International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *10 August 2023* ***Revised:*** *28 September 2023* ***Accepted:*** *20 October 2023*

DAR Model: A Novel Symmetric Key Enabled Security architecture for reliable data transfer in Wireless Sensor Networks

Seelamanthula Sreenivasu[1], Prof.James Stephen Meka[2]
1. Research Scholar, Department of Computer Sciences & Systems Engineering,
A.U.College of Engineering, Andhra University, Visakhapatnam,
Andhra Pradesh, India.
2. Dr. B. R. Ambedkar Chair Professor, Dean, A.U. TDR-HUB,
Andhra University, Visakhapatnam, Andhra Pradesh, India.

Abstract—Security is an indispensable aspect in every transaction happening in the network transmissions. Wireless Sensor Networks are pretty vulnerable to the security attacks. Hence a highly efficient architectural model is very much essential in designing the sensor networks. Cryptographic algorithms play a vital role in providing encryption and decryption to the data being transmitted consequently with which security is offered in an elegant manner. In this paper, a reliable design comprising three pioneering algorithms enabled with symmetric key is architected for secure communication in wireless sensor networks from a node to the base station. The design involves two phases. In the former phase two algorithms which are effective in all perspectives are used for data transmission from node to cluster head and in the latter phase another proficient algorithm is used for communication between cluster head to base station. The three algorithms used are Data Encryption Standard (DES), Advanced Encryption Standard (AES) and RC4. Both block and stream cipher algorithms are used to fine tune the performance; and in addition, the data has been compressed with unprecedented techniques to reduce the burden on encryption. This led to an amazing performance in terms of security parameters.

Keywords-Security in wireless sensor networks, Hybrid techniques in WSN security, Secure and fast transmission in wireless sensor networks, DAR security model.

1. Introduction

The prominence and usage of wireless sensor networks in distinguished domains is accelerating day by day. An equally significant factor that is multiplying in line, is the security aspect. Although the complication is being addressed, still there are problems arising.

A Wireless Sensor Network comprises several nodes that are spread over a region topographically and they sense the environment specific to a task. They transmit the information to the base station which further processes for the defined purpose. Every node is located at some position and has its own energy source that keeps it active. The predominant issue with a sensor node is that it should retain its energy levels to increase its life time. Also, WSNs must deal with different types of data and they must be fault tolerant. Not only the mentioned ones but most importantly quality of service and security are of prime features. Whichever application a WSN is intended for, Security and Energy efficiency are the paramount of performance.

WSN Security is encompassed of four core dimensions namely confidentiality, data availability, integrity, and authenticity. In other words, those are the security goals as defined [1]. Data confidentiality is the property that the data must be kept secret and only the authorized recipients should be able to extract the information. To do so there must be a set of rules in the form of an algorithm that could hide the data from illegitimate users accessing it. Message integrity is the property of data not getting tampered or there is no loss in the data. Changing the original data intentionally by any unauthorized entity is referred to as data tampering and is an impermissible act. Authentication is the process of verifying the credentials and confirming the validity of user so that the user could be designated as an authorized one. Determining whether the data is being sent by a legitimate sender whose credentials match with the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 10 August 2023 **Revised:** 28 September 2023 **Accepted:** 20 October 2023*

designated identity and path is said to be the Sender authentication. Failing to authorize an entity may lead to impersonation which otherwise means that the data may be originated from a duplicate node masquerading the original node due to which wrong data may be sent to mislead the entire application. All the above characteristics are to be retained with appropriate protocols so that right data reaches the right user in right time.

May it be a confidentiality preserving algorithm, an authentication algorithm or integrity preserving algorithm they should be designed in productive manner. Fragile design of protocols results in major loss and make the network delicate.

In this paper all the specifications of a wireless network design are reviewed and our focus is on designing an effective solution for secure transmission of data besides being energy efficient. Although several researchers explored various approaches for providing security, data encryption is considered as an effective and widely used method. Data encryption refers to the conversion of data said as plain text to another form which is said as cipher. In this conversion data gets scrambled from which the original data could be retrieved only by the legitimate user. There are various techniques introduced by distinguished researchers among which Data Encryption Standard (DES), Advanced Encryption Standard (AES), Blow Fish, RC4, RSA, ECC [2][3][4][5][6][7] are few. Each algorithm has its own importance and used in certain applications. Later on few researchers combined the basic algorithms and came up with hybrid algorithms and geared up the performance and strength of security.

When security is incorporated into wireless sensor network, it increases the overhead on a node or cluster head due to which energy becomes expensive and energy efficiency comes down. As security algorithms are instrumental in maintaining data secrecy, their usage is mandatory and at the same time energy efficiency is also crucial. To address this issue, solutions are to be designed in such a way that they provide robust security and at the same time the energy efficiency is preserved to an optimum level.

Computation, memory and power are the resources which are limited in the nodes of Wireless sensor networks. Computational inexpensiveness, memory and power savings make the WSN long-lasting. If the network topology is properly planned, the entire process could be run optimal with which meet the design parameters of a WSN. Clustering is a cogent approach in which the entire operational WSN area is divided into regions called clusters and each cluster is headed by a specific node called as cluster head. Instead of nodes communicating directly to the base station which is at farther distances, they can communicate to their respective cluster heads and in turn the cluster heads communicate to the base station. However, this approach can take a lofty advantage only if clustering is well performed. There are numerous clustering techniques proposed by researchers which exhibited fascinating performance. We also designed an elegant clustering technique [8] using GMM which is deployed in building the network topology. Due to effective clustering the energy efficiency is preserved impeccably.

One more critical feature of WSN security is that the formulated approach must be attack resistant. There are different forms of attacks such as ‘‘Brute Force attack”, ‘‘Sybil Attack”, ‘‘Denial of Service (DoS)”, ‘‘Node Capture attack” and so on [9].

We conceived a wireless sensor network methodology aiming at improving the security and energy efficiency in which a hybrid cryptographic technique is used. In this section the introduction has been given. In the next section related literature is reviewed and the proposed work is mentioned in the subsequent section. Finally, the conclusions are given in the last section.

2. Literature Survey:

Several researchers rendered their contributions in the field of wireless sensor networks and that too specifically on security in WSNs. To fine tune our study we had gone through them among which few were cited here which makes us understand the vitality of the research.

Pooja et.al. in [10] proposed a three phase hybrid algorithm that enforces security in wireless sensor network which is well designed. The three algorithms AES, DES and m-RSA are executed parallel on the data. Here the data is divided into three fragments which are encrypted using the respective algorithm. The results are promising when data size is less compared to others. Moreover energy efficiency and other such factors were not discussed.

Urooj et.al. [11] proposed a hybrid algorithm which is a combination of AES and ECC along with LEACH clustering technique so as to improve the energy efficiency, network longevity and security. Although the approach proved to be resisting side channel attacks and other security threats and even better than various techniques, the time consumption seem to be a bit high.

Mahlake et.al. [12] came up with a lightweight security algorithm to address the resource constraints in IoT networks which is a combination of SIT and SPINS [13] protocols. The proposed Light weight security algorithm LSA, reduced the

power consumption keeping the performance high. SPINS has the Security Network Encryption [14]and the µTESLA protocols as its building blocks for key distribution. However the algorithm is to be implemented and results are to be compared with other approaches.

Sharmila et.al. [15] in their article proposed a hybrid secure key management scheme using ECC and a hash function that generates key pre-distribution keys in wireless sensor networks. So as to achieve mutual authentication among the sensor nodes this hybrid approach is useful and it possesses less computational complexity. Key establishment happens in broadcasting mode and it is done using node identity. Although the scheme offers 30.67% of energy conservation and 13.07% broadcast delay yet it suffers from the latency in determining the rekeying material that preserves the energy consumption and improves the network lifetime.

Sampradeepraj et.al. [16] introduced a cryptographic technique that functions by employing AES and RSA in two phases which are symmetric and asymmetric cryptographic methods respectively. Although the two-phase technique proposed offers better execution time, security is still to be enhanced.

Uras et.al. [17] considering the security level and bit error rate in wireless sensor networks and to provide safety, proposed an efficient protocol which used reserved bits of FC field in Zigbee MAC header in identifying secure vs insecure nodes. They used RECTANGLE, Camellia and Fantomas techniques in devising the scheme and proved its effectiveness by comparing with AES in terms of performance metrics such as delay, power consumption, throughput and memory.

Hudhaifa et.al. [18] proposed a hybrid security scheme intended to provide effective security parameter avoiding computation and memory constraints. Blowfish, MD5 and ECDH are combined to compose the hybrid technique so as to offer security services. They experimented using two computers and obtained the results which exhibited better performance by reducing the text size and decrease in encryption (19.6%) and decryption (41.1%) times when compared to other algorithms.

Heon Jeong et.al. [19] in their research focussed on health care and proposed a secure routing technique SecAODV a heterogeneous WBSN. It operates in three phases namely bootstrapping, routing and communication security. During the first phase, the memory of sensor nodes are loaded with system parameters and encryption functions by the base station. In the next phase the cluster head nodes, basing on various parameters such as distance, residual energy, hop count and quality of the link compute their degrees and broadcasts the route request message. In the last phase the intra cluster communications happen and the cryptographic algorithm implemented is intended to provide security. Even though the proposed technique performs better in terms of delay, energy efficiency, throughput, packet delivery and loss rates; there is a room for improvement by adding an authentication layer to prevent from designated attacks. Also, artificial intelligence techniques could be employed to improve the performance further.

Kumar [20] proposed an efficient and secure user authentication protocol for Wireless sensor networks which employed a hash function. The protocol's security level is tested using AVISPA and its performance was analyzed in terms of various parameters. It is also tested in various attack formats. Nevertheless, the protocol could be further improved in reducing the computational as well energy consumption costs and could be deployed in various applications.

Ebadati et.al. [21] proposed a novel hybrid secure approach for WSNs which first encodes the data, splits the data into blocks and applies encryption, authentication and integrity related algorithms in two stages. Later the encrypted blocks are combined and forwarded. The algorithms used are RSA, ECDH, SHA 256 and ECDSA. Eight algorithms are used in performing these tasks which offered promising results in terms of security. But the approach consumed more time and the authors as part of their future work mentioned to make use of compression algorithms which reduces not only storage but also time and energy during the transmissions.

Kumar et.al. [22] and **Nidarsh et.al.** [23] made their efforts in working with chaotic maps in providing security for wireless sensor networks. The former research team improved a user authentication scheme in which the secret keys are made using large integers rather than large prime numbers which made the operations faster. Cryptanalysis is performed with various attack relays and confirmed that the scheme is attack resistant. Further it could be improved in terms of computational and storage costs. The latter team proposed a chaotic encryption with LEACH algorithm which resulted in less power consumption and security.

Rawya et.al. [24] proposed a notable hybrid technique that provide security with minimized key maintenance for image data in wireless sensor networks. They used AES and ECC for encryption, XOR-DUAL RSA for authentication and MD5 for maintaining data integrity. All the performance measures are satisfactory and the technique is robust to attacks in case of image encryption. They have done correlation analysis of the images before and after encryption to determine the efficiency

of the application. However there lies a scope for improvement in terms of other parameters such as time consumption energy efficiency and so on.

Ren et.al. [28] using RSA and DES formulated a hybrid approach for Bluetooth communication. Their approach infused security in the communication besides the technique being simple and efficient.

Subasree et.al. [26] proposed a hybrid technique which encompasses ECC, Dual-RSA AND MD5 algorithms to incorporate confidentiality, authentication and integrity respectively.

Murugan et.al. [25] proposed a security algorithm which maximizes key lifetime and security levels besides reducing power consumption level.

The above cited contributions reveal that wireless sensor network researchers made their efforts in accelerating the technology to an advance level not only in theoretical dimension but also in various applications. Also, security plays a lead role in making the WSNs widely useful. However, the contributions left an impression that there is a scope for enhancing the performance in various facets. Most importantly AES seems to be an efficient algorithm due to its capability and its inclusion is unavoidable in most security applications of wireless sensor networks. Security applications with single algorithm may not yield good results. Hence hybrid techniques are the prevailing ones. The design aspects of the techniques indicate that the security parameters such as confidentiality, integrity and authentication must be preserved. And at the same time the challenges of sensor networks viz. energy and other resource constraints, network life time, inexpensive computational complexity must be addressed. In [21] it is mentioned that usage of effective compression algorithms may reduce time consumption which leads the network to be energy efficient. Considering all the leads for an efficient algorithm we made our efforts towards our proposed contribution which is presented in the next section.

3. Proposed work:

Security is an indispensable aspect in every transaction happening in the network transmissions. Wireless Sensor Networks are quite vulnerable to the security attacks. Hence a highly efficient architectural model is very much essential in designing the sensor networks. Cryptographic algorithms play a vital role in providing encryption and decryption to the data being transmitted consequently with which security is offered in an elegant manner. As the third part of architecting our wireless sensor networks, secure design is of major concern in which three algorithms are used. Both block and stream cipher algorithms are used due to which the potentiality has been improved. The three encryption/decryption algorithms Data Encryption Standard (DES), Advanced Encryption Standard (AES) and RC4 are the part of trio model "DAR" proposed in this paper.

3.1 Architecture:

The model's functionality comprises two phases. In the primary phase, encryption is applied on the data being transmitted from sensor nodes to cluster heads and in the further phase, the encrypted data in the earlier phase would again be encrypted and transmitted from the cluster head to the sink. Moreover, the data which is being encrypted undergoes phase wise compression so that the data transmission becomes more secure and fast. The architecture of proposed security model is as shown in figure 1. The application of 2 phase compression mechanism and its advantage had already been articulated in our earlier research article [30]. In extension to the study made, we performed mentioned efforts and the network diagram is as shown in figure 2.

It could be observed from fig that the first phase activities happen in a node and then the data is transmitted to Cluster head. In the cluster head the second phase activities take place after which the data is transmitted to the base station. In the base station the reverse actions of phase 1 and 2 are applied with which the original data is retrieved. During the first phase the data which is to be transmitted is first divided into two parts in which the first part contains $1/3^{rd}$ of bits (r bits) to be transmitted and the other part contains $2/3^{rd}$ (n-r) of bits. The first part is encrypted using **D**ES while the other part is encrypted using **A**ES. On the other hand, the data from cluster head to base station is encrypted using **R**C4. Decryption happens at Base station.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *10 August 2023* ***Revised:*** *28 September 2023* ***Accepted:*** *20 October 2023*

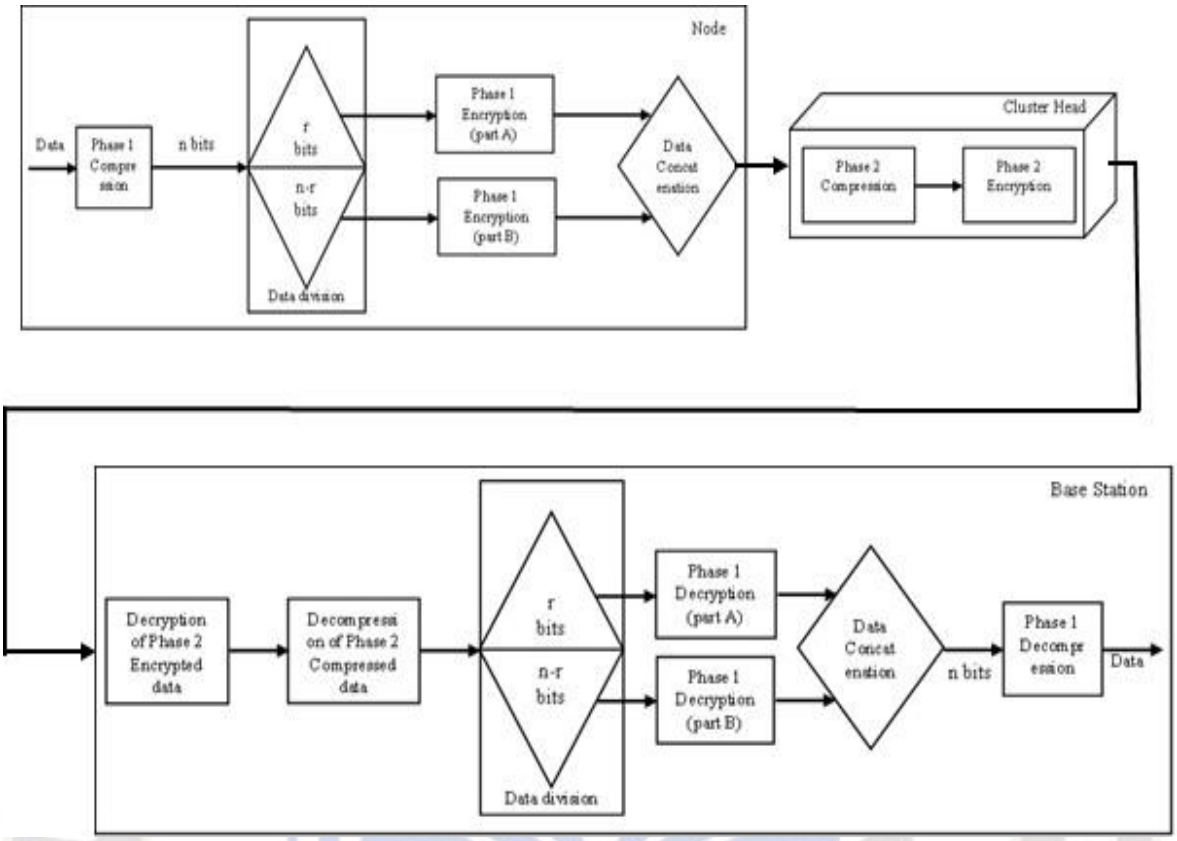


Fig 1: Architecture of the proposed DAR model

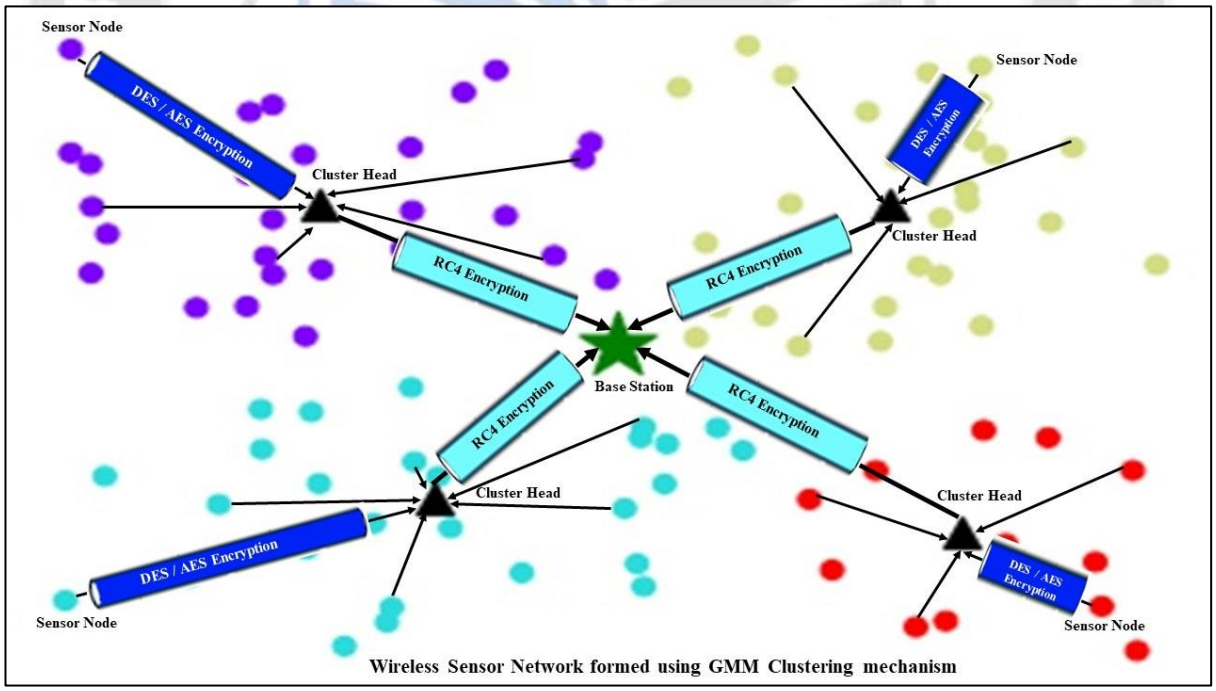


Fig 2: DAR Security WSN diagram

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 10 August 2023 **Revised:** 28 September 2023 **Accepted:** 20 October 2023*

3.2 Encryption and Decryption processes in DAR model:
The security process involves encryption & decryption as well compression & decompression processes at different levels which are described below. The data input originates in the node and supplied as X_k for the further steps.

Encryption at Node level (between node and cluster head):

$W_k \leftarrow FELACS_{N_{jk}CH_k}(X_k)$
$b_k \leftarrow$ num_bits(W_k)
if ($b_k = 3m$) //($\because m \in z^+$)
{
$b_{DES} = b_1$ to $b_{k/3}$
$b_{AES} = b_{k/3+1}$ to b_k
}
else if ($b_k = 3m-2$)
{
$b_{DES} = b_1$ to $b_{k/3+1}$
$b_{AES} = b_{k/3+2}$ to b_k
}
else
{
$b_{DES} = b_1$ to $b_{k/3-1}$
$b_{AES} = b_{k/3}$ to b_k
}
$C_{k_1} \leftarrow E_{DES_{k_1}}(b_{DES})$
$C_{k_2} \leftarrow E_{AES_{k_2}}(b_{AES})$

Encryption at Cluster head level (between cluster head and base station):

$Y_k \leftarrow LZMA_{CH_kBS}(C_{k_1} || C_{k_2})$ // LZMA Compression of $C_{k_1} || C_{k_2}$
$C_{k_3} \leftarrow E_{RC4_{k_3}}(Y_k)$

Data Retrieval at Base station:

$Y_k \leftarrow D_{RC4_{k_3}}(C_{k_3})$
$C_{k_1} || C_{k_2} \leftarrow decompress_{LZMA}(Y_k)$ // LZMA Decompression of Y_k
$b_{DES} \leftarrow D_{DES_{k_1}}(C_{k_1})$
$b_{AES} \leftarrow D_{AES_{k_2}}(C_{k_2})$
$W_k \leftarrow b_{DES} \parallel b_{AES}$
$X_k \leftarrow decompress_{FELACS}(W_k)$ // FELACS Decompression

In the above algorithmic procedures, firstly X_k is compressed using FELACS and produces X_k as the output of the message which is to be sent to the base station. Now the compressed data is divided into two parts (1/3rd and 2/3rd), among which first part is encrypted with DES and the next part is encrypted with AES; in the next step respective number of bits are identified for each encryption algorithm. b_{DES} & b_{AES} are the data supplied to DES & AES respectively for which C_{k_1} & C_{k_2} are outputted as ciphers. The ciphers are next compressed in the node using LZMA technique which output C_{k_3}. Upon receiving C_{k_3}, Cluster head further encrypts the received data using RC4 algorithm which outputs C_{k_3} as the cipher obtained. This cipher shall be sent to the base station. At base station the reverse of the above procedures i.e., Deciphering and Decompression takes place so that the original input messages are obtained. The terms $E_{DES_{k_1}}$, $E_{AES_{k_2}}$, $E_{RC4_{k_3}}$, $D_{DES_{k_1}}$, $D_{AES_{k_2}}$, $D_{RC4_{k_3}}$ represents the Encryption and Decryption procedures using DES, AES, RC4 with the keys k_1, k_2 and k_3 respectively.

3.3 Results and Discussion:
With the infused additional flavour of security by introducing "DAR" hybrid algorithm to the existing data compression proposed [8] in our earlier module of our research, we could derive three benefits security, speed and energy efficiency which are detailed in this sub section. The Clustering, Cluster head selection, Compression and Security algorithms are implemented in an i5 machine using python.

a) Security:
The DAR model is designed in such a way that the encryption provides high security. DAR model is a combination of three algorithms viz., Data Encryption Standard (DES), Advanced Encryption Standard (AES) and RC4. Among these algorithms, DES & AES are block ciphers while the RC4 is a stream cipher. To bring novelty in the model, the block cipher algorithms are used in one phase and the stream cipher algorithm is used in another phase. While transferring the data from node to cluster head block ciphers are used. It makes the data strong and as stream cipher is more advantageous than block ciphers, RC4 is employed to transfer data from cluster head to base station which surges the security. RC4 offers fast and strong encryption besides DES & AES being the potential ciphers. Thus, the security offered by the trio becomes robust.
The performance of proposed model "DAR" proves to be superior when compared to few hybrid algorithms used in providing security for wireless sensor network transmissions. The performance is depicted in table 1.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 10 August 2023 **Revised:** 28 September 2023 **Accepted:** 20 October 2023*

Table 1: Comparison of various security parameters with other contributions

Hybrid algorithm proposed by	Algorithm/s used	Encryption strength	Confidentiality	Authentication	Data Integrity
Subasree et.al. [26]	Dual RSA, ECC & MD5	++	+++	++	+
Kumar et.al. [27]	AES & ECC	++	++	++	+
Ren et.al. [28]	DES & RSA	++	++	+	+
Ramaraj et.al. [29]	AES, RSA & SHA 512	++	++	++	+
Shabana et.al. [11]	AES & ECC	++	++	++	+
Proposed	DES, AES, RC4, SHA 256 & HMAC	+++	+++	++	++

+, ++ and +++ indicates the feature offered and levels of strength of the feature

Encryption strength, confidentiality, Authentication and Data integrity are the measures of strength of any Security model. It could be observed from the above table that among the hybrid algorithms proposed by various researchers, there are Symmetric and Asymmetric encryption algorithms. Symmetric algorithms offer confidentiality to most extent while authentication and data integrity to moderate extent. On the other hand, asymmetric algorithms provide confidentiality and authentication mostly and moderate data integrity. Usage of Hash algorithms and Authentication codes improves the data integrity and Authentication. When compared to the other algorithms, the proposed algorithm has three symmetric algorithms, a hash algorithm and an authentication code due to which the encryption strength goes high consequently the confidentiality. In addition, the authentication and data integrity offered is high. Due to its features the proposed security model seems to be robust and substantial in terms of efficacy.

b) Efficient Key Management:

Keys play a major defensive role in providing security for wireless sensor networks. In [31] various key management schemes were discussed and among the discussed ones, the features of Energy Efficient Dynamic Key Management technique seem to be promising and similar featured key management process is followed in this article. The keys involved in proposed security model are made up of nimble and computational inexpensive featured attributes and operations, the key management is energy efficient as well dynamic in nature. The key computations are depicted below.

DES_{K_1} = $IV_1 \oplus T \oplus D$

AES_{K_2} = $IV_2 \oplus IP$

$RC4_{K_3}$ = HMAC(SHA256(IV_3, nonce,))

IV_1, IV_2, IV_3 – Initial Vectors

T – Time

D - Date

IP – IP Address

The three keys K_1, K_2 and K_3 used for the respective algorithms DES, AES and RC4 are designed in a simple and effective manner. K_1 is generated using three values; a 64 bit random value, the date and time of the encryption which are XORed and is applied to only one part of data. AES on the other hand uses the key value K_2 built using an XOR operation applied on 128 bit random value and IP address of the node. This AES algorithm is used to encrypt remaining part of the data. Depending on the length of IP address the same IP value is concatenated multiple times to reach the length 128 bit. To be more clear, if the length is 32 bit (IPv4), 4 times the concatenation happens while if the length is 128 bit (IPv6) no concatenation is required. For the third algorithm RC4 which is used to further encrypt the previously encrypted data using DES & AES, the key K_3 is used in which an initial random fixed value and a dynamic nonce are generated and supplied to HMAC which operates with SHA 256 digest. From the above it could be understood that the key management is computationally inexpensive and dynamic with which we can uphold that the proposed model constitutes Efficient key management.

c) Attack resistance:

Due to various algorithms being used, the overall key size is between 232 bits to 2240 bits. Hence launching brute force attack is highly difficult. As the node's IP address is involved in key formation, sensor node's anonymity attack, password guessing, and impersonation attacks [20] are also at a distance. Due to the usage of compression and encryption mechanisms Traffic analysis attack and routing attacks such as spoofed routing attack, sybil attack, so on could be resisted.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *10 August 2023* ***Revised:*** *28 September 2023* ***Accepted:*** *20 October 2023*

d) Speed:

Another vital facet of wireless sensor network is the speed at which data is transmitted to the base station. Usually, the data originates at a sensor node and needs to be transmitted to the base station. If clustering is implemented then the data must first be transmitted to Cluster head and from cluster head the data shall be transmitted to the base station. Although clustering is a overhead, for efficient and organized transmission the solution is acceptable. Undeniably Security is an essential factor in data transmission; but if incorporated it consumes time.

To handle this, efficient techniques must be chosen in providing high security with minimal time consumption. Such optimal solutions could be devised only with judicial implementation. In this research as compression and encryption are jointly ventured, both security and speed are preserved. In providing a secure solution the placement of encryption algorithms has been wisely done.

Security is provided by combining DES, AES and RC4 algorithms as described. The time complexity of all the three algorithms which are symmetric ciphers is O(n). The compression algorithms also have an order of time complexity O(n). Hence the overall time complexity of the proposed hybrid approach seems to be O(n).

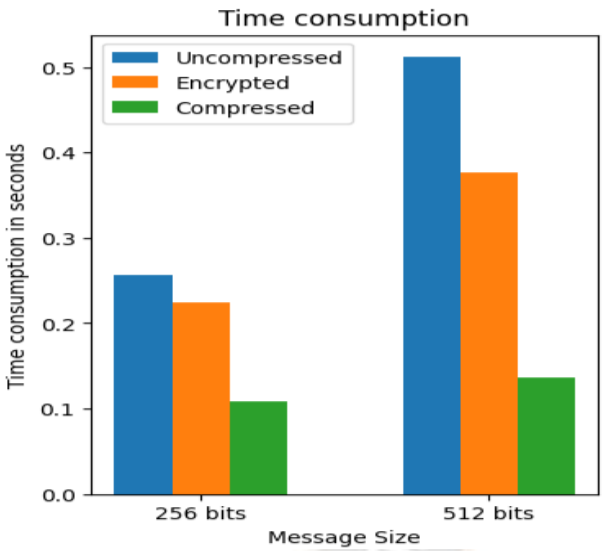
As the node handles less data when compared to a cluster head, two algorithms are used to encrypt the data between node and cluster head. Between cluster head and base station the data is encrypted using one algorithm which is simple, strong and efficient. The former two algorithms used are DES & AES which consumes more time than the later used algorithm RC4. This led to an innovative secured combination preserving the speed. As encryption alone would consume more time, data is compressed and submitted to the encryption so that the data which is to be encrypted becomes less consequently the encryption time gets reduced. This procedure is implemented in both the phases and it significantly impacts the time consumption which is depicted in table 2 and figure 3.

The time consumption for processing data at various stages could be observed from the above presentation which makes us understand that the uncompressed (UC) data takes much time, Compressed (C) – Encrypted (E) – Encrypted (E) data consumes less time than UC. The data which is encrypted after compression followed by compression and encryption (C-E-C-E) consumes less significant time. Similarly, the time consumption of UC and C-E-C-E data for various lengths of data is depicted in table 3 and figure 4 which reveals the same.

Table 2: Comparison of Time consumption (seconds)

Type of data	Time consumption for 256 bits	Time consumption for 512 bits
Uncompressed data (UC)	0.256	0.512
Encrypted data (C-E-E)	0.224	0.376
Compressed data (C-E-C-E)	0.108	0.136

Figure 3: Time consumption for uncompressed, encrypted and compressed data



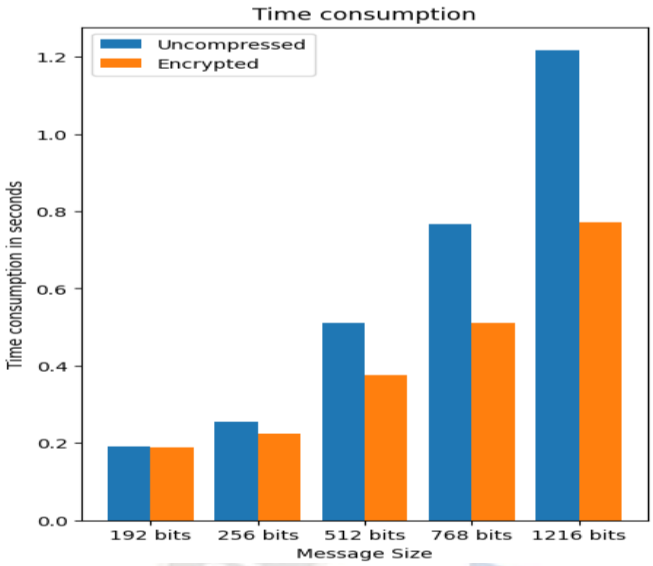
It is observed from the above figures that both Compression and Encryption when jointly used is offering significant results. Moreover, the proposed model DAR when compared with contributions of other researchers performed extremely well in terms of time consumption. The results are presented in the table 4 and figure 5.

Table 3: Encryption time comparison (sec)

Data length (bits)	Uncompressed data (UC)	Compressed data (C-E-C-E)
192	0.192	0.188
256	0.126	0.224
512	0.512	0.376
768	0.768	0.512
1216	1.216	0.772

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *10 August 2023* ***Revised:*** *28 September 2023* ***Accepted:*** *20 October 2023*

Figure 4: Uncompressed vs Compressed -encrypted process time comparision



e) Energy Consumption:

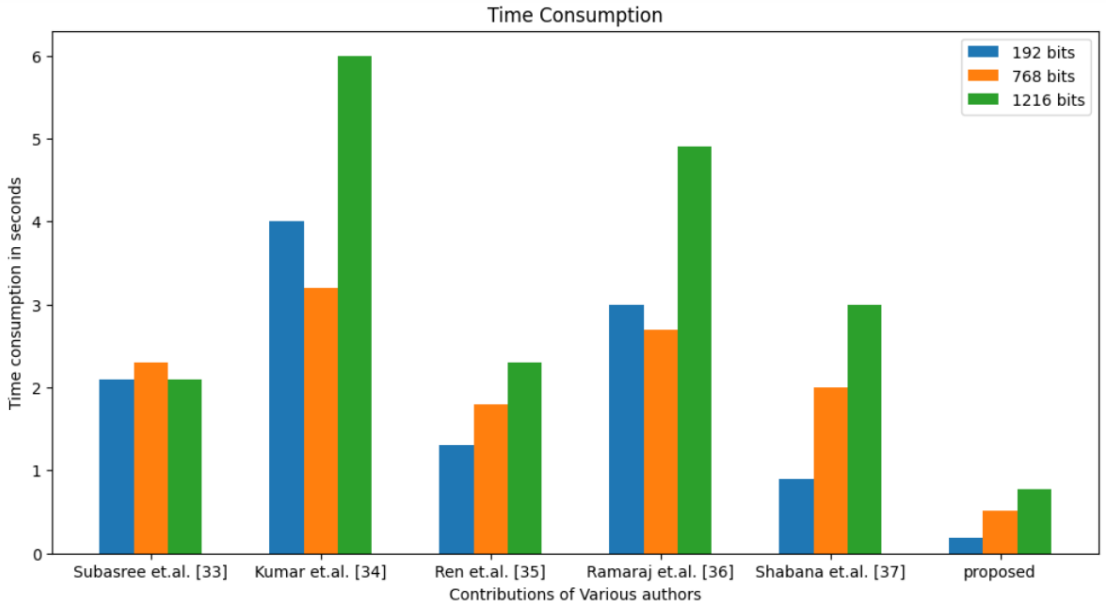
For longevity of a sensor node, energy of the node is a prime factor. In other words, Energy consumption for various activities of a node determines the life of a node due to which the performance of a wireless sensor network becomes influential. The prudent choice of algorithms for a node subsequently the network activity impacts the energy efficiency. The security model implemented in this research offered security as well it seems to be energy efficient. It could be observed from the following results depicted in table 5 and figure 6 that Energy consumption is promising.

The security model is experimented and the energy consumption for various lengths of data being encrypted are considered. The above results depict that the model yields in pleasing performance in terms of energy efficiency. Not only energy efficiency but also its performance is remarkable in terms of security, key management and time consumption.

Table 4: Encryption times of various contributions

Hybrid algorithm proposed by	Time for Encryption – in sec (192 bits)	Time for Encryption – in sec (768 bits)	Time for Encryption – in sec (1216 bits)
Subasree et.al. [33]	2.1	2.3	2.1
Kumar et.al. [34]	4	3.2	6
Ren et.al. [35]	1.3	1.8	2.3
Ramaraj et.al. [36]	3	2.7	4.9
Shabana et.al. [37]	0.9	2	3
Proposed	0.188	0.512	0.772

Figure5:Comparison of encryption times of various contributions

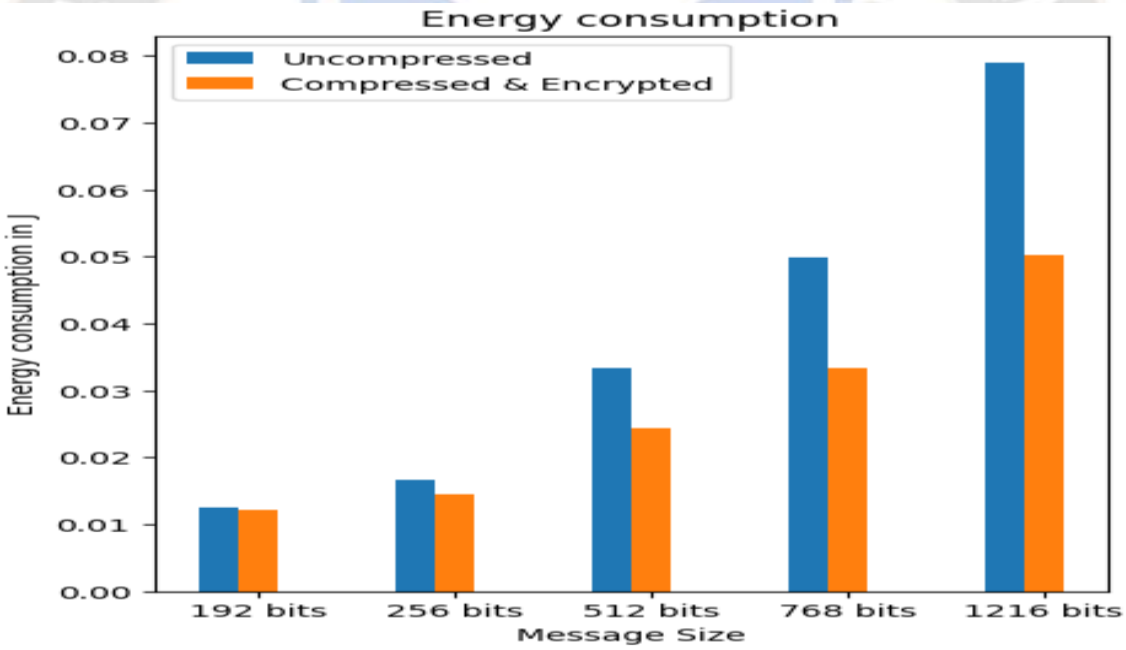


International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *10 August 2023* ***Revised:*** *28 September 2023* ***Accepted:*** *20 October 2023*

Table 5: Energy consumption comparison

Data length (bits)	Uncompressed data (UC)	Compressed data (C-E-C-E)
192	0.01248	0.01222
256	0.01664	0.01456
512	0.03328	0.02444
768	0.04992	0.03328
1216	0.07904	0.05018

Fig 6: Uncompressed vs Compressed & Encrypted energy efficiency comparison



4. Conclusion and Future scope

Usage of wireless sensor networks has become enormous due to their potentiality. However major challenges in implementing WSNs include security, energy efficiency, QoS, Scalability and others. In this paper a novel solution is architected to address the security issues while the data is being transmitted from sensor nodes to sink node. The major concerns while designing a security solution comprise the robustness of solution, transmission speed and energy constraints. The DAR model detailed exhibits strong encryption as three state of art algorithms are used. In addition, the key management also reveals its efficacy. Due to the novel Compression-Encryption-Compression-Encryption (CECE) process, the data is encrypted optimally and is attack resistant. The compression and encryption processes happen very quickly and the data size gets reduced drastically giving scope to faster transmission. Due to higher compression ratios, the encryption sounds high besides preserving the energy efficiency.

In this research work we focussed on providing security as well its impact on preserving the energy efficiency and time consumption. As a part of future extension, more focus is to be given on practical implementation of testing the algorithm for

all types of attacks which proves the technique to be highly vigorous. The hybrid approach is formulated and verified for textual information such as temperature, humidity, pressure and so on. However, the approach must be equipped for Image related data security.

References:

[1] Yazdinejad, M.; Nayyeri, F.; Ebadati E., O. M.; Afshari, N. (2017): Secure distributed group rekeying scheme for cluster based wireless sensor networks using multilevel encryption. Internet of Things: Novel Advances and Envisioned Applications, pp. 127-147.

[2] National Institute of Standards and Technology (1979). "FIPS-46: Data Encryption Standard (DES)." Revised as FIPS 46-1:1988, FIPS 46-2:1993, FIPS 46-3:1999, available at http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[3] Dworkin, M. , Barker, E. , Nechvatal, J. , Foti, J. , Bassham, L. , Roback, E. and Dray, J. (2001), Advanced Encryption Standard (AES), Federal Inf. Process. Stds. (NIST FIPS), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.FIPS.197

[4] De Cannière C (2005) Blowfish. In: van Tilborg HCA (ed) Encyclopedia of Cryptography and Security. Springer, Berlin. https://doi.org/10.1007/0-387-23483-7_34

[5] Fontaine, C. (2011). RC4. In: van Tilborg, H.C.A., Jajodia, S. (eds) Encyclopedia of Cryptography and Security. Springer, Boston, MA. https://doi.org/10.1007/978-1-4419-5906-5_365

[6] (2006). The RSA Public-Key Encryption Algorithm. In: Furht, B. (eds) Encyclopedia of Multimedia. Springer, Boston, MA. https://doi.org/10.1007/0-387-30038-4_206

[7] Hankerson, D., Menezes, A. (2011). Elliptic Curve Cryptography. In: van Tilborg, H.C.A., Jajodia, S. (eds) Encyclopedia of Cryptography and Security. Springer, Boston, MA. https://doi.org/10.1007/978-1-4419-5906-5_245

[8] Here we need to quote first paper

[9] P.B. Hari, S.N. Singh, Security issues in wireless sensor networks: current research and challenges, in: Paper presented at the 2016 international conference on advances in computing, communication, & automation (ICACCA) (Spring), 2016.

[10] Pooja & R. K. Chauhan (2022) Triple phase hybrid cryptography technique in a wireless sensor network, International Journal of Computers and Applications, 44:2, 148-153, DOI: 10.1080/1206212X.2019.1710342

[11] Shabana Urooj, Sonam Lata, Shahnawaz Ahmad, Shabana Mehfuz and S Kalathil, "Cryptographic Data Security for Reliable Wireless Sensor Network", Alexandria Engineering Journal, Volume 72, 2023, Pages 37-50, ISSN 1110-0168, https://doi.org/10.1016/j.aej.2023.03.061.

[12] Mahlake, Ntebatseng, Topside E. Mathonsi, Tonderai Muchenje and Deon Du Plessis. "A Hybrid Algorithm to Enhance Wireless Sensor Networks security on the IoT." *ArXiv* abs/2303.14445 (2023):

[13] F. Ullah, T. Mehmood, M. Habib and M. Ibrahim, "SPINS: Security Protocols for Sensor Networks", 2009 International Conference on Machine Learning and Computing IPCSIT, vol. 3, 2011. IACSIT Press, Singapore

[14] L. Tobarra, D. Cazorla and F. Cuartero, "Formal Analysis of Sensor Network Encryption Protocol (SNEP)," 2007 IEEE International Conference on Mobile Adhoc and Sensor Systems, 2007, pp. 1-6, doi: 10.1109/MOBHOC.2007.4428763.

[15] Sharmila, Kumar, P., Bhushan, S. *et al.* Secure Key Management and Mutual Authentication Protocol for Wireless Sensor Network by Linking Edge Devices using Hybrid Approach. *Wireless Pers Commun* **130**, 2935–2957 (2023). https://doi.org/10.1007/s11277-023-10410-7

[16] Sampradeepraj T, V. Anusuya Devi. A Hybrid Cryptography and End-to-end Security Model for Wireless Sensor Netwoks, 14 June 2022, PREPRINT (Version 1) available at Research Square [https://doi.org/10.21203/rs.3.rs-1619181/v1]

[17] Uras Panahi & Cüneyt Bayılmış,"Enabling secure data transmission for wireless sensor networks based IoT applications", Ain Shams Engineering Journal, Volume 14, Issue 2,(2023) 101866, ISSN 2090-4479, https://doi.org/10.1016/j.asej.2022.101866.

[18] Hudhaifa A. Abdulhameed, Ayoob A. Abdulhameed, Mahmood F. Mosleh, Alhamzah T. Mohammad; Lightweight security protocol for WSNs using hybrid cryptography algorithm. *AIP Conf. Proc.* 2 December 2022; 2547 (1): 060006. https://doi.org/10.1063/5.0112665

[19] Jeong H, Lee S-W, Hussain Malik M, Yousefpoor E, Yousefpoor MS, Ahmed OH, Hosseinzadeh M and Mosavi A (2022) SecAODV: A Secure Healthcare Routing Scheme Based on Hybrid Cryptography in Wireless Body Sensor Networks. Front. Med. 9:829055. doi: 10.3389/fmed.2022.829055

[20] Kumar, D. A secure and efficient user authentication protocol for wireless sensor network. *Multimed Tools*

Appl **80**, 27131–27154 (2021). https://doi.org/10.1007/s11042-021-10950-9

[21] E., Omid Mahdi Ebadati, Farshad Eshghi, and Amin Zamani. "A Hybrid Encryption Algorithm for Security Enhancement of Wireless Sensor Networks: A Supervisory Approach to Pipelines." Computer Modeling in Engineering Sciences 122, no. 1 (2020): 323–49. doi:10.32604/CMES.2020.08079.

[22] Kumar, D., Chand, S. & Kumar, B. Cryptanalysis and improvement of an authentication protocol for wireless sensor networks applications like safety monitoring in coal mines. *J Ambient Intell Human Comput* **10**, 641–660 (2019). https://doi.org/10.1007/s12652-018-0712-8

[23] Nidarsh M P and G Padmaja Devi, "Chaos based Secured Communication in Energy Efficient Wireless Sensor Networks", IRJET, Vol.05 Issue.06 (2018) pp 742-747

[24] Rawya Rizk and Yasmin Alkady, "Two-phase hybrid cryptography algorithm for wireless sensor networks", Journal of Electrical Systems and Information Technology, Volume 2, Issue 3 (2015), Pages 296-313, 10.1016/j.jesit.2015.11.005.

[25] M.Senthil Murugan and Dr.T.Sasilatha, "DESIGN OF HYBRID MODEL CRYPTOGRAPHIC ALGORITHM FOR WIRELESS SENSOR NETWORK", International Journal of Pure and Applied Mathematics, Vol. 117, No. 16 (2017), pp. 171-177

[26] S. Subasree, N.K. Sakthivel, Design of a new security protocol using hybrid cryptography algorithms, IJRRAS. 2 (2) (2010) 95–103.

[27] N. Kumar, A secure communication wireless sensor networks through hybrid (AES+ECC) algorithmk, Vol. 386, von LAP LAMBERT Academic Publishing, Koln, Germany, 2012.

[28] W. Ren, Z. Miao, A hybrid encryption algorithm based on DES and RSA in Bluetooth Communication, in: 2010 Second International Conference on Modeling, Simulation and Visualization Methods, 2010, pp. 221-225, doi:10.1109/ WMSVM.2010.48.

[29] D.E. Ramaraj, S. Karthikeyan, M. Hemalatha, A design of security protocol using hybrid encryption technique (AESRijndael and RSA), Int. J. Comput. Internet Manag. 17 (1) (2009) 78–86.

[30] Here we need to cite the second paper

[31] Seelamanthula Sreenivasu1 and Prof.James Stephen Meka, "A Survey Paper on Key Management Scheme in Wireless Sensor Network", Journal of Engineering Sciences, Vol 14 Issue 06,2023, pp. 1070 - 1103