International Journal of Control Theory and Applications

ISSN : 0974–5572

Volume 9 • Number 40 • 2016

Hybrid Key Encryption using Cryptography for Wireless Sensor Networks V-Algorithm

D. Anitha[a] S. Aruna[a] Mathew[a] K. Mathew[a] and Devilal[a]

E-mail: anitha.d@ktr.srmuniv.ac.in, aruna.s@ktr.srmuniv.ac.in, mathu95@gmail.com, devandermali556@gmail.com

Abstract : Wireless Sensor Networks consists of nodes which are equipped with inadequate battery power, low memory, limited computation and communication range. The sensed information should be accessed in a secure manner. Energy efficient secure routing is a major issue in wireless sensor networks. Hybrid key encryption is a technique which is commonly used these days by almost all the organizations such as the military, health and traffic. Many hybrid key schemes have been implemented in the past in order to strengthen the signals between existing wireless sensors. In order to address the issues in the existing system, V-Algorithm is proposed which will encrypt each message using vowels as keys. Few of the existing algorithms will be considered for this study and will be compared with the proposed algorithm to show its efficiency. The proposed algorithm will be helpful to increase the security and efficiency of the message being transmitted in a wireless sensor network.

Keywords: *Wireless Sensor Networks, Hybrid Key Encryption, Cryptography, V-Algorithm.*

1. INTRODUCTION

The Wireless Sensor Networks (WSNs) are mostly used in the applications of hostile environment, military, mission critical and personal tracking. The sensor nodes are typically constrained in their communication, computation, limited memory and power resource. The sensor nodes are deployed in an unattended area; the risk of physical attacks is high and securing the sensor network is difficult due to the limitations of resource constraint device. Sensor networks cannot work with the conventional cryptography methods. Key management scheme is the only solution for resource constrained device. In order to conduct secure communication in WSNs, the key has to be exchanged securely before the exchange of information takes place. Many key management schemes have been proposed for wireless sensor networks. The key management is a way to generate cryptographic keys. The Wireless Sensor Networks (WSNs) are mostly used in the applications of hostile environment, military, mission critical and personal tracking. The sensor nodes are typically constrained in their communication, computation, limited memory and power resource. The sensor nodes are deployed in an unattended area; the risk of physical attacks is high and securing the sensor network is difficult due to the limitations of resource constraint device. Sensor networks cannot work with the conventional cryptography

methods. Key management scheme is the only solution for resource constrained device. In order to conduct secure communication in WSNs, the key has to be exchanged securely before the exchange of information takes place. Many key management schemes have been proposed for wireless sensor networks. The key management is a way to generate cryptographic keys.

The key management scheme consist of four phases; key predistribution, key establishment, node addition and node eviction or refresh. Based on the encryption techniques the key management scheme is classified into three types as; symmetric key management, asymmetric management and hybrid key management techniques. In the symmetric key management scheme, both the sender and receiver share a common key for encryption and decryption. Although the technique is reliable and rapid fast, it lacks resilience, scalability and connectivity. The main drawback is that the sender and receiver should exchange the key in secure manner.

Two different types of keys are used in asymmetric based cryptography method. The key used for encryption is called as public key and for decryption is private key. The Ron Rivest, Adi Shamir and Leonard Adleman (RSA), Elliptic Curve.

Cryptography (ECC) and Hyperelliptic Curve Cryptography (HECC) are popular public key cryptography methods. Recently many researchers proved that the public key cryptography is suitable for resource constrain networks. Both of the symmetric and asymmetric schemes have trade-offs between the security and its resources. A hybrid key technique is combination of symmetric and public key cryptography scheme. These problems are overcome by means of combining asymmetric key predistribution with symmetric key generation using genetic algorithm for tiny wireless sensor network.

The main influence of this paper is:

1. Is to combine an already existing algorithm with the proposed algorithm to further encrypt the messages.
2. To compare the already existing algorithms with the proposed algorithm to check its efficiency.

2. RELATED WORKS

There are many encryption algorithms that are present around the world that are being used in various segments of industry such as traffic, health and military. Now when it comes to encryption there are basically 3 types of encryption that are there:

1. Symmetric Key Encryption
2. Asymmetric Key Encryption
3. Hybrid Key Encryption

3. EXISTING ALGORITHMS

3.1. AES Algorithm

The Advanced Encryption Standard (AES) algorithm, which is also known as Rijndael, is a block cipher that was adopted as an encryption standard by the US government. AES is one of the most popular symmetric-key cryptography algorithms. AES is fast in both software and hardware and is easy to implement.

It operates on a 4 by 4 array of bytes and has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits with 10, 12, and 14 number of rounds . To encrypt, each round of AES (except the last round) consists of four stages. a) SubBytes - a non-linear substitution step in which each byte is replaced with another according to a lookup table b) ShiftRows - a transposition step in which each row of the state is shifted cyclically a fixed

number of steps. c) MixColumns – a mixing operation which operates on the columns of the state. It combines the four bytes in each column using a linear transformation. d) AddRoundKey - each byte is combined with the round key; each round key is derived from the cipher key using a key schedule. AES algorithm consists of various rounds depending on the key size and block size. Out of all the rounds the Pre- round comprises only AddRoundKey whereas the final round omits the MixColumns stage.

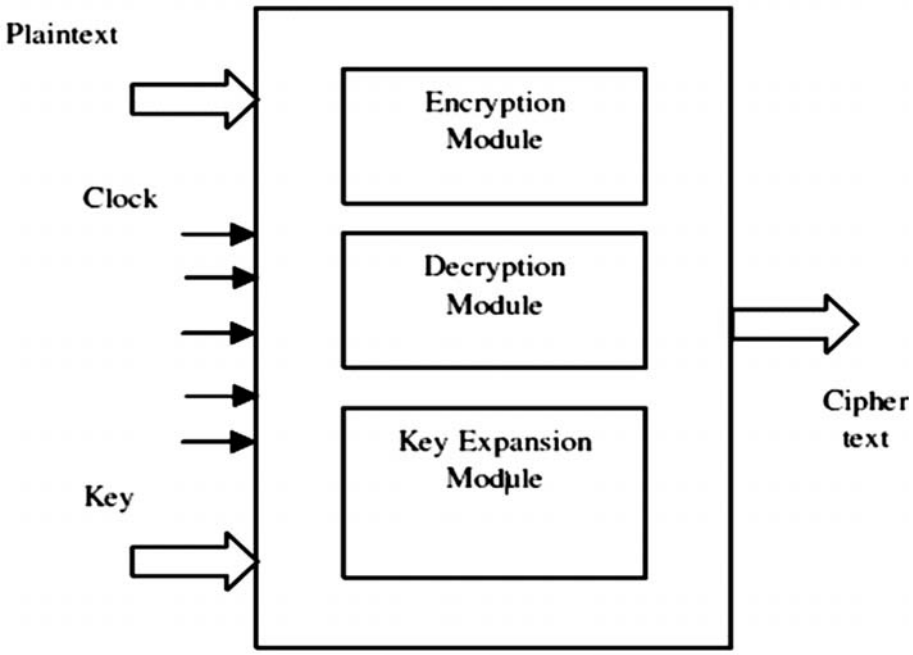

Figure 1: Demonstration of AES

3.2. RC5 Algorithm

RC5 is a fast symmetric block cipher suitable for hardware or software implementations. RC5 has a variable block size (32, 64 or 128-bits), key size (0 to 2040 bits) and number of rounds (0 to 255) . The original suggested choices of parameters were a block size of 64-bits, a 128-bit key and 12-rounds. It is fast symmetric block cipher suitable for hardware or software implementations. A novel feature of RC5 is the heavy use of data-dependent rotations. RC5 has a variable word size, a variable number of rounds, and a variable-length secret key.

The encryption and decryption algorithms are exceptionally simple. RC5 is not intended to be secure for all possible parameter values. On the other hand, choosing the maximum parameter value will be overkill for most applications. RC5 is hard to use in open environments and oneshot communications. 12-round RC5 (with 64-bit blocks) is susceptible to a differential attack using 244 chosen plaintexts. 18-20 rounds are suggested as sufficient protection.

A distinguishing feature of RC5 is its heavy use of data dependent rotation. The amount of rotation performed is dependent on the input data and it's not pre-determined. Word size, number of rounds and key size of RC5 can be varied. The different combinations of values for these parameters are used to fully understand their influence on the energy consumption caused by the encryption algorithm: 1. The usual word size for encryption is 32 bits (4 bytes) to study the impact of the word size on the time it takes to perform key setup, encryption, and decryption. 2. The number of rounds (4, 8, 12, 16, 18) has a proportional effect on the security of RC5. 3. RC5 also uses different key sizes as AES.

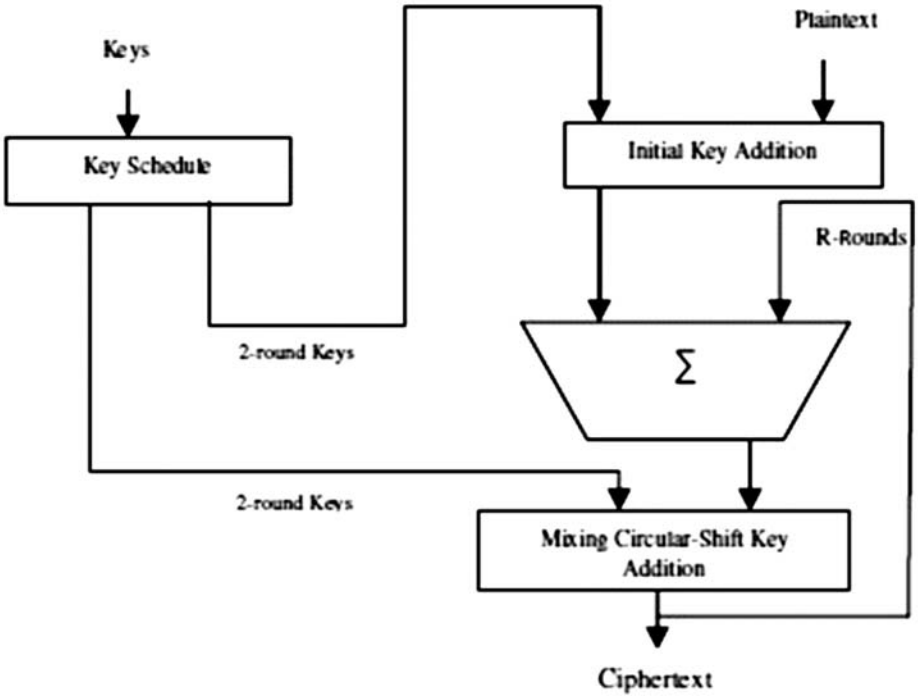

Figure 2: RC5 Algorithm demonstration

3.3. Skip Jack

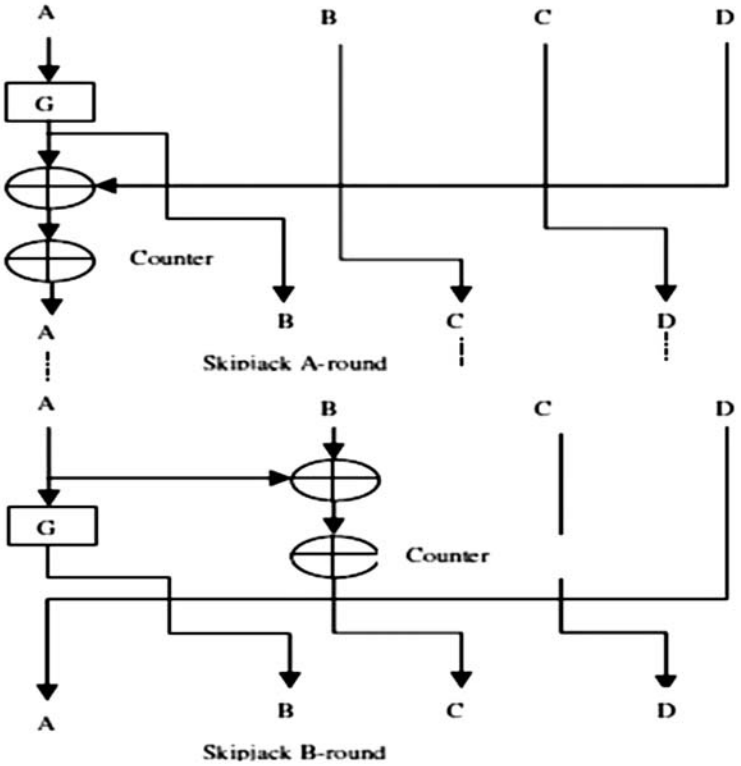

Figure 3: Skip Jack demonstration

Skipjack uses an 80-bit key to encrypt or decrypt 64-bit data blocks. It is an unbalanced Feistel network with 32 rounds. It has been found that the number of rounds is exponentially proportional to the amount of time required to find a key using a bruteforce attack. So, as the number of rounds increases, the security of the algorithm increases exponentially. Skipjack uses FBOX which can be stored in either RAM or program memory.

$$(a, b, c, d) = (d + Gk(a) + \text{counter}, GK(a), b, c);$$
$$(a, b, c, d) = (d; Gk(a); a + b + \text{counter}; c): A{-}1(a, b, c, d)$$
$$= (G - 1k(b); c; d; a + b + \text{counter});$$
$$B\text{-}1(a, b, c, d) = (G - 1k(b); c + G - 1k(b) + \text{counter}; d; a):$$

3.4. Hight

HIGHT has 64-bit block length and 128-bit key length, which is suitable for low-cost, low power and ultra-light implementation. 32-round iterative structure which is a variant of generalized Feistel network. The hardware implementation of HIGHT requires 3048 gates on 0.25 μm technology. It has been analyzed for the security against various attacks. The strength of the HIGHT algorithm is evaluated with respect to differential attack, linear attack, truncated differential cryptanalysis, impossible differential cryptanalysis, saturation attack, boomerang attack, interpolation and higher order differential attack.

4. V-ALGORITHM

4.1. Introduction

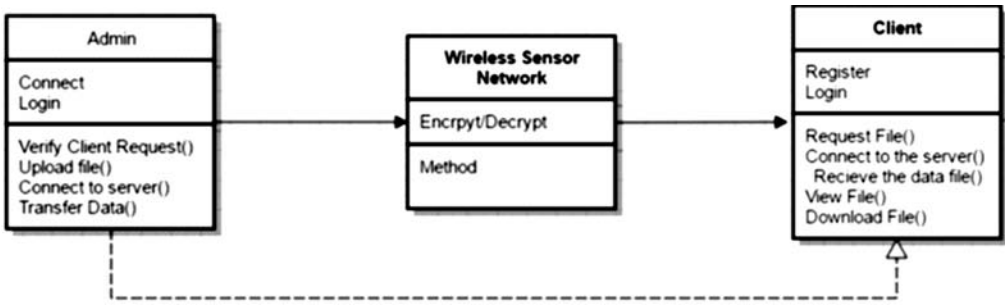

Figure 4: Class diagram of V-algorithm

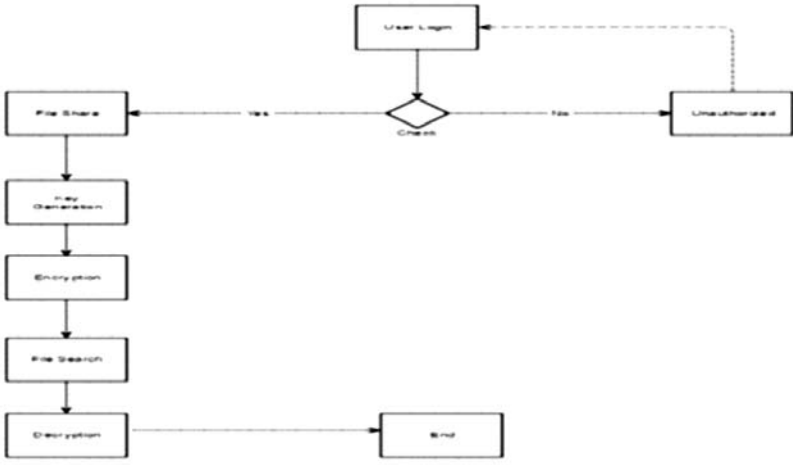

Figure 5: Data Flow diagram demonstrating V-algorithm

The V-Algorithm or the proposed algorithm works with using vowels as keys that are used to encode and decode the messages that are being transmitted through the wireless sensor networks.

The V-Algorithm, when received a message, first transfers the give word into an array.

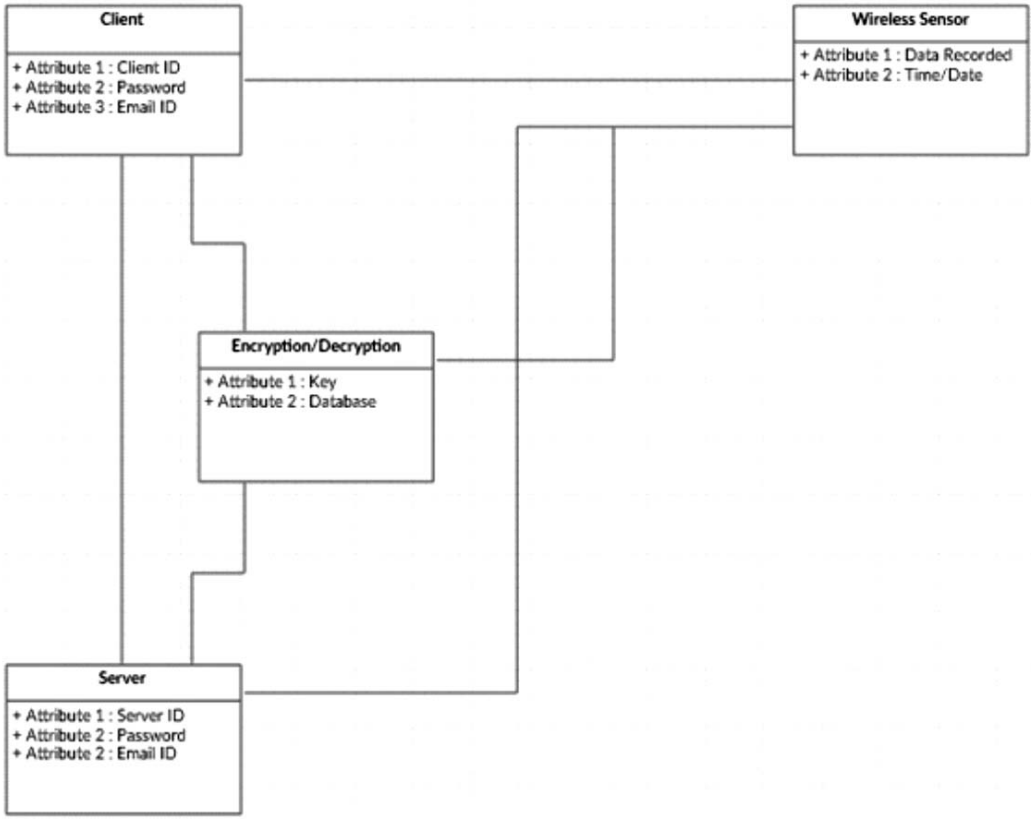

Figure 6: Relational Model diagram

Using a loop it goes through all thecharacters that are present in the word looking for vowels. Once a vowel is detected, the vowel is places into a new array along with the position of the index number of the vowel. This is repeated till the all the vowels have been placed in the new array along with their respective index numbers at the end of the array. The rest of the consonants are taken and reversed in order and placed in the new array to form the new encrypted message. For example given the word "hello" the decrypted message would be "eollh14".

4.2. Encoding Algorithm

1. Compute T(n)
   Compute A(n) = T(n + sum)
   End
2. Compute the size of the given array = n
3. for(i = 0 ; i < n ; i ++) if(T(i) == {a,e,i,o,u})
   sum = sum + 1
   T(i) = A (i) A (n) = i else if
   sum = sum
   A(n - sum) = T(i)
4. End

4.3. Decoding Algorithm

1 Compute A(n) = T(n - sum)

End.

2. for(i = 0 ; i < n ; i ++) if (T(i) == number) sum = sum + 1 End.

3. for(i = 0 ; i < n ; i ++) if(T(i) == {a,e,i,o,u}) A(sum) = T(i) else

A(i ++) = T(--i)

4.4. Proposed Method

Since using only one encryption technique to encrypt the messages that are sent between wireless sensors is not secure enough in some fields such as military, we propose to use the V-Algorithm combined with another already existing algorithm to encrypt and decrypt the messages.

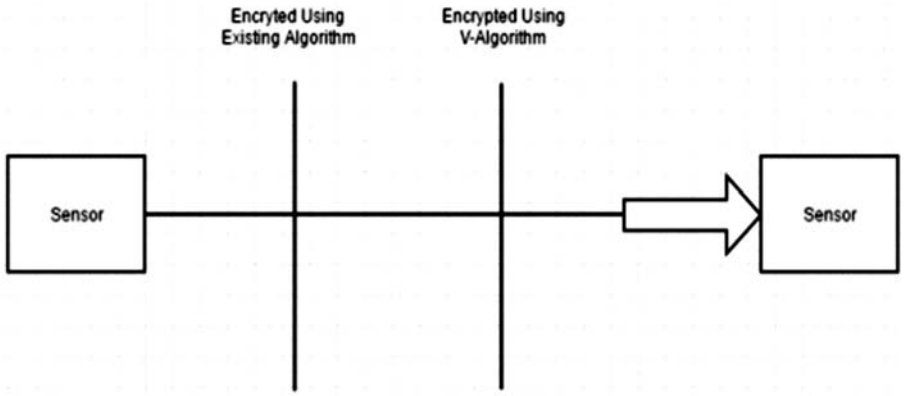

Figure 7: Proposed method

As the diagram shows when the signal is passed from one sensor node to another sensor node it will be first encrypted using an already existing algorithm and then after that will be further encrypted using the VAlgorithm to secure the message that is being sent even more.

4.5. Experimental Results and Comparison

Table 1

Input	*Expected Output*	*Actual Output*
Hello	Elloh14	Elloh14
Apple	Aellp04	Aellp04
Happy	Aypph1	Aypph1
Yakov	Aovky13	Aovky13

These are some of the samples of data that were used to test messages that were sent from the server to the client. These data were encrypted and decrypted using only the V-Algorithm.

5. CONCLUSION

For any Wireless Sensor Network the battery life time and the energy of the network are limited. In this paper, it is shown that the proposed V-Algorithm helps to improve the security of the messages that are transmitted through sensor nodes are further encrypted with the help of the VAlgorithm.

The main aim of the proposed algorithm is to be combined with an already existing algorithm to make sure that the messages are encrypted twice which makes sure that cracking these messages will become close to impossible. Such conditions can be used by the military for transmitting sensitive messages from sensors.

REFERENCES

[1] R.Sharmila and V.Vijayalakshmi, "Hybrid Key Management Scheme for Wireless Sensor Networks", from the " International Journal of Security and Its Applications" in 2015

[2] A. Babu Karuppiah, Dr. S. Rajaram, "Energy Efficient Encryption Algorithm for Wireless Sensor Network", from the International Journal of Engineering Research & Technology (IJERT) in May 2012.

[3] R.PushpaLakshmi, Dr.A.Vincent Antony Kumar, "Cluster Based Composite Key Management in Mobile Ad Hoc Networks" from International Journal of Computer Applications (0975 – 8887) in July 2010

[4] Mrs.A.S. Bhave, Mr.S.R.Jajoo, " Secure Communication in Wireless Sensor Network using Symmetric and Asymmetric hybrid Encryption Scheme" from IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 4, June 2014.

[5] M. Rajalakshmi, C. Parthasarathy and R.V. Indrajith, "Advanced Cryptographic Algorithm to Secure the Sensor Node Data in Wireless Sensor Networks" fromMiddle-East Journal of Scientific Research 24 (6): 1926-1931, 2016

[6] Bharat Singh, Parvinder Singh & Dr. V.S. Dhaka, "Sensor Data Encryption Protocol for Wireless Network Security" from Global Journal of Computer Science and Technology Volume 12 Issue 9 Version 1.0 April 2012.