Security Enhancement of Wireless Sensor Networks: A Hybrid Efficient Encryption Algorithm Approach

Omid Mahdi Ebadati E*
Faculty of Mathematics and Computer Science, Kharazmi University, Tehran, Iran
ebadati@khu.ac.ir
Farshad Eshghi
Faculty of Electrical & Computer Engineering, Kharazmi University, Tehran, Iran
farshade@khu.ac.ir
Amin Zamani
Faculty of Knowledge Engineering and Decision Science, Kharazmi University, Tehran, Iran
amin.zamani.cert@khu.ac.ir

Received: 24/Feb/2018 Revised: 22/Aug/2018 Accepted: 16/Sep/2018

Abstract

Wireless sensor networks are new technologies that are used for various purposes such as environmental monitoring, home security, industrial process monitoring, healthcare programs and etc. Wireless sensor networks are vulnerable to various attacks. Cryptography is one of the methods for secure transmission of information between sensors in wireless sensor networks. A complete and secure encryption system must establish three principles of confidentiality, authentication and integrity. An encryption algorithm alone cannot provide all the principles of encryption. A hybrid encryption algorithm, consisting of symmetric and asymmetric encryption algorithms, provides complete security for a cryptographic system. The papers presented in this area over the last few years, and a new secure algorithm present with regard to the limitations of wireless sensor networks, which establishes three principles of cryptography. The details of the algorithm and basic concepts are presented in such a way that the algorithm can be operational and showed a very high efficiency in compare to the current proposed methods.

Keywords: Wireless Sensor Network; Cryptography Algorithm; Hybrid Cryptography; Confidentiality Integration Authentication

1. Introduction

A wireless sensor network is a collection of sensor nodes connected to each other by wireless communication channels. Each sensor node is a small device that can collect data from the surrounding area, perform simple calculations and communicate with other nodes or with the main station. Such networks have been developed with the help of recent advances in micro-electromechanical systems and are expected to be widely used in applications such as environmental monitoring, home security, industrial process monitoring, healthcare programs, etc.

A comprehensive and optimized solution for reliable data sensing and secure, fast and timely data transmission is the use of wireless sensor networks. Wireless sensor network technology to monitor structural accuracy with regard to the advancement of technology related to that, such as the ability to measure, communicate protocols, processor speeds, embedded systems, etc. have been of great importance over the years. These developments gradually affected oil and gas industries in order to automate the processes, system capability and control.

Security in wireless sensor networks depends on what it protects. Three security goals in wireless sensor networks include confidentiality, integrity and authentication. Confidentiality in sensor networks is the ability to hide messages from an attacker. Integrity is the ability to detect unread or unrecognized messages. Authentication is the reliability of the message's origin. Furthermore, other security objectives are defined in accordance with these three principles. Availability is to confirm the ability to use the node's network resources to send the message. The freshness feature is to ensure that the recipient receives new data so that the attacker cannot send the old data recently.

Security can be established in each layer of application, network, data link, and physical layer. Cryptographic algorithms play a significant role in information security systems, and can also meet security goals in wireless sensor networks. Encryption is the process of changing message or information so that only authorized people can read that information. Encryption does not prevent the attack, but the content of the message is protected by the attacker. In an encryption scheme, the information or message set to be transmitted using an encryption algorithm change so, that it can only be read by decrypting. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. For a good design encryption scheme, computational resources and much more skills are required. An authorized recipient of the message can easily decrypt

* Corresponding Author

the message with a key and an encryption algorithm. Cryptography is a knowledge of hiding information and verification, and includes protocols, algorithms, and secure strategies to prevent unauthorized access to critical information. Encryption provides a mechanism for verifying each component of a communication.

An encryption algorithm is a component for secure electronic data transfer. Operational and mathematical stages develop cryptographic algorithms. Cryptographic algorithms prevent data frauds and unauthorized access to electronic information. Some cryptographic algorithms are faster than others. The designers and developers of the algorithms make the math background more complicated by the algorithms so that the attackers cannot penetrate. The power of an encryption algorithm usually depends on the length of the key.

In the past, organizations and companies that needed encryption or cryptographic services designed their own cryptographic algorithms. Over time, major security weaknesses appeared in these algorithms, which made it easier to decrypt. For this reason, cryptographic encryption is now outdated, and in new encryption methods, it is assumed that the full information of the cryptographic algorithm has been published, and what's hidden is just the password key. Therefore, all the security derived from standard encryption algorithms and protocols relies on the security and secret key encryption, and the full details of these algorithms and protocols are released to the public. Cryptographic algorithms and functions used in cryptography are divided into symmetric, asymmetric, hashing, key exchange, key derivation and hybrid.

Symmetric and asymmetric cryptography each has advantages and disadvantages. Symmetric cryptography is significantly faster than asymmetric cryptography, but requires the exchange of a common key. Asymmetric algorithms do not require key exchange systems, but run fast in terms of speed. The combination of asymmetric and symmetric cryptographic systems creates a hybrid encryption system. In asymmetric encryption, the sender and receiver need not to subscribe to a shared key in order to communicate securely, and often rely on complex mathematical calculations. To transmit a hidden random key from a symmetric encryption, the corresponding key can be encrypted using the public key and then sent. The receiver uses its private key to decrypt the key and use it and a symmetric encryption algorithm to send and receive encrypted messages. This protocol is a simple example of a hybrid encryption system. In many applications, the cost of encrypting long message in an asymmetric cryptographic system is very high, which is why hybrid encryption is used. All cryptographic algorithms cannot achieve the three main cryptographic goals: confidentiality, integrity, and authentication. In a hybrid cryptographic system, the weaknesses of an algorithm are covered with the strengths of the other algorithm, so that in one system, all the main purposes of the encryption are met. PGP (Pretty Good Privacy) and TLS (Transport Layer Security) are examples of hybrid cryptographic systems.

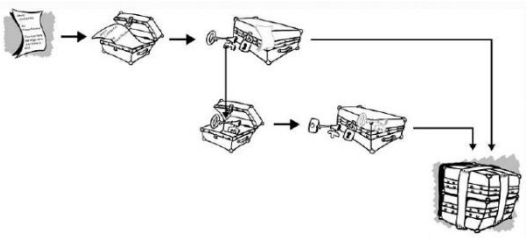

Fig. 1. Hybrid cryptography

2. Literature Review

In the Madhumita Panda [1] paper, two public-key RSA and ECC algorithms have been investigated. The ECC algorithm has significant advantages over the RSA algorithm, which reduces the computation time as well as the amount of data transmitted. The RSA algorithm is a method for implementing a public key encryption system whose security depends on the complexity of the large primes' number factoring. The RSA is made up of the first letter of last names of Ron Rivest, Adi Shamir, and Leonard Adleman in 1977. This method is suitable for data encryption and digital signature creation. Today, the RSA algorithm is a public key encryption that is widely used in the world. The ECC algorithm is related to the algebraic structure of elliptic curves and its difficulty in elliptical curve size. The key advantage of this algorithm is the smaller key size, which reduces storage and transmission. For example, an elliptic curve algorithm can provide the same level of security in an RSA based system with smaller modules and keys. For current cryptographic purposes, an elliptic curve is a curved surface that contains points of the equation $y^2 = x^3 + ax + b$. Compared to the RSA, ECC has a smaller key and uses less memory, which is highly regarded by wireless sensor networks.

The symmetric key algorithm has a weak point in the key distribution, and the asymmetric algorithm requires much computation. Therefore, it is more appropriate to use an algorithm that combines both asymmetric and symmetric algorithms, so that the benefits of both algorithms are more appropriate. A hybrid encryption system is a combination of different types of encryption protocols and is best served by this. A common method is to generate a random hidden key for a symmetric encryption, and then asymmetric encryption of this key using the public key of the receiver. The message is also encrypted using symmetric encryption and hidden key. Hidden encryption key and encrypted message are sent to the recipient. The receiver decrypts the hidden key using its private key, and then decrypts the message key using it. The main approach in the PGP algorithm is the same. Another combination algorithm can be DHA + ECC (Diffie-Hellman algorithm + Elliptic curve cryptography). Public key cryptographic designs were introduced based on the elimination of problems with symmetric cryptographic approaches. Two designs were compared in the Madhumita

Panda paper. The ECC algorithm uses less memory, less processing, and a shorter key than the RSA algorithm.

A new method for ECC cryptography has been proposed by Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh [2] that eliminated the classical methods of mapping characters to offsets in ECC. ASCII values match pairs of texts, and pairings are used as ECC encryption inputs. This proposed new method reduces the cost of the mapping operation and requires the sharing of the table between the sender and the receiver. The algorithm is designed to be used to encrypt or decrypt any type of text with the values of the ASCII. In the Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh article, some ECC encryption concepts are fully described, and the remainder of the fractional calculation is described in brief with the use of the Euclidean algorithm developed.

In the Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh article, a real example presented and key size, key sensitivity to change, time complexity, resistance to some attacks checked out. In this paper, a new method for encrypting text using ECC is presented. ASCII values are divided into groups whose group size is calculated using the P-value of the ECC parameters with a base that is smaller than the maximum amount of ASCII. Large numbers with a specific procedure are divided into P_m pairs. This process helps eliminate the cost of mapping characters to the corresponding elliptic curve. The proposed algorithm is applicable to any text with ASCII values. According to the efficiency comparison table, we can say that the proposed algorithm has positive aspects. It even comes with a lot of words as input, decryption and encryption. The smaller size of encrypted text contributes greatly to bandwidth saving compared to other methods.

Many images are moving through the network daily. Most of these images are confidential and should be transmitted securely. Cryptography plays a significant role in the safe transfer of images. The exponential problem solving a discrete logarithm of an elliptic curve proportional to the size of the ECC key provides a high level of security in comparison with other smaller size key encryption methods, which depends on the correct factoring or discrete logarithmic problem. In another article on Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh [3], an ECC algorithm for encryption, decryption, and digital signature of an image has been implemented. In this paper, a real case study was presented and histogram analysis, key size, key sensitivity to change, correlation analysis, entropy analysis, and resistance to some attacks. In Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh paper, a cryptographic method was provided to match the encrypted photo. The algorithm was presented by grouping the pixels according to ECC parameters. The grouped pixel values are paired together instead of the values mapped to elliptic curve coordinates. This helps to override the use of the mapping table for encryption and decryption. The algorithm produces a cryptographic image with low correlation, even with a picture taken from similar pixels.

Data encryption is required to prevent unwanted access to information by individuals. In Gaurav Patel and Krunal Panchal [4] paper, hybrid methods are investigated by combining two important RSA algorithms and Diffie-Hellman's algorithm. This hybrid cryptographic algorithm provides more security than the RSA algorithm. RSA is the foundation of many encrypted applications. Great progress is for public key encryption and is also used for digital signing. The algorithm process consists of three steps: key generation, encryption and decryption. Whitfield Diffie and Martin Hellman developed the Diffie-Hellman algorithm in 1976. The Diffie-Hellman key exchange protocol is a special method for exchanging cryptographic keys and is one of the first practical examples of cryptographic key exchanging. The Diffie-Hellman key exchange method allows two entities that have no prior knowledge to share a common key through an unsecured connection channel. Then use this key to encrypt the next communication. Diffie-Hellman has been involved in multi-protocol development, including SSL (Secure Sockets Layer), SSH (Secure Shell), and IPS (Internet Protocol Security).

In the proposed Gaurav Patel and Krunal Panchal, the XOR (Exclusive or) Bit Operator is used to enhance the message's complexity. This operation is performed after the message is converted into a cipher text. In this method, two prime number is selected first, and exponential keys of the encryption and decryption process are made. Two numbers A and B are selected for Diffie-Hellman algorithm. R is a randomized number generated by the system automatically. A generic number is generated by Diffie-Hellman's algorithm. Using this common number, KA and KB hidden keys are used in the XOR operator. On the sender side, encryption is performed using the algorithm. When the encryption process is complete, the XOR operation takes place between the secret text and the first hidden key. After the operation, the message is sent securely through the communication channel. On the receiver side, the XOR action is performed again between the second secret key, and the message sent by the sender. Using this operation, the original text is obtained. We can get the main message through the decoding algorithm with the inverse of the same process.

The RSA algorithm is used as one of the most efficient encryption algorithms and provides confidential, information integrity and privacy. In Meenakshi Shankar and Akshaya P [5], RSA algorithm has been integrated with Round-Robin priority scheduling to enhance security and reduce the effectiveness of infiltration. The minimum overhead, increased throughput and privacy are its benefits. In this method, the user uses RSA algorithm and generates encrypted messages that are categorized according to priority and then sent. The receiver decoded messages using the RSA algorithm and according to their priority. This method reduces the risk of man-in-the-middle and timing attacks so that encrypted and decrypted messages are more based on priority. Moreover, if there is

little information exchanged, it also reduces the risk of a power monitoring attack. This approach expands the standards of information security by ensuring greater productivity. In Meenakshi Shankar and Akshaya P research, a brief description of cryptography, steganography, cryptanalysis and cryptology was presented. Then, cryptographic types such as secret key cryptography, public key, and hash function were described. Some changes were made to the RSA algorithm. The first numbers p and q were received from the user. N and Φ(n) were calculated. All the prime numbers are listed between 1 and Φ(n) and allow the user to select value e from the given values. The private key was calculated using d. Priority messages were divided into various priority sections, medium priority, and high priority. The message was encrypted using $C = M^e \bmod n$ and sent to the recipient based on the Round-Robin method.

In Meenakshi Shankar and Akshaya P article, an effective way is presented, which is a combination of successful ways to communicate secretly in a network. The proposed algorithm also reduces brute-force attack effect even if the attacker intercepts and decrypts the message. Furthermore, decrypting a part of a message is not so easy. The RSA algorithm is an efficient and common encryption algorithm and reduces the impact of attacks. The side channel attack is not very effective in this way as it uses a different RSA algorithm. If an attacker is detected, the sender can be stopped; thus, the attacker will not receive the entire message. As a result of this, the impact of a man-in-the-middle attack is reduced. Therefore, if effective methods are combined to prevent side channel and man-in-the-middle attacks, they will be much more productive. This function is effectively performed by an application that encrypts and decrypts messages.

Symmetric and asymmetric hybrid encryption algorithms provide integrated data transfer and concealment at higher speeds and play an important role in virtual private networks. Shi-hai Zhu [6] article deals with the implementation of a hybrid algorithm. System performance analysis and practical tests show that an AES and ECC algorithm provides higher security than the DES and RSA algorithms, especially in virtual private networks that require secure transport.

The proposed hybrid encryption algorithm by Shi-hai Zhu has many advantages. By encrypting AES and ECC keys, we no longer need to send a secret key before we can communicate the secret key management with ECC. The speed of the encryption and decryption process is as large as AES, and the time consumed for ECC is only for AES key. If there are a lot of transfer data, then the use of ECC will be negligible. We send the keys to the ECC and use a digital signature.

The proposed encryption algorithm by Shi-hai Zhu is a combination of public key encryption features that easily distributes the key and is calculated at a high speed and provides a good and fast way to transmit information. In general, hybrid encryption algorithms have many benefits. For example, simple rules, high security, comprehensibility and the ability to execute with hardware and software are largely the criteria for designing a hybrid encryption algorithm. In addition, key security is a tight principle to ensure privacy and file security. In the short term, the hybrid algorithm used in virtual private networks can help to achieve the goal of fast and secure data transmission.

The Internet in the world today is widely used to access information, which is why there is a need to send secure information. The main goal of K. Brindha and others [7] paper is to examine the encryption methods, to improve some of the current algorithms, to create a way to increase the security and implementation of information encryption so that it is impossible to read the resources sent to the attackers on the web. AES and ECC are methods used for encryption. In the proposed algorithm by K.Brindha and others, the file containing the text is encrypted using AES algorithm and its key using ECC algorithm, and the encrypted text is decrypted on the recipient's side. The AES and ECC algorithms are implemented together to provide hybrid encryption. The text is encrypted using AES. The key is encrypted using ECC. The text and the encrypted key are sent to the recipient. The text and the encrypted key are received. The key is decrypted using ECC. Encrypted text is decrypted using decrypt keys and AES.

Secure data transmission on wireless networks is provided using hybrid encryption. For better communication, advanced algorithms are used to break them hard. K.Brindha and others suggest for future that they choose the right encryption so that they can use all the network resources effectively and take into account all network constraints.

The application of the network and the internet is growing at a high rate, thus increasing the need to protect such applications. Rashmi Singh and others [8] highlight this problem by providing two cryptographic methods. The first way is to compress data in half, and the second method focuses on producing characters of encrypted text differently for the same text characters than the different events of the character in the text. The combined effect of using symmetric algorithms with the proposed algorithm creates a hybrid encryption scheme that makes it difficult for an attacker to learn from messages transmitted in an unsecured transmission environment. In Rashmi Singh and others, encryption and decryption are described in detail in four sections along with the code. In the last section, the key generated is different for each character, which means that a single character in the text may have a different cipher character corresponding to the character position. A hybrid encryption scheme is a good combination of data compression and encryption to enhance data security. In this way, the data size is reduced by 50% and security increases. The characters produce the cipher text according to their position. There is currently a demand for reducing space and data security during the transfer. Rashmi Singh and others try to cover all these needs.

Prakash Kuppuswamy and Saeed Al-Khalidi [9] suggest a hybrid cryptographic system using a new public-key algorithm and a private key algorithm. A hybrid encryption system combines the convenience of a public-key system with the efficiency of a symmetric key. In the article by Kuppuswamy and Saeed Al-Khalidi, two secure data encryption methods are provided that are important for confidential. The system uses two different encryption algorithms for the encryption and decryption process; one is public key encryption based on a linear block cipher, and the other is private key encryption based on a symmetric simple algorithm. This encryption algorithm provides more security is better than other existing hybrid algorithms. Cryptography and decryption of any information require a secure key. For this purpose, in Kuppuswamy and Saeed Al-Khalidi paper, the asymmetric key is used, and the linear block cipher algorithm is used for data security. The linear block cipher algorithm is more efficient than the symmetric encryption method. Research results show that its processing time is more efficient than other algorithms. Therefore, AES algorithm, coupled with the RSA algorithm for key management, is an efficient way to ensure the security of transmission data. The security of the combination of RSA and AES is better than the combination of RSA and DES, and the proposed algorithm by Kuppuswamy and Saeed Al-Khalidi is more efficient than the combination of RSA and AES in data transfer. In the article by Kuppuswamy and Saeed Al-Khalidi, a new procedure for future research is also outlined.

A computer network is an interconnected group of independent computing nodes that interact with each other by using a proper definition and a set of agreed rules and conventions known as protocols, and permitting the sharing of resources preferably in a way that can be Predictable and controllable. Today, communications have a major impact on businesses, and data transfer with high security is demanded. Attacks have compromised security; hence, various symmetric and asymmetric encryption algorithms are provided to achieve security services such as authentication, confidentiality, integrity and availability. At the moment, various types of cryptographic algorithms provide high security for information in a controlled network. These algorithms need to specify the data security and authenticity of the user. In order to improve the strength of these security algorithms, a new security protocol for online transactions has been designed using the combination of symmetric and asymmetric encryption methods in the S. Subasree and N. K. Sakthivel [10]. This protocol meets the three basic principles of encryption: integrity, confidentiality, and authentication. These basic principles can be met by using elliptic curve cryptography, Dual RSA and MD5. ECC for encryption, Dual RSA for authentication and MD5 for integrity. This new security protocol uses a combination of symmetric and asymmetric methods for better security and integrity. The text is encrypted using ECC. At the same time, the hash value is calculated using MD5. The resulting hash value is then encrypted with the Dual RSA algorithm. The process of decrypting is an inverse process of encryption.

A computer network is a set of computing nodes that can exchange data with meaningful interaction with each other and allow resource sharing in the appropriate manner. A set of connected computers using communication channels requires security for the exchange of information. This field of work involves a specialist in network security with the network administrator that prevents and monitors unauthorized access, modifies, and disables the use of the network. To combat this growing problem, security professionals are looking for better protection. Attacks have endangered security; hence, various symmetric and asymmetric encryption algorithms are provided to achieve the appropriate security services such as identity, confidentiality, integrity and availability. These algorithms are designed to provide security and authenticate users. To improve the strength of these security algorithms, Manali J Dubai and others [11] have developed a new security algorithm using both symmetric and asymmetric encryption methods. This algorithm provides three principles of cryptography: integrity, confidentiality, and authentication. This algorithm is derived from the combination of ECDH, ECDSA, DUAL RSA algorithms and MD5 hash algorithms. This new security algorithm has been used for better security and integrity of the combination of symmetric and asymmetric encryption methods. In the paper by Manali J Dubal and others, a brief description of encryption, crypto analyzer, cryptosystem and ECDH algorithms, DUAL RSA and MD5 are presented. The text is encrypted using DUAL RSA encryption algorithm, and the key generated with ECDH. Encrypted text for identifying with the ECDSA algorithm is combined. The encrypted text is hashed by the MD5 algorithm. To decrypt, the hash value is first calculated. The computed value is compared with the signature to confirm the message. Decrypting cipher text is done with DUAL RSA.

In Manali J Dubal and others paper, a strong and lightweight protocol is being used that uses ECC pattern. The proposed protocol addresses several problems, such as operational implementation, short response time, efficient computing and cryptographic power. The ECC charm compared to RSA is to provide better security with a smaller key, which reduces processing overhead. Advantage of using it, higher speed, lower power consumption, bandwidth saving, storage efficiency and smaller certificate.

Wireless sensor networks consist of hundreds or thousands of low-cost, low-power and self-organized nodes that are highly distributed [12]. Wireless sensor networks are growing and require effective security mechanisms, because sensor networks may interact with sensitive data. Cryptographic algorithms have a good role in information security systems. Currently, various types of cryptographic algorithms provide security in wireless sensor networks, but there are still some problems. At present, symmetric and asymmetric encryption methods

can provide a level of security with some constraints. In a paper by Bhupinder Singh Dhaliwal and Vivek Soi [13], a new hybrid encryption algorithm is proposed to improve the power of these algorithms. The algorithm is designed using a combination of two symmetric and asymmetric encryption methods. The proposed algorithm is a cryptographic method composed of ECC and AES algorithms. RSA and Blowfish are used for authentication and MD5 for integrity. The results show that the proposed encryption algorithm performs better in terms of computation time and encrypted text size. Bhupinder Singh Dhaliwal and Vivek Soi, an attempt to make a fair comparison between the new protocol and the four existing protocols. The comparison is done in different ways, such as the size of the data block and the speed of encryption and decryption. The empirical results in the article determine the effect of each. Then ECC, ECDSA, ECDH, MD5, RSA and Blowfish algorithms were briefly described. Previous work in this area included Subasree, Kumar, Kady and Zhu. By changing the perception of a sensor, the performance and progress of the sensor network can be enhanced. ECC encryption supports various encryption methods and privacy by generating keystrokes. This scheme will lead to network management in an agile manner.

One of the goals of wireless sensor networks is to transmit trusted information from one node to another in the network. In the paper by Bhave and Jajoo [14], an encryption scheme of improved AES and ECC algorithms has been used to increase the security of wireless sensor networks. This paper analyzes AES algorithm and the S-Box structure and provides an improved AES encryption algorithm. Using the AES algorithm, the message sent by the sender changes to be completely new encrypted text so that the attacker cannot guess the recipient's original message.

AES is rightly recommended as the most suitable symmetric encryption algorithm for wireless sensor networks. The AES algorithm has complex mathematical computations on the text, such as the transformation of the primary key and the XOR operator with a polynomial matrix. This algorithm is 10 rounds to convert text to encrypted text. Using the S-Box Replacement makes inverse easy, but makes it harder for attackers. Moreover, in this algorithm, the time required for encryption is very low. In Bhave and Jajoo article for exploring purposes, plain text is given with 16 bytes, and a key is considered and the algorithm is implemented.

Many key management schemes are provided in a wireless sensor network. Sensor nodes are provided with insufficient battery power, low memory, limited computing, and communication constraints. Energy in safe and efficient routing is a major issue for wireless sensor networks [15]. In the article by R. Sharmila and V. Vijayalakshmi [16], the key management scheme consists of a public key encryption scheme and a symmetric schema. The symmetric key is generated using the genetic algorithm. The initial entry for the genetic algorithm is the key generated by the HECC (Hyperelliptic CurveCryptography) encryption. The design offers energy efficiency, flexibility against node capture attacks, and key refreshment between cluster heads and cluster nodes. The simulation results show that this hybrid scheme has more robustness, more energy-efficient, and smaller-sized keys. A key management pattern consists of four steps before the key distribution, deployment of the key, adding and deleting the node. Based on cryptographic methods, the key management schema is categorized into three types of symmetric management, asymmetric management, and hybrid key management techniques. The key is deployed using the HECC. The proposed new key management plan combines the benefits of using elliptical curve and symmetric key generation using the genetic algorithm to secure wireless sensor networks. The proposed new hybrid algorithm describes the combination of the genetic algorithm with public key cryptography and is applicable to encryption of text and images and is suitable for wireless sensor networks. The algorithm is strengthened by a predetermined permutation factor for the cluster head node and member nodes; thus breaking it is very difficult. The proposed method is divided into two stages of key deployment and symmetric key generation. The key deployment step is divided into three stages of key generation, before key distribution and key agreement. The server generates a key in a key repository using the HECC. Whenever a key is generated, a key pool is generated for a key using a specified process. Each time the keys and corresponding key pools are generated, they are distributed in the sensor nodes. Sensing nodes attempt to establish a secure connection by connecting the key pool. If they are not able to establish a secure connection, they will use an interface node to establish a secure connection to their neighbor's node.

Wireless sensor networks include a different set of communication levels and types of routing protocols. In another research [17], they shared the key between cluster head and member nodes using the asymmetric key distribution and genetic algorithm. Secure the internal cluster of communication and it's effective in key reconstruction for hierarchical sensor networks. The proposed method is energy-efficient use, efficient authentication and high flexibility against cluster-head compromise attacks.

Some sensors use Bluetooth technology to communicate in wireless sensor networks. In a paper by Wuling Ren and Zhiqian Miao [18], a communication encryption algorithm based on DES and RSA is provided to enhance the security of data transmission in Bluetooth communication. Currently, the encryption algorithm used in Bluetooth protects the confidentiality of data during transmission between two or more devices, and a 128-bit symmetric encryption called E0. This encryption is broken down under certain conditions with the complexity of time O (2^{64}). In the proposed hybrid algorithm instead of E0 encryption, DES algorithm is used for data transmission because it has higher efficiency in block encryption and uses the RSA algorithm to decrypt the DES key because it is superior to cryptographic key management. Under the

protection of DES and RSA algorithms, the Bluetooth system is safer. It is clear that the whole encryption method is simple and efficient, and in addition, the confidentiality of the algorithm is high. Bluetooth features include a wireless, short-range and low-power. In Wuling Ren and Zhiqian Miao, the current Bluetooth cryptographic structure is described using pin, E2, E3 and link key. The process of decrypting is an inverse process of encryption. The proposed algorithm has many advantages. The use of RSA algorithm and DES key for transmission have been used. Key management is done by RSA. The use of RSA algorithm allows the use of digital signatures. The encryption and decryption speed is similar to DES, and RSA usage time is only for the DES keys. Hybrid cryptographic algorithm is safer than the safety of the two RSA and DES algorithms.

Bluetooth technology is a new technology that has changed the way it is transmitted. However, Bluetooth technology does not fully address security issues in the standardization process. Bluetooth is used as a wireless communication channel in the transmission environment and more vulnerable to fixed networks. For programs with priority security, achieving a high level of security is essential. Currently, the E0 encryption is used with all the shortcomings in the Bluetooth standard, while the DES and RSA combination encryption algorithm is relatively safer and easier. In this way, the security of data transfer between Bluetooth devices is guaranteed in real time.

In Komal Rege and others [19], a hybrid encryption algorithm is based on AES and RSA to increase the security of data transfer in Bluetooth communications. At present, the E0 algorithm is used to transfer information between two devices or more via Bluetooth. The combination of the encryption algorithm instead of E0 uses AES algorithm, which has a great effect on block encryption, and uses RSA algorithm to encrypt AES key to exploit the key management benefits. Therefore, the use of AES and RSA algorithms makes it safer to transfer information in Bluetooth. In addition, the hybrid encryption algorithm is a convenient and easy way to encrypt data and enhance confidential. In the Komal Rege and others, the current structure of Bluetooth encryption is described using pin, E2, E3 and the link key, and the weaknesses of the E0 algorithm, such as address spoofing, LFSR (Linear Feedback Shift Register) constraint, PIN reliability, and low credibility of link key.

The process of decrypting is an inverse process of encryption. For private key encryption, there are many algorithms such as DES, 3DES, AES, and Blowfish. The DES algorithm was developed and popular in 1970. However, today, for many applications, it is insecure and weak because the 56-bit key length is too small. Many of the attacks exploited DES's shortcomings. 3DES offers an improvement on DES, in which the DES algorithm is used three times, but it is very slow. Blowfish algorithm is used in public domain for applications and suffers from poor key issues. The AES algorithm has the most priority and is considered as the best encryption standard. Brute-force attack is the only known attack against the AES algorithm. RC4, 128-bit and a fast encryption, preventing many kinds of attacks. Due to the weaknesses of other algorithms, AES is the best cryptographic standard and is preceded by other standards. Studies have shown that Blowfish is the fastest in terms of processing time, but security is a concern. In this respect, AES works best. Therefore, AES algorithm, coupled with RSA algorithm for key management, is an efficient way to ensure the security of data transmitted using Bluetooth.

Bluetooth technology is widely used to transmit information over short distances. Bluetooth as a wireless technology is more prone to attacks than other networks. Therefore, data security is important during transfer. E0 is an encryption algorithm that is currently used in Bluetooth for encryption, which has many shortcomings and can be easily broken. The AES algorithm with a low number of published attacks is very secure. Moreover, the difficulty of factoring large integers guarantees the security of RSA algorithm. Accordingly, the proposed combination of encryption algorithms using AES and RSA provides a safer and easier way to transfer data between Bluetooth devices compared to the E0 algorithm.

Security is one of the most important and fundamental issues for transmitting data in wireless sensor networks. Hence, innovative hybrid encryption algorithms for security have been developed. DNA (Deoxyribonucleic Acid) cryptography plays a vital role in the fields of communication and data transmission. In DNA encryption, the biological concept of DNA is used not only to store data and information carriers, but also to perform computations. In the paper by Monikaa and Shuchita Upadhyaya [20], computing security is provided using DNA-based encryption. This paper presents an innovative algorithm that uses a DNA encryption and SSL protocol to provide a safer channel for the exchange of information in wireless sensor networks. In Monikaa and Shuchita Upadhyaya paper described the definition of a wireless sensor network and shared cryptographic keys between sensors as a problem. Three patterns of key subscription (release by a secure server, agreement on a specific contract for the distribution and distribution of keys before network development) and their disadvantages were identified. The third pattern was chosen, and based on this, a combination of DNA encryption and the SSL protocol was presented after providing a brief description of the DNA molecule and the SSL protocol.

The process of decrypting is an inverse process of encryption. The data in the encryption is hidden using DNA-related methods. In Monikaa and Shuchita Upadhyaya paper, the concept of DNA is used in cryptography and SSL protocol, which meets three levels of security in wireless sensor networks. In the proposed system, the power consumption problem for generating key pairs and producing certificates for sensors has been raised, to a certain extent, by assigning keypads and digital certificates prior to deploying sensors in the environment. The public key and digital certificate are shared using SSL protocol. Therefore, the calculation overhead for key generation may be reduced and ultimately leads to energy efficiency in the sensors. It is anticipated that the proposed solution may provide promising results.

Encryption plays an important role in securing wireless sensor networks. In the article by Rawya Rizk and Yasmin Alkady [21], a new algorithm is comprised of symmetric and asymmetric encryption methods with a small security key. This algorithm guarantees three principles of cryptography: integrity, confidentiality and identity. The combination of ECC and AES encryption algorithms is provided. The XOR and DUAL RSA algorithms are used to identify and MD5 for integrity. The results show that the hybrid algorithm presented in computational time, cipher text size, and energy consumption. This algorithm is resistant to a variety of attacks.

In the article by Rawya Rizk and Yasmin Alkady, past activities on hybrid encryption have been investigated, including Subasree, Dubal, Kumar, Ren and Zhu algorithms. This article is one of the most complete articles in the field of cryptography for wireless sensor networks. The process of decrypting is the inverse of the encryption process. The reason for the superiority and power of the proposed algorithm is a set of features of RSA, ECC, XOR, AES and MD5. In the paper by Rawya Rizk and Yasmin Alkady, a hybrid algorithm for the security of wireless sensor networks is presented. This algorithm is designed to solve several problems, including operational implementation, short response time, efficient computing and power of the cryptographic system. An algorithm called THCA (Two phase Hybrid Cryptography Algorithm) is suggested. The THCA tries to divide the text and then apply two different methods. First of all, the advantages of using a combination of both symmetric and asymmetric encryption methods are AES and ECC. Then it uses a custom RSA algorithm that is robust and cannot be easily attacked. In addition, the hash has been used with MD5 to control the data to ensure that the original text does not change during the transmission. Also, the performance of THCA is compared to other algorithms. This algorithm provides better security with less encryption and decryption time and a shorter cipher text size. As a result, reducing the overhead of data processing has achieved lower energy consumption, which is suitable for all applications of wireless sensor networks. In the article by Rawya Rizk and Yasmin Alkady, the proposed THCA algorithm was used to encrypt an image and its resistance to various types of attacks were investigated.

3. Proposed Method

The purpose of this research is to develop it as an applied research. The general scheme of the proposed algorithm is as follows:

The process of the proposed algorithm is as follows:

1. The information string is read from a text file.

2. The information string is converted to binary string using Huffman's coding.

2.1. Create a leaf node for each character and add it to the priority queue.

2.2. While there is more than one node in the queue:

2.2.1. Remove the two nodes of highest priority (lowest probability) from the queue

2.2.2. Create a new internal node with these two nodes as children and with probability equal to the sum of the two nodes' probabilities.

2.2.3. Add the new node to the queue.

2.3. The remaining node is the root node, and the binary string constructed.

3. The binary string is divided into 256-bit blocks. If the final block is not a multiplier of 256, it will be padded with 0.

4. The 256-bit strings are divided into two categories. If the number of blocks is odd, the dividing point of the relation $\frac{n(B)+1}{2}$ and if the number of blocks is even, the dividing point is obtained from the relation $\frac{n(B)}{2}$.

5.1. In the Rijndael algorithm, 14 rounds are used to convert each block information.

5.2. The initial block or state is added to the extended key.

5.3. Round processes include S-Box, shift and mix columns operations. These processes are performed at all times, except for the column mix that are not done in the last round. The result state is added to the extended key for each round. The final result is the cipher block.

6.1. The cryptographic key required to Rijndael encryption for the first group of blocks is generated by ECDH algorithm.

6.2. For generating the secret encryption key between two nodes, A and B using ECDH, both sides of the relationship must agree on the elliptic curve domain parameters. On both sides of communication, a pair of keys contains a private key d (a random integer less than n) and a public key Q = d × G. G is the generator point for cryptographic operators. Suppose (d_A, Q_A) the private and public key pair of node A and (d_B, Q_B) are the private and public key pair of node B.

6.3. The node A, $K = (x_K, y_K) = d_A \times Q_B$, calculates.

6.4. The node B, $L = (x_L, y_L) = d_B \times Q_A$, calculates.

6.5. Since $d_A \times Q_B = d_A \times d_B \times G = d_B \times d_A \times G = d_B \times Q_A$, then K = L and hence $x_K = x_L$ is established.

6.6. The hidden encryption key is x_K.

7.1. The cryptographic key required to Rijndael encryption for the second group of blocks is generated by RSA algorithm.

7.2. The two prime numbers p and q are chosen. Being prime of the numbers should be checked through the tests.

7.3. n = pq is calculated. n is a base Modular in public and private key.

7.4. $\lambda(n) = LCM(\lambda(p), \lambda(q)) = LCM(p-1, q-1)$ is calculated.

7.5. An integer e is chosen so that $1<e<\lambda(n)$ and $GCD(e, \lambda(n)) = 1$ are established. In fact, e and $\lambda(n)$ are relative to prime.

7.6. $d = e^{-1} \bmod \lambda(n)$ is computed.

7.7. If node B wants to send node key of Rijndael algorithm, node A sends the public key (n, e) to node B. After the node B takes the public key node A, it can send the message M to node A. First, the message M must be converted to the integer m such that $0<m<n$.

7.8. The node B generates a ciphered message using the public key e and $c = m^e \bmod n$. The node B sends message c to node A. The node A retrieves the number m from message c using the private key power d and $c^d = (m^e)^d = m \bmod n$.

4. Pseudocode

Algorithm 1. Loading information string from a text file

```
1. string plaintext = read (string TextFilePath);
```

Algorithm 2. Encoding

```
1.   binary[] encodedText;
2.   for (int i=1; i<= (plaintext.Length)-1; i++)
2.1.      {
2.2.      Assume new node z;
2.3.      Z_left = X = Min(plaintext);
2.4.      Z_right = Y = Min(plaintext);
2.5.      Z_prop = X_prop+Y_prop;
2.6.      Insert Z into encodedText;
2.7.      };
```

Algorithm 3. Blocking and split blocks

```
1.   binary blockedText[] = encodedText;
2.   int padding = (encodedText.Length) mod 256;
3.   if (padding != 0)
3.1.      {
3.2.      binary paddedBits[256-padding] = 0;
3.3.      Append paddedBits to blockedText;
3.4.      };
4.   int blockCount = (blockedText.Length) / 256;
5.   binary blockedText1[(blockCount / 2) * 256];
6.   binary blockedText2[(blockCount - (blockCount / 2)) *
256];
7.   Copy blockedText from 0 to blockedText1.Length index
into blockedText1;
     8.   Copy blockedText from blockedText1.Length+1 to
blockedText.Length index into blockedText2;
```

Algorithm 4. Rijndael encryption

```
1.   binary[] resultBlock = inputBlock;
2.   for(n=1; n<=14; n++)
2.1.{
2.2.      binary[] extendedKey;
2.3.      binary block[];
2.4.      resultBlock=extendedKey[n]+resultBlock;
2.5.      S-Box_n(resultBlock);
2.6.      Shift_n(resultBlock);
2.7.      if(n != 14)
2.7.1.            {
2.7.2.            MixColumn_n(resultBlock);
2.7.3.            };
2.8.      };
```

Algorithm 5. ECDH

```
1. int d_A,Q_A,d_B,Q_B; // domain parameters of an elliptic curve
2. int K = (x_K,y_K) = d_A×Q_B;
3. int L = (x_L,y_L) = d_B×Q_A;
4. int keyForRijndael = x_K;
```

Algorithm 6. RSA

```
1. int p,q; //p and q are prime numbers
2. int n = p×q;
3. int lmbda(n) = LCM(p-1, q-1);
4. find e where GCD(e, lmbda(n)) =1;
5. int d = e^-1 mod lmbda(n);
6. (n, e) is private Key;
7. (n, d) is public Key;
```

5. Comparison

In the proposed algorithm, the advantages of symmetric and asymmetric encryption algorithms are combined to establish the three principles of confidentiality, authentication and integrity. Furthermore, the limits of wireless sensor networks are considered in the exchange and transfer of information. The cryptographic process is performed using the Rijndael algorithm with 256-bit blocks. Rijndael algorithm is a high speed symmetric encryption algorithm and variation in implementation. Based on Kerckhoffs's principle, the security of a cryptographic system depends on maintaining the confidentiality of the encryption key. In the proposed algorithm, the encryption key required by the Rijndael algorithm is provided in two ways. The reason for doing this is to increase the security of the key exchange in the wireless network. If the encryption key is identified for some of the blocks of information, since the key exchange process of the other information blocks is different, it will not be possible for the attacker to recover all information.

6. Time Complexity

The time complexity of an algorithm is the quantity that represents the amount of time consumed to run that algorithm as a function of the input string size. The time complexity of an algorithm is usually expressed by a large O that overlooks the lower-order coefficients and phrases. This display method is an asymptotic description of the complexity of time. For example, if the time needed to run an algorithm for all inputs $n > n_0$ is equal to $an^3 + bn$, the asymptotic time complexity is equal to $O(n^3)$. a, b and n_0 are constant values. The complexity of the time is estimated by counting the number of main operations of the algorithm.

The proposed hybrid encryption algorithm consists of an encoding algorithm, a symmetric encryption algorithm, two asymmetric encryption algorithms for key exchange. The time complexity of Huffman's algorithm is O(nlogn). A stack is used to store the weight of each node. The time complexity is to determine the lowest weight and add new weight O(logn) and the time complexity of cycles O(n). Rijndael's algorithm consists of 14 rounds and four distinct operations per round. Operations are all of a mapping type by a predefined table or a linear operation, resulting in a time complexity of O(14n). The time complexity of the elliptic curve encryption algorithm is equal to $O(\sqrt{n})$ and the time complexity of the RSA algorithm is $O(\log n^2)$. The remaining operations are linear and do not affect time complexity, because their grades are in the degree of other operations affecting the algorithm is less. Other operations, such as dividing the information string into two categories, blocking, padding with 0, etc., are all constant; therefore, their complexity is equal to O(k), so that k is the fixed number of the input string function. In general, the time complexity of the entire algorithm is equal to O(nlogn). The proposed algorithm has a good time complexity compared with

other proposed algorithms in recent years. While the proposed algorithm is more secure than other hybrid algorithms provided on the communication platform of wireless sensor networks, it fully enforces the three principles of confidentiality, authentication and integrity.

7. Memory Consumption

A hypothetical information string has 446 characters, and an ASCII encoding system needs to store 446 bytes or 3568 bits of space in the physical memory. However, in the proposed algorithm, the final file needs 285 bytes or 2280 bits of space for storage in physical memory. The proposed algorithm has a variable-length encoding system, and in this string of information, about 36% of the memory consumption is saved.

In the table below, the number of information blocks for transmission in a wireless sensor network is compared in several blocking methods for the hypotheses' string:

Table 1. Different blocking methods for hypothetical information

Blocking Method	Block size	Padding bits	Number of Blocks
64-bit	64	48	56
128-bit	128	112	28
256-bit	256	240	14
Proposed method	256	232	9

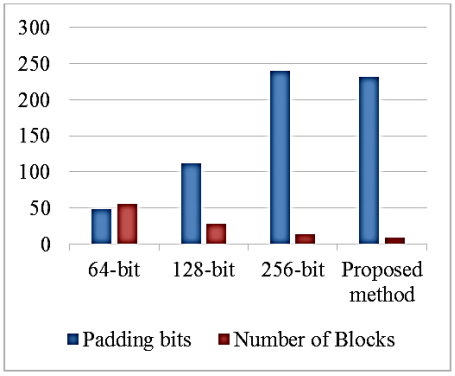

Fig. 2. Different blocking method chart for hypothetical information

The number of transition blocks in the proposed algorithm is lower than in other blocking methods. Typically, the DES encryption algorithm contains 64-bit blocks, the AES encryption algorithm has 128-bit blocks, and the Rijndael encryption algorithm has 256-bit blocks. By increasing the size of blocks, the probability of increasing the number of layers of bits in the final block increases, which only affects the final block, and its number is entirely dependent on the length of information string. The table above is achieved without regard for integrity, and it only considers the enclosed blocks of information to be transmitted. The hash algorithms also create additional information blocks to encrypted information blocks and transfer them to the wireless communication platform for integrity and authentication purposes. In the following table, several blocking methods in combination with the hash algorithms and the number of final blocks for transmission of the encrypted information strings are specified:

Table 2. Different blocking methods with hash algorithms for hypothetical information

Blocking Method	Hash Algorithm	Number of Final Blocks
64-bit	MD5	112
64-bit	SHA1	196
64-bit	SHA-256	280
128-bit	MD5	42
128-bit	SHA1	63
128-bit	SHA-256	84
256-bit	MD5	18
256-bit	SHA1	23
256-bit	SHA-256	28
Proposed method	SHA-256	18

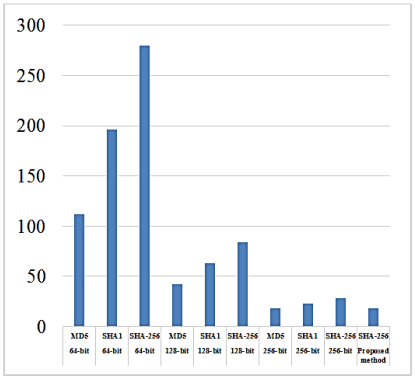

Fig. 3. Different blocking method chart with hash algorithm for hypothetical information

Because the length of final information string in the hybrid method for authentication and integrity is only dependent on the hash algorithm, only the hash algorithms are defined in the table above. The number of blocks in the 256-bit blocking methods with the MD5 and SHA1 hash algorithms is lower than the proposed algorithm. The MD5 algorithm is currently broken, and the SHA1 algorithm is broken in certain conditions. As a result, they will not be a good choice in terms of security.

The proposed algorithm provides three principles of cryptography: confidentiality, integrity, and authentication with the optimal number of blocks of information.

8. Time Consumed

The proposed algorithm consists of the steps for reading the information file, encoding, blocking, dividing the information blocks into two groups, encrypting the first group of information blocks and generating the corresponding digital signature, and encrypting the second group of information blocks and generating the corresponding digital signature. In ten times the implementation of the algorithm, the measured consumption times are shown in the table below:

Table 3. Results of ten times implementation of the proposed algorithm

Implementation	Reading information	Encoding	Blocking	Split blocks	First encryption	Second encryption	Total
1	0.2135	1.5627	0.0347	0.0033	441.9149	103.4469	547.176
2	0.1961	1.8367	0.036	0.0043	413.9018	103.8879	519.8628
3	0.2078	2.9879	0.0347	0.0033	427.2974	102.6035	533.1346
4	0.2071	1.6052	0.0277	0.0033	416.0835	120.1658	538.0926
5	0.1948	2.6196	0.0417	0.003	415.6013	99.2333	517.6937
6	0.1851	1.51	0.0307	0.0026	393.9851	99.4391	495.1526
7	0.2522	1.9788	0.0414	0.003	491.8431	103.231	597.3495
8	0.2071	2.0696	0.0357	0.003	399.3358	105.4186	507.0698
9	0.1921	1.8698	0.033	0.004	590.7126	101.8583	694.6698
10	0.1917	1.5561	0.04	0.003	405.2739	97.8342	504.8989
Average	0.2047	1.9596	0.03556	0.00328	439.5949	103.7119	545.51003

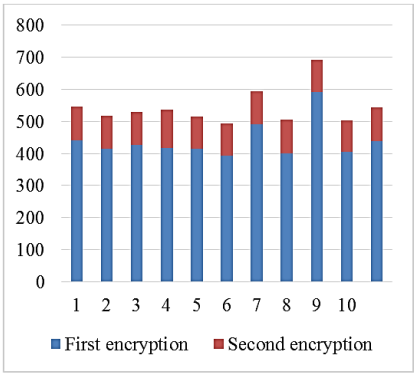

Fig. 4. Chart of results of ten times implementation of the proposed algorithm

The unit of measurement for the time consumed in each step is based on milliseconds. The first and second encryption steps take most time to execute the algorithm. As a result, only two of most influential factors are considered in the above diagram. The RSA algorithm uses longer time to encrypt longer strings than ECC algorithm. Naturally, there is a direct relationship between the increased security of data transmission and the time consumed. In the proposed algorithm, there is a balance between the time consumed and the increased security of data transmission, so that the cryptographic key for half of the information is rapidly distributed, and half of the information is distributed securely. The distribution of the encryption key in two ways has also helped to increase the security of the proposed algorithm.

9. Conclusion

In this research, a comprehensive and optimized solution for reliable data and secure, fast and timely data transmission is the use of wireless sensor networks. Wireless sensor network technology has been gaining great importance over the years, due to the advancement of technologies associated with this technology such as the ability to measure, communicate protocols, processor speeds, embedded systems, and more. Wireless sensor networks are new technologies that are used for various purposes. Wireless sensor networks are vulnerable to various attacks in different layers. Cryptography is one of the methods for secure transmission of information between sensors in wireless sensor networks. A complete and secure encryption system must establish three principles of confidentiality, authentication and integrity. Cryptography is a knowledge of hiding information and verification, and includes protocols, algorithms and secure strategies to prevent unauthorized access to critical information. Encryption provides a mechanism for verifying the components of a connection. An encryption algorithm alone cannot provide all of the principles of encryption. A hybrid encryption algorithm, consisting of symmetric and asymmetric encryption algorithms, provides complete security for a cryptographic system. The papers presented in this area over the past few years, and a new secure algorithm is presented that provide three cryptographic principles. The proposed algorithm is presented with regard to the limitations of wireless sensor networks. The proposed algorithm has optimum time complexity, time and memory usage. The details of the algorithm and basic concepts are presented in such a way that it is possible to implement the algorithm operationally.

Many advantages of the proposed algorithm are presented. Computer science is very broad and covers a variety of topics. There are many ideas to improve the performance of hybrid encryption algorithms in securing the transmission of data between sensors in wireless sensor networks. Some of them can be the basis for future research.

The use of compression algorithms reduces the amount of memory usage and the number of transition blocks in the communication platform of the wireless sensor network. Compression algorithms have complex operations that use sensor processing resources. Hence, the use of a compression algorithm commensurate with the limits of wireless sensor networks helps to improve the performance of a hybrid encryption system.

A high-security encryption system is also used for wireless sensor networks in other networks. As a result, modifying and improving algorithms helps to provide more security in monitoring systems.

References

[1] M. Panda, "Security in wireless sensor networks using cryptographic techniques," American Journal of Engineering Research (AJER), vol. 3, pp. 50-56, 2014.

[2] L. D. Singh and K. M. Singh, "Implementation of Text Encryption using Elliptic Curve Cryptography," Procedia Computer Science, vol. 54, pp. 73-82, 2015/01/01/ 2015.

[3] L. D. Singh and K. M. Singh, "Image Encryption using Elliptic Curve Cryptography," Procedia Computer Science, vol. 54, pp. 472-481, 2015/01/01/ 2015.

[4] G. R. Patel and K. Panchal, "Hybrid Encryption Algorithm," International Journal of Engineering Development and Research (IJEDR), vol. 2, pp. 2064-2070, 2014.
[5] M. Shankar and P. Akshaya, "Hybrid Cryptographic Technique Using RSA Algorithm and Scheduling Concepts," International Journal of Network Security & Its Applications, vol. 6, p. 39, 2014.
[6] S.-h. Zhu, "Research of hybrid cipher algorithm application to hydraulic information transmission," in Electronics, Communications and Control (ICECC), 2011 International Conference on, 2011, pp. 3873-3876.
[7] K. Brindha, G. Ramya, and R. A. Jayantila, "Secured Data Transfer in Wireless Networks Using Hybrid Cryptography," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, 2013.
[8] R. Singh, I. Panchbhaiya, A. Pandey, and R. H. Goudar, "Hybrid Encryption Scheme (HES): An Approach for Transmitting Secure Data over Internet," Procedia Computer Science, vol. 48, pp. 51-57, 2015/01/01/ 2015.
[9] P. Kuppuswamy and S. Q. Al-Khalidi, "Hybrid encryption/decryption technique using new public key and symmetric key algorithm," International Journal of Information and Computer Security, vol. 6, pp. 372-382, 2014.
[10] S. Subasree and N. Sakthivel, "Design of a new security protocol using hybrid cryptography algorithms," IJRRAS, vol. 2, pp. 95-103, 2010.
[11] M. J. Dubai, T. Mahesh, and P. A. Ghosh, "Design of new security algorithm: Using hybrid Cryptography architecture," in Electronics Computer Technology (ICECT), 2011 3rd International Conference on, 2011, pp. 99-101.
[12] K. Yaeghoobi SB, M. Soni, S. Tyagi, and O. M. Ebadati E, "SAERP: An energy efficiency Real-time Routing protocol in WSNs," in 2014 International Conference on Reliability Optimization and Information Technology (ICROIT), 2014, pp. 249-254.
[13] B. S. Dhaliwal and V. Soi, "Reprogramming of Wireless Sensor Network Securely with New Hybrid Encryption Scheme," International Journal of Engineering Technology, Management and Applied Sciences (IJETMAS), vol. 3, pp. 258-263, 2015.
[14] A. Bhave and S. Jajoo, "Secure Communication in Wireless Sensor Network using Symmetric and Asymmetric hybrid Encryption Scheme," International Journal of Innovative Science, Engineering & Technology (IJISET), vol. 1, pp. 382-385, 2014.
[15] K. Yaeghoobi SB, M. Soni, S. Tyagi, and O. Ebadati E, "Impact of NP-complete in triangle segments tree energy efficiency model in wireless sensor networks," J. Basic Appl. Sci. Result, vol. 3, pp. 808-817, 2013.
[16] R. Sharmila and V. Vijayalakshmi, "Hybrid Key Management Scheme for Wireless Sensor Networks," International Journal of Security and Its Applications, vol. 9, pp. 125-132, 2015.
[17] M. Yazdinejad, F. Nayyeri, and N. Afshari, "Secure Distributed Group Rekeying Scheme for Cluster Based Wireless Sensor Networks Using Multilevel Encryption," in Internet of Things: Novel Advances and Envisioned Applications, ed: Springer, 2017, pp. 127-147.
[18] W. Ren and 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 (WMSVM 2010), 2010, pp. 221-225.
[19] K. Rege, N. Goenka, P. Bhutada, and S. Mane, "Bluetooth communication using hybrid encryption algorithm based on AES and RSA," International Journal of Computer Applications, vol. 71, pp. 10-13, 2013.
[20] Monika and S. Upadhyaya, "Secure Communication Using DNA Cryptography with Secure Socket Layer (SSL) Protocol in Wireless Sensor Networks," Procedia Computer Science, vol. 70, pp. 808-813, 2015/01/01/ 2015.
[21] R. Rizk and Y. Alkady, "Two-phase hybrid cryptography algorithm for wireless sensor networks," Journal of Electrical Systems and Information Technology, vol. 2, pp. 296-313, 2015.

Omid Mahdi Ebadati E. earned his Ph.D. degree in computer science with network security expertise from Hamdard University, New Delhi, India. He is currently an assistant professor and head of information and communication technology center at Kharazmi University, Tehran. He is a senior member of IEEE and the Computer Science Association of America and India. He has published numerous research papers in peer-reviewed international journals and conferences and published books and chapter books in the field of Computer Networks, Internet of Things, Cloud Computing and Machine Learning.

Farshad Eshghi earned his Ph.D. degree in telecommunications engineering from Concordia University, Montreal, QC, Canada. He is a member of IEEE, IEEE communications society, and IEEE computer society and is currently an assistant professor at Kharazmi University. He has published dozens of research papers and books in international journals and conferences on MAC/Routing Protocols in Ad Hoc WLANs/WSNs Cooperative Transmission in Ad Hoc WLANs, Localization in Wireless Networks, Intelligent Building Management Systems and Intelligent Transportation Systems.

Amin Zamani earned a Master degree in computer science from Kharazmi University, Tehran, Iran. His current research interests are in the areas of wireless sensor networks, information security and cryptography.