International Journal of Security and Its Applications
Vol.9, No.11 (2015), pp.125-132
http://dx.doi.org/10.14257/ijsia.2015.9.11.13

Hybrid Key Management Scheme for Wireless Sensor Networks

R.Sharmila[1] and V.Vijayalakshmi[2]

[1]*Research Scholar, Department of ECE,*
Pondicherry Engineering College, Puducherry
[2]*Assistant Professor, Department of ECE,*
Pondicherry Engineering College, Puducherry
[1]*sharmila1ece@gmail.com;*
[2]*vvijizai@pec.edu*

Abstract

Many key management schemes have been proposed in systematically deployed Wireless Sensor Networks (WSNs).The sensor nodes are equipped with inadequate battery power, low memory, limited computation and communication range. Energy efficient secure routing is major issue in wireless sensor networks. In this paper, the hybrid key management scheme is proposed by combining public key cryptography scheme with symmetric scheme. The symmetric keys are generated by using genetic algorithm. Initial input for the genetic algorithm is the seed key generated by Hyperelliptic Curve Cryptography (HECC).The proposed scheme addresses the energy efficiency, resilience against node capture attack, key refreshment between the cluster head and member nodes in the cluster. The simulation results show that the hybrid scheme is more robustness, efficient energy with reduced key size.

Keywords*: key management, wireless sensor networks, genetic algorithm, Hyperelliptic curve cryptography, key refresh*

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. The conventional cryptography methods are not suitable for sensor networks. Key management scheme is the only solution for resource constrained device. To achieve secure communication in WSNs, the key has to exchange securely before they exchange information. Many key management schemes have been proposed for wireless sensor networks. The key management is a technique to generate the cryptographic keys, distributed, exchanged between the nodes, used, abolished and refreshed the 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.

In asymmetric based cryptography method, two different types of keys are used. The

ISSN: 1738-9976 IJSIA

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 the symmetric and asymmetric schemes have trade-off between the security and its resources are constraint.

A hybrid key technique is combination of symmetric and public key cryptography scheme. Most of the conventional cryptography schemes are not suitable due to more memory and high energy consumption. These problems are overcome by means of combining asymmetric key predistribution with symmetric key generation using genetic algorithm for tiny wireless sensor network.

The Genetic Algorithm (GA) is a Meta heuristic random search algorithm and optimization method depend on natural selection method [5]. It is a vital tool for resolving optimization problem due to its sturdiness. The basic operation of Genetic algorithm comprised into selection of chromosomes, crossover and mutation. A random key is generated using the randomness operations of genetic algorithm. The hybrid scheme is further divided into three parts: sensor node communication, intracluster communication and intercluster communication. Before the sensor nodes are deployed in the field, the server generates the key using Hyperelliptic curve based cryptography scheme and predistributed into the nodes. Once nodes are deployed in the field, it tries to communicate with their neighbors and base station. Each node is preloaded with unique seed key and shared key to communicate with base stations. Once nodes establish the secure communication with its neighbor and it sends neighbor information to the base station. Base station knows the complete topology of the network. In any routing protocol, base station can initiate creation of routing path.

In this paper, the hybrid key management using genetic algorithm for hierarchical sensor networks is proposed. The secure intra and inter clustering problems are analyzed based on the hybrid key management protocol using genetic algorithm.

The main influence of this paper is:

(i) The keys are established using HECC based key generation and predistribution

(ii) A novel key management scheme is proposed to integrate the advantages of Hyperelliptic curve based key predistribution scheme and symmetric key generation using genetic algorithm for secure WSNs.

(iii) A novel Hybrid algorithm is proposed to describe the convention of combining genetic algorithm with public key cryptography. It can be suitable for image and text encryption. This scheme is suitable for WSNs as well Wireless Multimedia Sensor Networks (WMSNs).

(iv) Algorithm is strengthened by a predefined permutation factor agreed upon by cluster head and member nodes. It is robust and hard to break.The rest of the paper is organized as follows: In section 2, the possibilities of existing key predistribution scheme and key generation scheme for WSNs are detailed. Section 3 offers the novel key establishment using HECC, Symmetric Key generation and refreshment using genetic algorithm. Section 4 provides the performance analysis of the proposed scheme. Finally, Section 5 concludes the paper.

2. Related Works

The existing public key cryptography techniques are DES, AED, DSA and RSA provides secure communication. The cryptographic techniques require larger key size to provide higher level of security. So these techniques are not suitable for wireless sensor networks. It requires more computational power and more processing time for encryption

and decryption of data. RSA algorithm was first developed in 1977[1]. The key sizes used in the RSA algorithm is 512 to 2048 bits. In this method, the message (m was encrypted using the key k and obtained the cipher text c. Then the two prime numbers p and q were multiplied together to get the modulus n. The modular multiplication thus derived, lowered the computation time by ¾ and complexity by 25%.

Watro *et al*. proposed the Tinypk model based on RSA based cryptosystem. In the scheme the wireless sensor networks are secured using public key scheme. The public key protocols are allowed authentication and key agreement between the sensor nodes.

Gura *et al*. suggested that RSA and Elliptic Curve Cryptography (ECC) is possible using 8 bit CPU. It has advantage over RSA. The key size used in ECC is 160 bit keys size compared to the 1024 bit RSA keys [2]. Link layer encryption scheme engaged with suitable authentication mechanism provides solutions to many types of attacks. The standard link layer encryption is called as Tinysec. It was developed at university of California at Berkeley [1]. Tiny sec based on block cipher and keying mechanism; it is tightly coupled with the Tinyos. Tinysec allocates 80 bits for the key space, so adversary could theoretically have to do more number of operations to find the keys. Tinysec may reduce the message transmission and memory; it needs 7.9 KB of space on the mote from the 128kb of programmable rom and 4 kb of flash memory. Tinysec does not have perfect resilience and compromise single key, the rekeying is not possible. These limitations are overcome by Diffie-Hellman scheme to securely distribute the keys. The shortcoming of implementing this scheme is the computation overhead and memory. Running this algorithm on mica2 mote at full duty cycle, will decrease the life span quickly.

Tinyos is micro operating system mote developed by Berkeley for motes and now available for much other sensor nodes. The main advantage of Tinysec is before transmitting a packet; it encrypts the message using cipher block chaining mode with SKIPJACK. Along with encryption hash function is applied as CBC-MAC. Computations of this kind of scheme take large amount of memory space.

Recently elliptic curve cryptography has been proposed for wireless sensor network. It perform computation very fast, smaller keys (*i.e*., need less memory) and less bandwidth than RSA [3].A mica2 mote using ECC can reduce the key size.

Chien *et al*. (2009) proposed a GA based key management scheme for hierarchical wireless sensor networks [4]. In this scheme, using genetic algorithm the several key generating functions is generated and refreshed a key using key generating function.

Rahul *et al* proposed an algorithm [5] to enhance position of sensor nodes and improves the resilience against the malicious node using genetic algorithm.

Radhika *et al*. suggested an efficient intruder detection system [6] using genetic algorithm to find misbehavior's depends on node attributes. Sandeep *et al*. [7] proposed a random key generation based on artificial immune system for clustered sensor networks.

3. Proposed Hybrid Method

The proposed method is divided into two phases; Key Establishment phase and Generation of symmetric key. Each phase is discussed in detail below.

3.1. Key Establishment Phase

The key Establishment phase is further divided into three phases: 1. Key generation phase, 2.Key predistribution phase 3.Key agreement phase.

3.1.1. Key generation phase: Key predistribution carried out only once before the sensor nodes are deployed in an area. In this phase, the server generates a key pool using public key cryptography scheme, such as Elliptic Curve Cryptography and Hyperelliptic Curve Cryptography (HECC) scheme. The key establishment is carried out using HECC over prime field. Using HECC, the server generates the key pool and key rings are randomly

selected from the key pool and predistributed into the sensor nodes. The HECC *E* defined over a field G is a curve of genus g in the form,

$$E: y^2 + h(x)\,y = f(x) \tag{1}$$

Where degree of $f = 2g + 1$.

The genus curve 2, the value of $g = 2$ then $f = 2 \times 2 + 1 = 5$

$$y^2 = x^5 + h_3x^3 + h_2x^2 + h_1x + h_0(mod p) \tag{2}$$

Where h_1, h_2, h_3 are the coefficient from the finite field and p is the prime field.
In HECC, the group structure is defined by Jacobian divisor of hyper elliptic curve points. The divisor can be reduced by using Mumford representation. The polynomial equation *[m, n]* of the divisor is generated by Mumford representation. The seed keys are the coefficients of the polynomial *[m, n]*.The unique seed keys are assigned to the each sensor nodes before deployment.

3.1.2. Key ring generation phase: Once the seed keys are generated, the key ring is generated for the seed key using point addition and doubling using cantor's algorithm. The key rings are predistributed in the sensor nodes.

3.1.3. Key predistribution phase: Once the seed key and its corresponding key rings are generated, it is predistributed in the sensor nodes.

3.1.4. Key Agreement Phase: The sensor nodes are randomly deployed in the field, it tries to establish secure communication link by sharing its corresponding key ring identifier. If it fails to establish a communication link, using an intermediate node it establishes a secure communication with its neighbor nodes.

3.2. Symmetric Key Generation using Genetic Algorithm

The base station chooses the cluster head according to the routing algorithm [8] [9]. The base station knows the complete topology of a network. Once the cluster is formed, base station send the information to the cluster head about the member nodes and its unique keys. To provide secure communication, the base station knows the unique seed key of the nodes in the network. The seed keys are generated using HECC and distributed before the nodes deployed in an area. The cluster and member nodes in the network establish a new key by using genetic algorithm. In this section, the keys are generated for intra cluster communication to achieve greater resilience and authenticity of nodes.

3.2.1 Intra cluster communication: During the steady state phase, the member nodes want to communicate with cluster head has

(i) It randomly picks two numbers $(x, y)$from the unique key (m, n).
(ii) Calculate the intermediate value I between (x, y) ,it offers the randomness and depends on the robustness needed; $I = \frac{x + y}{2}$
(iii) Find $C = I\%l$, which provides the crossover ratio. Where l is the size of communication bit, here the value of $l = 8$.
(iv) Convert the decimal number into binary
(v) Generate the random symmetric key based on cross over, Mutation and its corresponding fitness check.
(vi) Calculate r and s
(vii) The key length is given by

$K = 3(C + M + 1)$ Where C and M are the crossover and mutation fitness.

(viii)

3.2.2. Crossover operation: To generate a new offspring, two keys are randomly chosen among the best parents of the population; here the best parent is key that chosen randomly from a unique key (m, n) and the crossover operation is performed on (x, y). Before performing the crossover operation, the chromosomes are encoded. They are many methods to encode chromosomes (*e.g*. binary encoding, permutation encoding, value encoding, tree encoding). In this paper, the binary encoding is performed. In the binary encoding, each chromosome's is a string of binary bit 0's and 1's.The genes in the chromosome are encoded into binary; the single point crossover operation is applied. The crossover fitness function is calculated by $C = I\%l$.The robustness can be increased by varying the number of points flipped in the crossover operation.

3.2.3. Mutation operation: After the crossover operation, each bit of an offspring is changed or swapped using mutation operator. In this mutation operation, the bits in the new offspring are complemented or swapped to evade repetition of individuals. It guarantees genetic variation within the population. Then, the fitness value is calculated for mutated offspring.

For example, the following steps ~~are~~ depicts the generation of symmetric key generation using asymmetric key cryptography and genetic algorithm:

Step 1: Seed key of sensor node $(m, n) = (0,21)$
Choose two random numbers from $(x, y) = (12,18)$
Find the intermediate value between $(x, y) = \frac{(12+18)}{2} = 15 = I$
Perform mod operation, $I\%8 = 7 = C_r$

Step 2: Cross over $(x, y) = (12,18)$
i. Convert decimal to binary value
12 0000 1100
18 0001 0010

ii. Mutual exchange bit from the position $C_r = 7$
0100 1100 76
0101 0000 80
iii. Calculate the fitness value $f_c = 80$; $(c, d) = (76,80)$

Step 3: Mutation $(c, d) = (76,80)$
The mutation rate is calculated by $(c, d) = \frac{(76+80)}{2} = 78 = M$
$M\%8 = 6 = M_r$
1. Convert number to binary
76 0100 1100
80 0101 0000
2. Find complement,
1011 0011 179
1010 1111 175
3. Calculate fitness value $f_m = 179$

Step 4: Calculate $r = \left(f_m/_2\right)$ and $s = (f_m\%2)$

Step 5: Random key length $K = 3(C_i + M_i + 1) = 9$

3. Simulation Results

In this section, the hybrid key management schemes for WSNs are simulated against resilience and energy consumption for different rounds to transmit and receive the packet for intracluster communication is measured. Then the important security analysis like message authentication and integrity are analyzed. The simulation results were analyzed in Matlab12b simulator. The algorithm was verified using LEACH protocol till 100 rounds for the proposed scheme, ECC and HECC. Table 1. depicts the radio characteristics and simulation parameters of the proposed scheme.

Table 1. Radio Characteristics and Simulation Parameters

PARAMETER	VALUE
Number of nodes	100
Transmitter electronics, Etx	50nJ/bit
Receiver electronics, Erx	50nJ/bit
E_{amp} (Amount of Amplifier Energy)	0. 0013pJ/bit
E_{fs} (Free space Energy)	10pJ/bit
Initial energy of the node	0.5J
Distance, d	50m
Packet Length in bit	32,80,160 bit

3.1 Energy Consumption Analysis of Cryptographic Scheme

The energy consumption analysis of the symmetric key generation using genetic algorithm is compared with ECC and HECC. The communication overhead to transmit and receive a packet based on the size of the key generated by a cryptography scheme is compared with proposed scheme. In the proposed method, the total size of key generated for intra cluster communication is 32 bits. The key size of ECC is 160 bits and for the HECC is 80 bits. The energy consumption to transmit and receive the 32 bit control packet of the symmetric key generation for 100 rounds is shown in Figure 1.

3.1.1 Message Integrity & Authenticity : Using the hybrid genetic algorithm, the message integrity and authentication are achieved efficiently. During the intraclustering phase or steady phase, the member nodes and cluster head has to authenticate each other by including the value of R and S in the trailer of packet. The security of hybrid genetic algorithm is directly associated to the length of MAC (4 byte).The normal traditional security protocol customs MACs of size 8 or 16 bytes. For the 4 byte, compromiser has a chance of 1 in 2^{32} thoughtlessly faking a MAC for particular message. The value of R and S are calculated using the fitness value of crossover c_r and mutation ratio m_r.

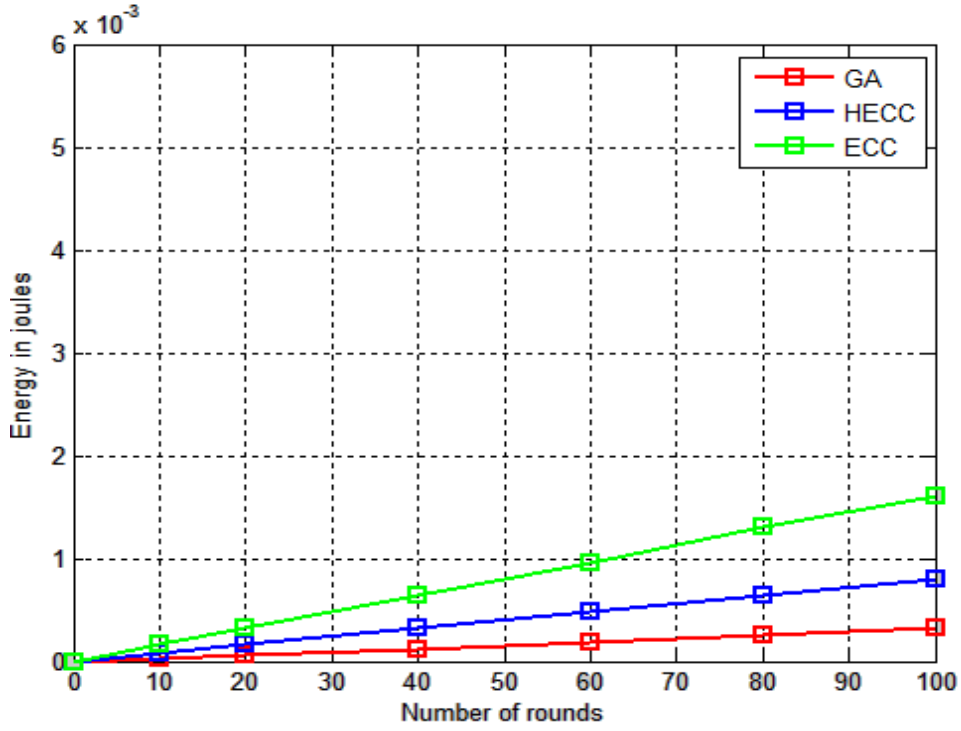

Figure 1. Total Energy Consumption for 100 Rounds for Different Cryptography Schemes

3.2 Resilience Against Node Capture and Cluster Head Attack

In the proposed method, each sensor node is predistributed with a unique key using HECC. It saves the memory of sensor nodes; it provides high resilience against node capture attacks.

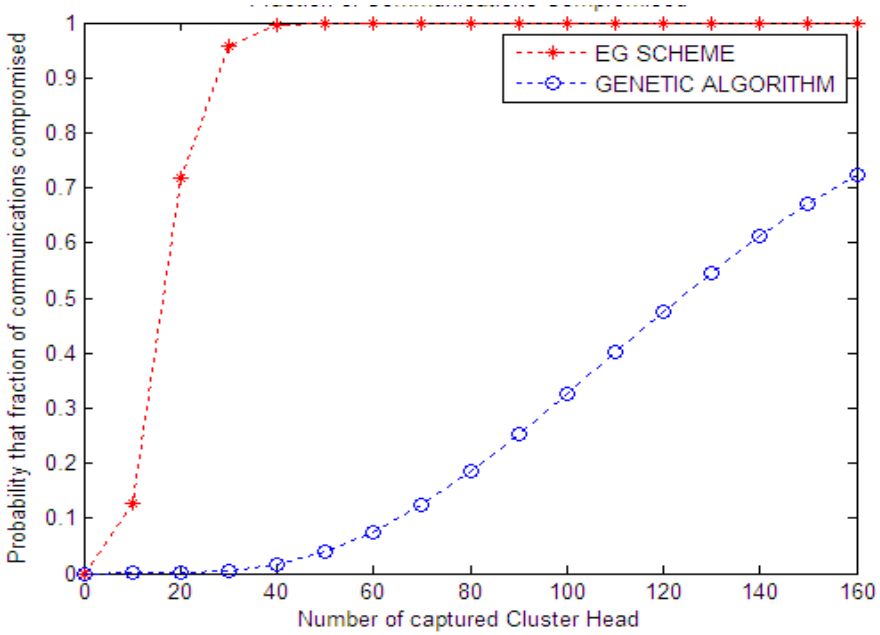

Figure 2. Resilience against Cluster Head Compromised Attack

The probability of adversary compromise the cluster head is less compared to the basic key management scheme.Fig.2. shows the simulation results of resilience against cluster head attack between EG scheme and hybrid protocol. The result shows that, if attacker capture 40 cluster heads the network is totally compromised in EG scheme, but in the proposed method the attacker captured more than 160 cluster heads compromising only 72% of network.

4. Conclusion

The wireless sensor networks consist of different set of levels communication pairs and the types of routing protocol. In this paper, the key sharing between the CH and member nodes are addressed by using asymmetric key predistribution based the symmetric keys are generated using Genetic algorithm. The intra cluster secure communication and key refreshing for hierarchical sensor networks are achieved efficiently in the proposed method. The proposed method reduces the energy consumption, efficient authentication and robust resilience against the cluster head compromise attacks.

References

[1] D. Malan, M. Welsh, and M.D. Smith, "A Public- Key Infrastructure for Key Distribution in Tinyos Based on Elliptic Curve Cryptography", Proceeding of 1st IEEE International Conference Communications and Networks (SECON), Santa Clara, **(2004).**

[2] N. Gura, A. Patel, A. Wander, H. Eberle, and S.C. Shantz, "Comparing Elliptic Curve Cryptography and PSA on 8-bit CPUs", Proceedings of 6th International Workshop on Cryptographic Hardware and Embedded Systems , Boston, Massachusetts, **(2004).**

[3] A.S. Wander, N. Gura, H. Eberle, "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks", Proceedings of the 3rd International Conference on Pervasive Computing and Communications (PERCOM), **(2005)**.

[4] M. Eltoweissy, M. Moharrum, R. Mukkamala, "Dynamic key Management in Sensor Networks", IEEE Transaction on Communications Magazine., vol. 44, no. 4,**(2006)**, pp. 122-130.

[5] C. Lung Wang, T.- P Hong, G. Hoing, W- H Wang, "A GA- Based Key- Management Scheme in Hierarchical Wireless Sensor Networks", International Journal of Innovative Computing, Information and Control., vol. 5, **(2009)**, pp. 4693-4702.

[6] R. Khanna, H. Liu, H- H Chen, "Dynamic Optimization of Secure Mobile Sensor Networks: A Genetic Algorithm", IEEE International Conference on Communications (ICC) **(2007)**, pp. 3413-3418.

[7] R. Basicar, P.C Kishore Raja, C. Joseph, M. Reji, " Node Attribute Behavior based Intrusion Detection in Sensor Networks", International Journal of Engineering and Technology (IJET)., vol. 5,no.5, **(2013)**, pp. 3692- 3698.

[8] E. Sandeep Kumar, S.M. Kusuma, B.P. Vijaya Kumar, "A Random Key Distribution based Artificial Immune System for Security in Wireless Sensor Networks", Proceeding of IEEE International Students' Conference on Electronics, Electrical and Computer Science (SCEECS), MANIT, Bhopal, Madhya Pradesh, **(2014).**

[9] Attea BA, Khalil EA, "A new evolutionary based routing protocol for clustered heterogeneous wireless sensor networks", Application Soft Computer, **(2011)**.