ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Reliable Data Transmission Using Cryptography Mechanism in CWSN

Sunitha B.J, Sheethal Raj T.G

M. Tech, Department of CSE, Sapthagiri College of Engineering, Bangalore, India

Assistant professor, Department of CSE, Sapthagiri College of Engineering, Bangalore, India

ABSTRACT: the main aim of the proposed work is to provide security for the data in wireless network as the data is to be passed through wireless channel. Secure data transmission plays a vital role in wireless sensor network. In this paper we have considered clustered wireless sensor network (CWSN).Clusters are formed using K-means algorithm. Our main goal is to securely transmit the data in CWNS. In order to achieve this we are using SET IBOOS scheme and implements Elliptic Curve Cryptography (ECC) for secure key distribution and data exchange. ECC provides same level of security by using lesser key size than RSA.

KEYWORDS: CWSN, k-means, Elliptic curve Cryptography (ECC).

I. INTRODUCTION

In clustering, the sensor nodes are partitioned into different clusters. Each cluster is managed by a node referred as cluster head (CH) and other nodes are referred as cluster nodes. Cluster nodes do not communicate directly with the sink node. They have to pass the collected data to the cluster head. Cluster head will aggregate the data, received from cluster nodes and transmits it to the base station. Thus minimizes the energy consumption and number of messages communicated to base station. Also number of active nodes in communication is reduced. Ultimate result of clustering the sensor nodes is prolonged network lifetime. Sensor Node: It is the core component of wireless sensor network. It has the capability of sensing, processing, routing, etc.

Online/Offline Signature Schemes: Online/Offline signature schemes divide the process of message signing into two phases, the Offline phase and the Online phase. The Offline phase, which consists of complex computations, is performed before the message to be signed becomes available. Once the message is known, the on line phase starts. This phase retrieves the partial signature calculated during the Offline phase and performs some min or quick computations to obtain the final signature. The Online phase is assumed to be very fast, consisting of small computations. The Offline phase can be performed by a resourceful device. Online/Offline allows a resource constrained sensor node to sign a message quickly.

ID-based Online/Offline Signature (IBOOS): An Online/Offline Signature (OOS) scheme divides the process of message signing into two phases, the Offline phase and the Online phase. The Offline phase is performed before the message to be signed becomes available. This phase performs most of the computations of signature generation and results in a partial signature. Once the message is known, the On line phase starts. This phase retrieves the partial signature calculated during the Offline phase and performs some minor quick computations to obtain the final signature. The Online phase is assumed to be very fast consisting of small computations while the Offline phase can be performed by any other resourceful device.

IBOOS is the ID-based version of OOS, where a message signed with a signer's private key is verified using the signer's ID.An ID-based online/offline signature (IBOOS) scheme consists of five elements as follows:

1. System Setup (SS):
Given a security parameter 1k , outputs a master secret key SK PKG and system parameters SP.
2. Key Extraction (KE): Given a user's identity ID i and a master secret key SK PKG , outputs a corresponding private key D ID
3. Offline Signing (OffSign): Given a signing key D ID i and system parameters SP, outputs an offline signature
4. Online Signing (OnSign): Given a message m and an offline signature S, outputs an online signature σ

5. Signature Verification (Ver): Given a message m ,user's identity ID i , signature σ and system parameters SP, returns 1 if the signature is valid and 0 if not.

II. Related Work

L. B. Jivanadhamet al[1] proposed creation of a Secured Cluster-based architecture for a Dynamic Wireless Sensor Network that applies two topology management procedures: node-move-in and node-move-out. The planned security protocol incorporate one round Zero Knowledge Proof and AES algorithm to relate for node authentication, wherever only authenticated nodes will be acknowledged through node-move-in operation. In addition they explained that, itneeds O(h+q) rounds for a node to connect into a network securely, where h is the height of the dynamic cluster based wireless sensor network and q is the number of adjacent nodes of a joining node. After the O(h+q) attempts to join then network, the node is considered as insecure and is eventually discarded from joining the network .

Yasmin, R et.al [7] have proposed secure and efficient framework for authenticated broadcast/multicast by sensor nodes and for outside user authentication, which uses identity based cryptography and online/offline signature schemes. The most important objectives of this framework are to allow all sensor nodes in the network, initially, to broadcast and/or multicast an authenticated message rapidly; secondly, to confirm the broadcast/multicast message sender and the message contents; and lastly, to confirm the authenticity of an outside user .The projected framework is also evaluated by means of the most secure and efficient identity-based signature.

Huang Lu et.al [8] proposed anew secure routing protocol with ID-based signature scheme for cluster-based WSNs within which the security is dependent on the hardness of the Diffie-Hellman problem in the random oracle model. Here the deficiency in the secure routing protocols with symmetric key pairing is pointed out by authors. Because of the communication operating cost for security, authors provide simulation investigation results in details to demonstrate how various parameters act among energy efficiency and security.

Nguyen Xuan Quy et.al [9] proposed a data aggregation method for cluster-based WSN that improves the security against attackers. This method was based on accelerated homomorphism public key encryption which presents continuous suppression of and supports hop-to-hop verification. The logical investigation and association demonstrate that this approach has both lower computational and better security performance.

III. PROPOSED SYSTEM.

Figure 1 shows the block diagram of proposed system,

a. Network Initialization

Network initialization is to specify various network parameters before actually starting a network. The parameters include the working channel, the network identifier, and network address allocation.

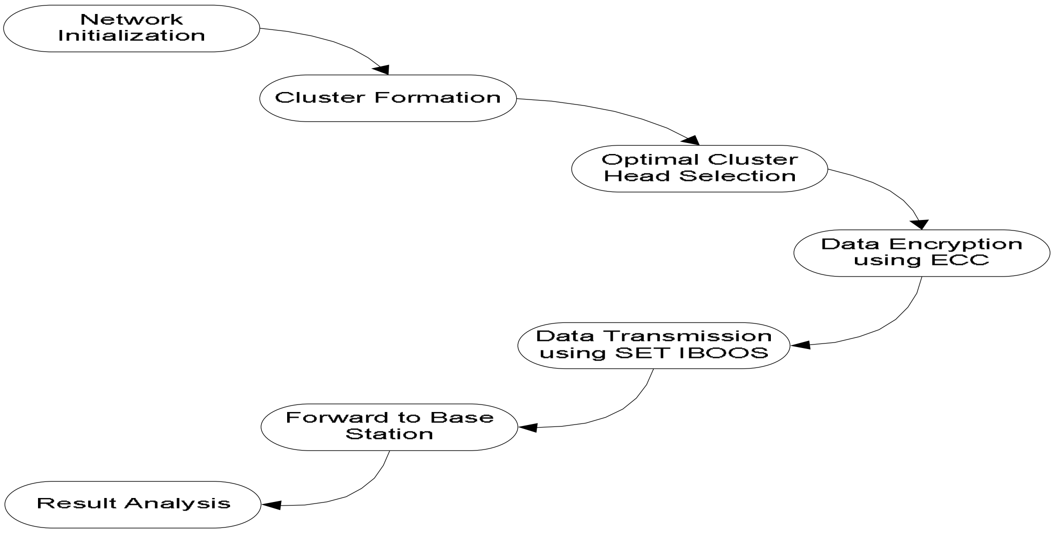
Network Initialization
Cluster Formation
Optimal Cluster Head Selection
Data Encryption using ECC
Data Transmission using SET IBOOS
Forward to Base Station
Result Analysis

Figure 1: Block Diagram of Proposed System

DOI: 10.15680/IJIRCCE.2016. 0404322

1. Cluster formation using K-means Algorithm:

Step 1: Initial clustering

K-mediod algorithm is executed for cluster formation with the target WSN. Assume that the WSN of n nodes is divided into k clusters. First, k out of n nodes is randomly selected as the CHs. Each of the remaining nodes decides its CH nearest to it according to the Euclidean distance.

Step 2: Re clustering

After each of the nodes in the network is assigned to one of k clusters, the centroid of each cluster is calculated. With the new CH in each cluster, Step 2 is recursively executed until the CH is not changed any more.

Step 3: Choosing the CH

After the clusters are formed, an ID number is assigned to each node of a cluster according to the distance from the centroid, assigning smaller number to the closer one the ID number of a node indicates the order to be chosen as the CH.

2. Optimal Cluster head selection:

1. Creation of Clusters
    a. Select random K points as initial Centroid
    b. Repeat
    c. Form K clusters by assigning all points to the closest centroid
    d. Recalculate Centroid for each cluster
    e. Until the Centroid don't change

2. Re -selection of Cluster Head

    a. Input on Base Station: the nodes with ID number
    b. If Energy of cluster head < Energy of threshold
       then
    c. .All nodes ← CheckID()
    d. Current cluster head = ChangeHeader()
    e. All nodes ← InformMsg()
    f. Send data to BS

The residual energy of the CH is checked every round to retain the connectivity of the network. If the energy of the CH is smaller than the preset threshold, the node in the next order
is selected as a new CH. The newly elected CH informs other nodes of the change of the CH.

3. Data Encryption Using ECC

Suppose that we have some elliptic curve E defined over a finite field GF(p) and that E and a point P ∈ E are publicly known, as is the embedding system $m \rightarrow mP_m$; which imbed plain text on an elliptic curve E. Then, when Alice wants to communicate secretly with Bob, they proceed in the following way:

Encryption

- Bob chooses a random integer a, and publishes the point aP (while a remains secret).
- Alice chooses her own random integer l and computes the pair of points
  $P_1(x_1, y_1) = lP$
  $P_2(x_2, y_2) = P_i + l(aP)$
- Read the sequence generated from algorithm Step 4. Calculate S(x1, y1) and S(x2, y2) with S is a corresponding sequence value in step3. Then, the cipher text is as following:

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

C_m=(s(x1, y1) , S(x2, y2))

- Alice converts $C_m$to binary form with: 0 =⇒ 00, 1=⇒ 01 , 2 =⇒ 10 and send to Bob a serie of bits.

4. Data transmission using SET IBOOS

Secure and Efficient data Transmission (SET) protocols for CWSNs is proposed, called SET-IBS and SETIBOOS, by using the IBS scheme and the IBOOS scheme, respectively; Workflow of SET-IBOOS and its Operation SET-IBOOS is proposed in order to further reduce the computational overhead for security using the IBOOS scheme, in which security relies on the hardness of the discrete logarithmic problem. Private Key is generated in similar way as that of IBS, Along with private key online signature is generated for encrypting the data. This online signature is obtained using offline signature. While decrypting the data online signature, sensor node ID and message M parameters are used

The key idea of both SET-IBS and SET-IBOOS is to authenticate the encrypted sensed data, by applying digital signatures to message packets, which are efficient in communication and applying the key management for security. Secret keys and pairing parameters are distributed and preloaded in all sensor nodes by the BS initially, which overcomes the key escrow problem described in ID-based crypto systems. Secure communication in SET-IBS relies on the ID-based cryptography, in which, user public keys are their ID information. Thus, users can obtain the corresponding private keys without auxiliary data transmission, which is efficient in communication and saves energy.

After applying SET-IBOOS, data is forward to base station and results are analyzed

IV. RESULTS

In this section we have computed performance of our proposed parameters using QoS parameters. Figure2 shows the graph plotted to measure energy efficiency vs no. of nodes. Energy is nothing but the total energy consumed over the entire route. Next parameter is throughput which is the accuracy in delivering packets from source to destination. In figure3 shows high throughput of our proposed system.

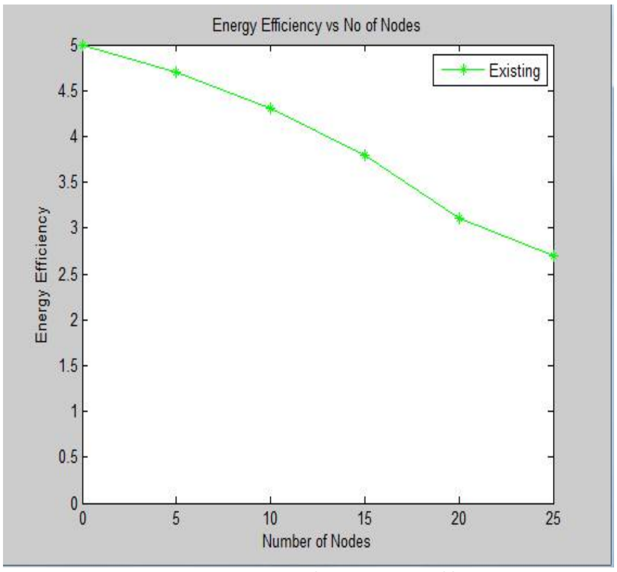

Figure 2: Graph for energy efficiency

DOI: 10.15680/IJIRCCE.2016. 0404322

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

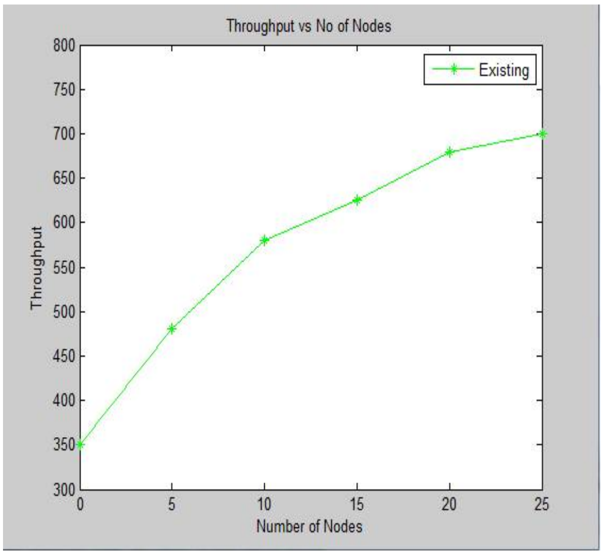

Figure 3: Graph for Throughput.

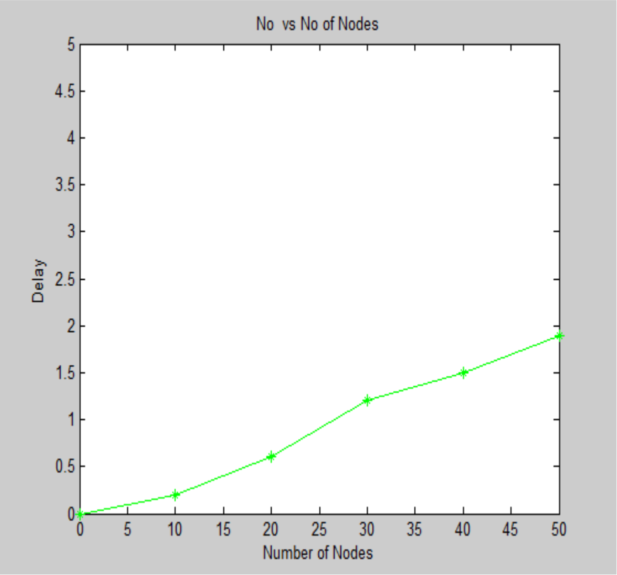

Figure 4: Graph for Delay.

V. CONCLUSION

In this paper we have used the SET-IBOOS which is more suitable for node-to-node communications in CWSNs, since the computation is lighter to be executed. In SET-IBOOS, the offline signature is executed by the CH sensor nodes, thus, sensor nodes do not have to execute the offline algorithm before it wants to sign on a new message. Furthermore, the offline sign phase does not use any sensed data or secret information for signing. This is particularly useful for CWSNs, because leaf sensor nodes do not need auxiliary communication for renewing the offline signature. And proposed system shows more energy effiency, throughput and less delay thus a secure transmission in CWSNs.

DOI: 10.15680/IJIRCCE.2016. 0404322

REFERENCES

[1]. S. Sharma and S.K. Jena, “A survey on secure hierarchical routing protocols in wireless sensor networks,” in Proc. ICCCS, 2011.

[2]. Heinzelman W. B., Chandrakasan A. P., Balakrishnan H., ”An applicationspecific protocol architecture for wireless microsensor networks,” IEEE Trans on Wireless Communications, Vol. 1, No. 4, pp. 660-670, 2002.

[3]. X. H. Wu, S. Wang, ”Performance comparison of LEACH and LEACHC protocols by NS2,” Proceedings of 9th International Symposium on Distributed Computing and Applications to Business, Engineering and Science. Hong Kong, China, pp. 254-258, 2010.

[4]. P.T.V.Bhuvaneswari and V.Vaidehi ”Enhancement techniques incorporated in LEACH-a survey” .Department of Electronics Engineering, Madras Institute Technology, Anna University Chennai, India, 2009

[5]. Wu Xinhua and Huang Li ”Research and Improvement of the LEACH Protocol to Reduce the Marginalization of Cluster Head”Journal of Wuhan University of Technology Vol. 35, No. 1, pp. 79-82, 2011.

[6]. Tao, L, Zhu, QX, Zhang, L. “An Improvement for LEACH Algorithm in Wireless Sensor Network”.Proc.5th IEEE Conf. Indust.Electr., 2010.

[7]. S.K. Singh, M.P. Singh, and D.K. Singh, ”A survey of Energy-Efficient Hierarchical Cluster-based Routing in Wireless Sensor Networks”, International Journal of Advanced Networking and Application (IJANA), Vol. 02, No. 02, pp. 570-580,2014.

[8]. Thiemo Voigt, Hartmut Ritter, Jochen Schiller, Adam Dunkels, and Juan Alonso, ”. Solar-aware Clustering in Wireless Sensor Networks”, In Proceedings of the Ninth IEEE Symposium on Computers and Communications, 2000.