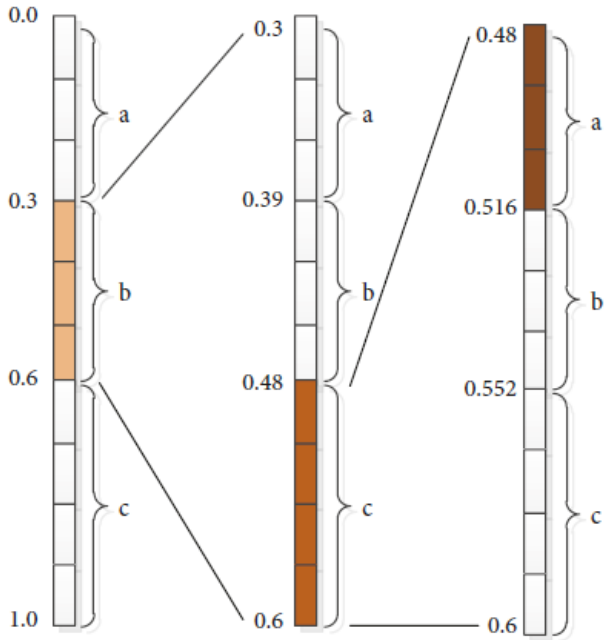

Figure 2. Arithmetic coding procedure

A key-based distance splitting arithmetic coder can be executed with performances close to those created in conventional arithmetic coding and preserve profit from the identical optimizations for hustle, restricted exactitude, etc. The major dissimilarity lies in the repetition of the quantity of periods, which two times the remembrance prerequisite as the superior and minor frontiers of two periods should be sustained. The quantity of impending split conditions is illustrated in ingredient by the exactitude of the solution. The solution should be created to openly recognize split conditions, or it must have the orientation locations in a table known to together the encoder and decoder. Figure 3 demonstrates the structure of the UDIS.

The splitting constructs encryption, the stage of which is an occupation of the explicit characteristics of the solution and the encoded progression. The objective of this attack is to steadily expose data about an encrypted communication, or concerning the security. For public-key systems, adaptive-chosen-cipher texts are generally applicable only when they have the possessions of cipher text flexibility that is, a cipher text can be customized in detailed ways that will encompass an expected result on the decryption of that message. The attack is totally flourishing if the equivalent plaintexts can be construed to acquire some data at all about the fundamental plaintext is stationary measured an attainment.

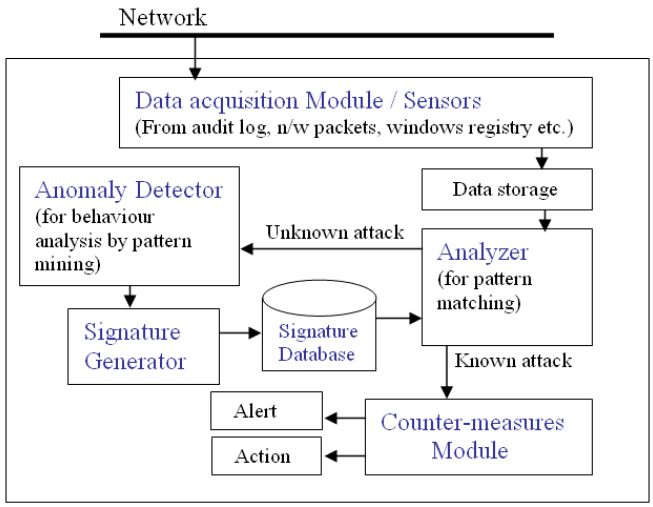

Figure 3. Structure of UDIS

Figure 4 demonstrates the Data communication through UDIS. The total amount of clients can forward the request and the responses have received for every request before the expiry time to identify the invalidate requests by the proxy server. The handle is capable of checking the ID with the training set provides the previous data history, the latest request is in the queue to discard the invalid requests.

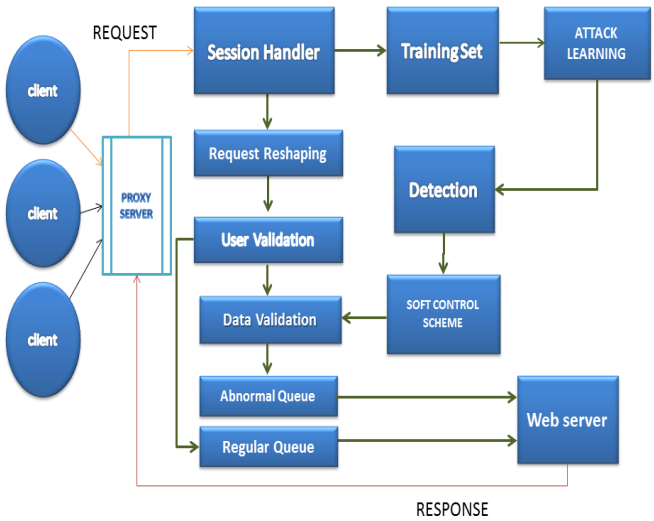

Figure 4. Data communication through UDIS

A cluster signature is a technique that permits a component of a set of secretly indication a communication on behalf of the collection. At this point it is recognized that the sign is completed by an element of that group but could not recognize the entity member. This system has a group manager who is responsible for adding all other members in the group. Besides the group manager has the capability to expose the security and Figure 5 demonstrates the Session

handler procedure. The data can be uploaded or downloaded from the server by the user; the initial process is to provide the request re-shaper, the user generates the request, it is divided into several parts for uploading or downloading. After receiving the data, the proxy server has stopped the process to enhance the authentication.

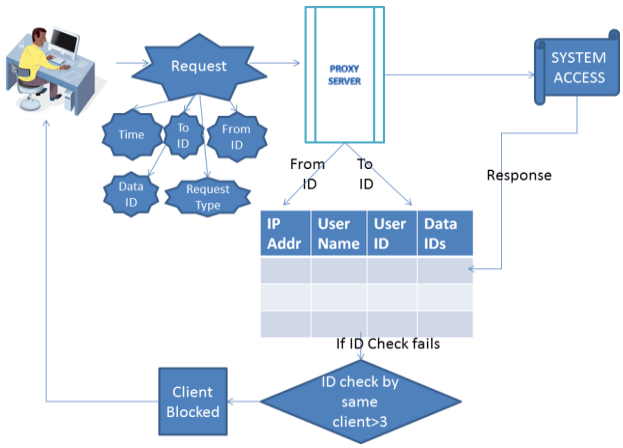

Figure 5. Session handler procedure

For example, if an opponent is to transfer ciphertext endlessly to uphold traffic flow safety, it would be extremely helpful to be capable to differentiate authentic messages from empty values. For the construction of the network, the nodes are shifting from one place to another place. The nodes cannot rely on any infrastructure-based centralized network. Best possible paths differ significantly as a result of altering network topology. In this category of networks the link breakdown is extensive. So, it necessitates focused routing protocol. The reasons of link breakdown and mobile node failures are due to the infrastructure of the mobile nodes and the aggressive inadequate surroundings. A simple security related security model has been implemented that achieves the assessment between routing protocol and optimized security model with similar parameters of performance metrics. Both are network proactive routing protocols. The route to an explicit destination is instantly accessible. Optimized security model has organized over the routing interchanges since it continues just the direct packets of the network that needs to continue the message communication with Topology organization. In static routing system, the routing algorithm encompasses highest bit rate compared to optimized security model. Optimized security model has lower bit rate due to radio abnormality. In source touching network where there be no routes followed by optimized security model could work superior than other related methods. Here, optimized security model must safeguard the packets within the node relatively than reducing packets. This methodology separates the information regarding the optimum path between the network nodes for communication and intermediate nodes. In this technique throughout the situation is used to eliminate the unwanted nodes in the network. The explanation was that the paths are unpredictable, breakdown of the path are short-term whereas the authentic node is still energetic and this technique has huge energy utilization.

ID-based encryption is a kind of public key-based encryption model of a system is several exclusive data regarding the uniqueness of the user. Distinctiveness-related scheme permits any user to produce a public key starting a recognized distinctiveness model like ASCII characters. A confidential user described the Private Key Generator that creates the equivalent personal keys. To manage the Private Key Generator initially distributes a functional kind of keys. Granting the master key to the other user can calculate a public key equivalent to the distinctiveness ID by appending functional public key with the unique value. Figure 6 illustrates the user profile creation.

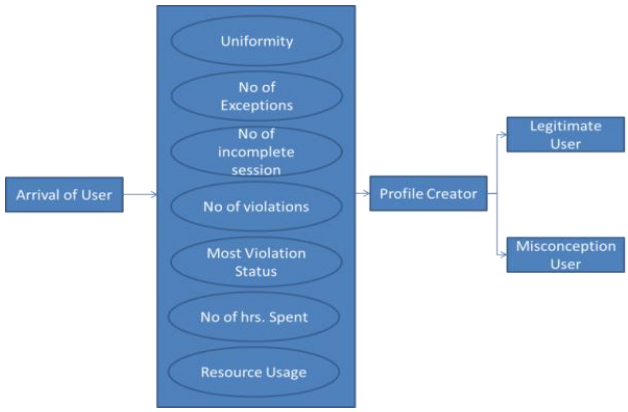

Figure 6. User profile creation

Unspecified routing schemes supply privacy preserving at dissimilar cost. It uses key related technique to attain obscurity and link ability failures that uses network routing where the data communication will be done using the packets were modified using the encryption technique further more time and the data is transmitted from source to the destination. It also produces some key pair or public/private keys to split the links among the packets transmission. It accomplishes link ability failures within the specified packets. It attains routing secrecy that the packets were captioned publicly so the kind of the packet was noticeable by the invaders.

The security related autonomous routing has been used the specific key pairs of public/private keys, it guarantees privacy in communications. The improved technique has the tiny size data packet named TAG was contained through the data packets throughout communication. All the mobile nodes can decrypt with decryption technique that uses TAG; if successful, and then it must decrypt the entire data from the packet, it guarantees the similarity privacy and data security. The invention of key pair for every RREQ in the network is costly. With all probable key pairs the communication needs to be decrypted since there is no links within the RREQ packets and RREP packets. The security related reliable data communication has been provided the disseminated routing which guarantees protection, secrecy, and high reliability. Here, path composition is recognized without endangering the ambiguity belongings. It utilizes lengthy for autonomous intermediate network-based transmission models.

A secure dynamic routing method distributes the secret key through the active network nodes. After distributing that secret key to the users, it utilizes that key to produce a trapdoor dynamic routing to broadcast the secured information. This technique realizes tough protection and secrecy protection. This technique has excellent reliability. The location related secured routing technique attains privacy and safety by building a position based on mysterious routing functionality. This technique applies the cluster signature and estimate aligned with routing overload and permits the source to identify the destination range and determine numerous

recipient nodes in that network and also reveals smallest amount of topology for privacy pleasant and Figure 7 demonstrates the Data query processing.

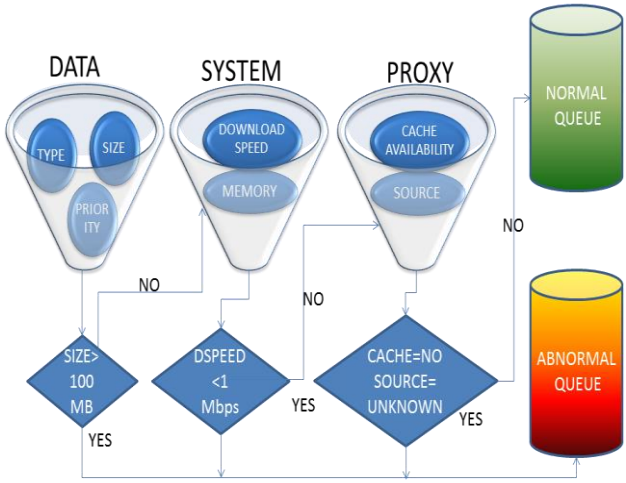

Figure 7. Data query processing

The encryption process is demonstrated as follows:

(1). The numbers are to be sure with in 100. Now the integers are converted into two characters and then into two integers.

(2). Using that two integers as an index, refer the symbol in the matrix. A new symbol will be obtained.

(3). Then the index will be reversed; row as column and column as row. Again referring the matrix, a new symbol will be yield.

(4). Combined the symbols obtained in 2nd and 3rd step to get a new Composite symbol. The Encryption process is described in Figure 8.

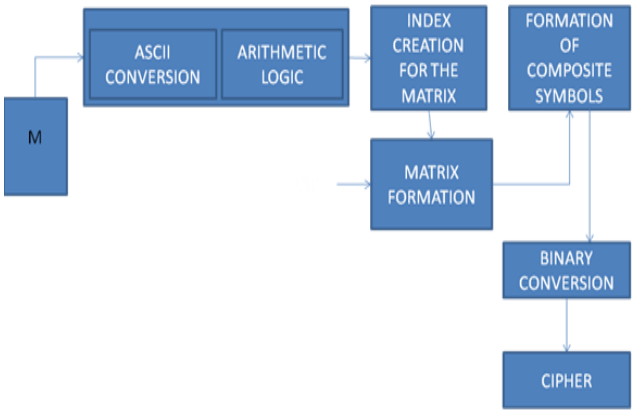

Figure 8. Encryption

After performing the Encryption process, the comprehension process is demonstrated as

(1). The binary value after obtained is converted in to Decimal values.

(2). Then the decimal value is recursively divided by the value 2 until answer below 2.

(3). If the value gets above 1 and below 2. At last append a bit 1 to indicate to subtract the number by 1.

(4). The output obtained is compressed one which should be between 0 and 1. The Comprehension process is described in Figure 9.

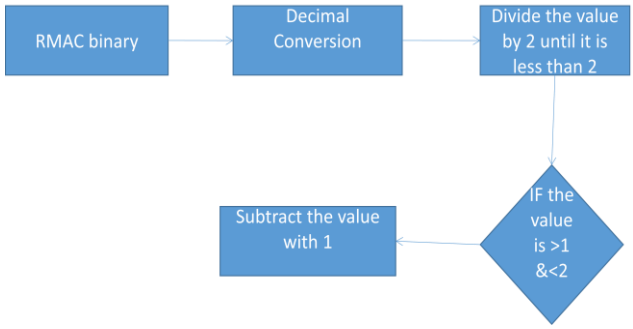

Figure 9. Comprehension

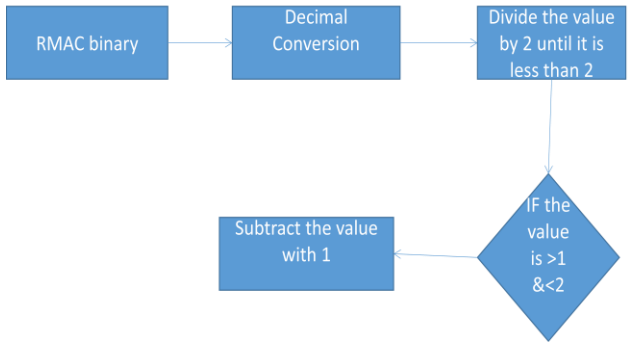

Figure 10. Inverse comprehension

The Inverse Comprehensive is used to check the last bit after completing the encryption and comprehension process.

(1). Check if the last bit if it is 1, then add the output with 1.

(2). Else recursively multiply the value with 2 until the answer is obtained.

(3). Then convert the value into its decimal form.

(4). Then convert the decimal value into its binary form.

The Inverse Compression is described in Figure 10, Decryption process is described in Figure 11.

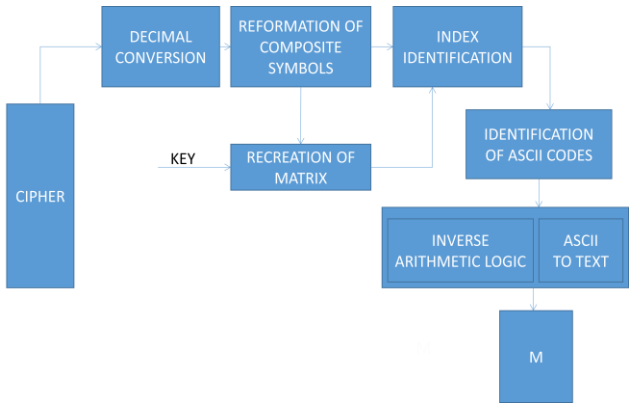

Figure 11. Decryption

The Matrix Formation is performed after the decryption process is successfully completed. The entire process is demonstrated as:

(1). The first row of the matrix will be filled by the symbols except the symbols produced in the generated key.

(2). The second row of the matrix will be filled by the symbols except the symbols produced in the generated key and symbols present in the first row.

(3). Repeat the 4th step till the ninth row is filled. Fill the

last row with a key in shuffled way in order to crosscheck the key in receiver side.

(4). The Matrix Formation is described in Figure 12.

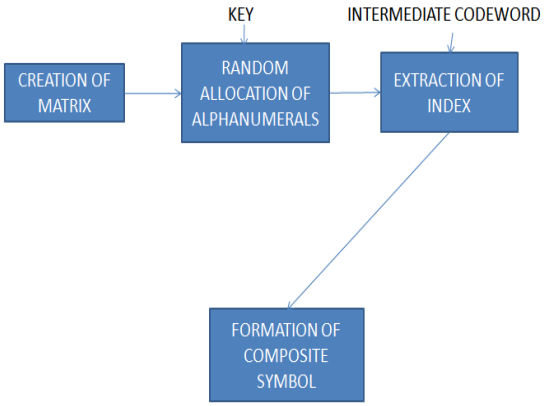

Figure 12. Matrix formation

The arithmetic coding based authentication for providing security for the proposed unique data identification system is having the optimized function in Eq. (1)

$$\alpha = \sum_{i=1}^{N} \beta_i(x) \tag{1}$$

The multiplication value is computed using Eq. (2)

$$\gamma_i = \frac{\alpha}{|x_i|^2} \tag{2}$$

The receiver side authentication is computed using Eq. (3)

$$\gamma_y = \alpha^2 + \sum_{i=1}^{N} \gamma_i |x_i|^2 \tag{3}$$

3. PERFORMANCE EVALUATION

The performance evaluation is conducted using the network simulator NS2 in secured data transmission in wireless sensor networks. The communication range for conducting the simulation is 500 m range. The proposed method is compared with the relevant techniques of SAC [7], SDPCAC [11] and TAG [12].

Table 1. Performance comparison based on time

Data Size	Request Time	Response Time	Mean Time	Security Time
50	2	5	3	3
100	4	10	8	6
150	8	15	13	11
200	12	20	18	15
250	14	25	23	20
300	18	30	28	23
350	21	35	33	28
400	28	40	38	32
450	32	45	43	35
500	40	50	48	38

Table 1 demonstrates the comparison result according to the time parameter that the request time, mean time, security time and response time is generated with the proposed technique.

Table 2. Comparison of UDIS with existing technique

Data Size	Total time			
	SDPCAC	TAG	SAC	UDIS
50	10	15	17	8
100	17	21	24	15
150	24	27	29	21
200	29	33	35	27
250	35	39	42	33
300	42	44	46	39
350	46	48	50	44
400	50	52	54	48
450	54	55	57	52
500	57	60	62	55

Table 2 demonstrates the comparison of UDIS with the existing technique with respect to the data size and the result proves that the UDIS has improved performance.

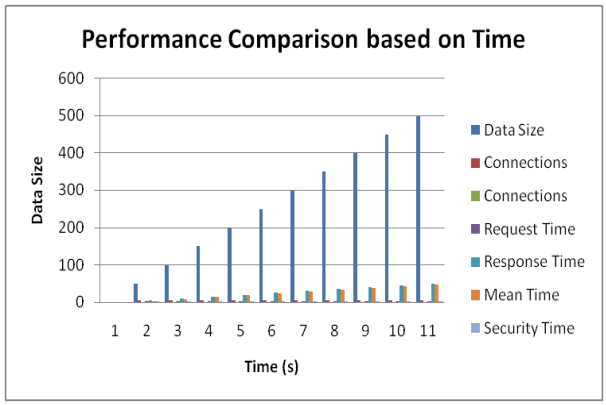

Figure 13. Performance comparison based on time

Figure 13 demonstrates the performance comparison according to the time with respect to the data size that the different kinds of time are analyzed for the proposed UDIS technique such as the request time, response time, mean time and security time. Figure 14 illustrates the data size in spite of time to analyze the performance of the proposed technique. Figure 15 demonstrates Comparative performances of UDIS which is compared with the existing techniques. The performance results prove that the proposed UDIS has the improved performance in terms of user load.

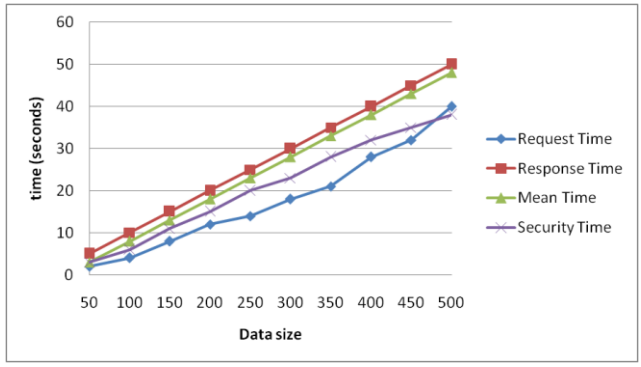

Figure 14. Performance comparison of data size with time

Figure 16 demonstrates the percentage of transmission rate for the proposed UDIS technique compared with the relevant methods and the simulation result shows that the proposed method has the increased amount of transmission rate. Figure 17 illustrates the packets lost while providing the data tranmsission in the wireless sensor networks and the result shows that the proposed UDIS technique has the minimized packets lost compared to the relevant techniques.

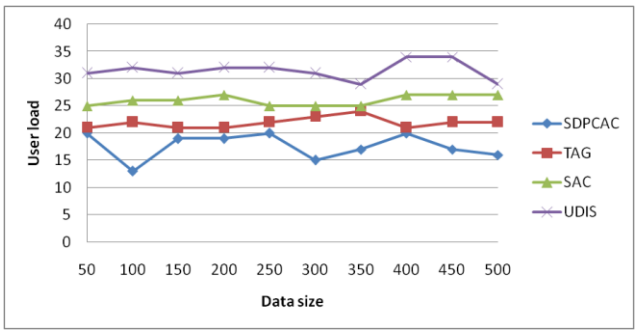

Figure 15. Performance comparison between existing and UDIS

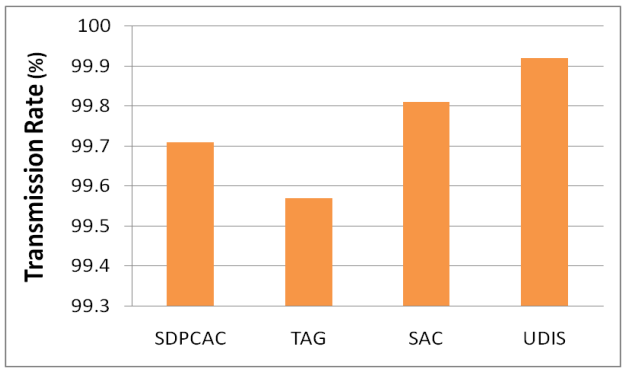

Figure 16. Transmission rate

Figure 17. Packets lost

4. CONCLUSIONS

In a large scale wireless sensor networks, the cluster based arithmetic coding technique and the unique data identification system is implemented successfully for reliable data transmission. The proposed technique is performed well for creating the encoding and the decoding methods and implements the secured data transmission through the base station. The simulation results proved that the proposed technique has the improved amount of efficiency compared with the relevant techniques.

REFERENCES

[1] 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): 256-2691. http://dx.doi.org/10.1109/TDSC.2013.44

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

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

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

[5] 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

[6] Xu, Y.H., Wang, J.L., Wu, Q.H., Anpalagan, A., Yao, Y.D. (2012). Opportunistic spectrum access in unknown dynamic environment: A game-theoretic stochastic learning solution. IEEE Trans. Wireless. Communication, 11(4): 1380-1391. http://dx.doi.org/10.1109/TWC.2012.020812.110025

[7] Kim, H., Wen, J.T., Villasenor, J.D. (2017). Secure arithmetic coding. IEEE Transactions on Signal Processing, 55(5): 2263-2272. http://dx.doi.org/10.1109/TSP.2007.892710

[8] Iftekharul Alam, S.M., 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

[9] Chen, L., Zhang, J., Cai, L.J. (2018). Overlapping community detection based on link graph using distance dynamics. International Journal of Modern Physics B, 32(3): 1850015. https://doi.org/10.1142/S0217979218500157

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

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

[12] 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
[13] 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
[14] Robinson, Y.H., Julie, E.G. (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
[15] 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
[16] 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
[17] Katti, R.S., Srinivasan, S.K., Vosoughi, A. (2011). On the security of randomized arithmetic codes against ciphertext-only attacks. Information Forensics and Security, 6(1): 19-27. http://dx.doi.org/10.1109/TIFS.2010.2096809
[18] Rozum, J.C., Albert, R. (2018). Identifying (un)controllable dynamical behavior in complex networks. PLOS Computational Biology, 14(12): e1006630. https://doi.org/10.1371/journal.pcbi.1006630
[19] Balaji, S., Julie, G.E., Robinson, H.Y. (2019). Development of fuzzy based energy efficient cluster routing protocol to increase the lifetime of wireless sensor networks. Mobile Networks & Applications, 24: 394-406. https://doi.org/10.1007/s11036-017-0913-y
[20] Wen, J.T., Kim, H., Villasenor, J.D. (2006). Binary arithmetic coding with key-based interval splitting. IEEE Signal Processing Letters, 13(2): 69-72. http://dx.doi.org/10.1109/LSP.2005.861589
[21] 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
[22] Balaji, S., Julie, E., Robinson, Y.H., 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: 103358. http://dx.doi.org/10.1016/j.csi.2019.103358
[23] Zhu, Z.L., 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
[24] 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
[25] 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
[26] Kusyk, J., Cem, S.S., Uyar, U., Urrea, M.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
[27] Chen, X.Q., Jones, H.M., Jayalath, D. (2011). Channel aware routing in MANETS with route handoff. IEEE Trans. Mobile Computing, 10(1): 108-120. http://dx.doi.org/10.1109/TMC.2010.144
[28] Bergen, H.A., Hogan, J.M. (1992). Data security in a fixed-model arithmetic coding compression algorithm. Computer & Security, 11(5): 445-461. http://dx.doi.org/10.1016/0167-4048(92)90011-F
[29] Robinson, H.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
[30] Witten, I.H., Clearly, J.G. (1988). On the privacy offered by adaptive text compression. Computer Security, 7(4): 397-408. https://doi.org/10.1016/0167-4048(88)90580-9
[31] Bergen H.A., Hogan, J.M. (1993). A chosen plaintext attack on an adaptive arithmetic coding compression algorithm. Computer Security, 12(2): 157-167. https://doi.org/10.1016/0167-4048(93)90099-Q
[32] Robinson, H.Y., Rajaram, M. (2015). Energy-aware multipath routing scheme based on particle swarm optimization in mobile ad hoc networks. The Scientific World Journal, 2015: 284276. https://doi.org/10.1155/2015/284276
[33] 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
[34] Harold, R.F., Balaji, S., Golden, J.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
[35] 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
[36] 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
[37] Robinson, Y.H., Balaji, S., Julie, E.G. (2019). Design of a buffer enabled ad hoc no-demand multipath distance vector routing protocol for improving throughput in mobile Ad hoc networks. Wireless Personal Communications, 10: 2053-2078. https://doi.org/10.1007/s11277-018-5925-9
[38] 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
[39] 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

[40] Robinson, H.Y., Julie, G.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

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

[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.D., 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, USA, pp. 1-12. http://doi.acm.org/10.1145/2807591.2807668

[45] Shahmoradi, M.R., Ebrahimi, M., Heshmati, Z., Salehi, M. (2019). Multilayer overlapping community detection using multi-objective optimization. Future Generation Computer Systems-The International Journal of Escience, 101: 221-235. https://doi.org/10.1016/j.future.2019.05.061

[46] Mirzaei, S., Soltanian-Zadeh, H. (2019). Overlapping brain community detection using Bayesian tensor decomposition. Journal of Neuroscience Methods, 318: 47-55. https://doi.org/10.1016/j.jneumeth.2019.02.014

[47] Binesh, N., Rezghi, M. (2018). Fuzzy clustering in community detection based on nonnegative matrix factorization with two novel evaluation criteria. Applied Soft Computing, 69: 689-703. https://doi.org/10.1016/j.asoc.2016.12.019

[48] Jonnalagadda, A., Kuppusamy, L. (2018). Overlapping community detection in social networks using coalitional games. Knowledge and Information Systems, 5: 637-661. https://doi.org/10.1007/s10115-017-1150-1

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

NOMENCLATURE

α	encryption value
β_i	arithmetic coding parameter
x	optimized value
N	number of user loads
γ_i	multiplication value
γ_y	receiver side value