International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016 [ICSSCCET 2016]

ISBN	978-81-929866-6-1	**VOL**	02
Website	icssccet.org	**eMail**	icssccet@asdf.res.in
Received	25 – February – 2016	**Accepted**	10 - March – 2016
Article ID	ICSSCCET068	**eAID**	ICSSCCET.2016.068

An Secure Data Collection in Cluster Wireless Sensor Networks Based on Anchor Point Selection Algorithm

T Yawanikha[1], R Meyanand[2], M Appavu[3], M Dinakar[4], S Karthickagilan[5]

[1]Assistant Professor, Department of Information Technology, Karpagam Institute of Technology, Coimbatore

[2]Assistant Professor, [3,4,5] UG Scholar, Department of Information Technology, Selvam College of Technology, Namakkal

Abstract: *Wireless sensor network is a large number of spatially distributed small autonomous devices which cooperatively monitors and tracks the target data. The aggregate data from multiple sources provides data trustworthy data using iterative filter algorithm. The main challenge is that the each and every node sends data to base station, that energy will be wasted and duplicate data occurs, so thus the network energy will be depleted quickly. This main issue to be avoided by using data aggregation technique called "Redundancy Elimination for Accurate Data Aggregation". In this technique grouping and compression mechanism is applied to remove duplicate data. The accuracy of final aggregate data is obtained without losing the data which is sent to the base station. A Secure Data aggregation scheme based on cryptographic primitives reduces the total length of cipher text. In addition, HE scheme allows authenticating data hop by hop in each cluster. Finally the experimental analysis shows that the scheme and techniques are used to achieve high end confidentiality.*

Index Terms: *Iterative filter, HE scheme, Secure Data Aggregation, Compression Technique*

1 INTRODUCTION

The WSN is an ad-hoc network composed of a multitude oftiny devices with limited computation and energy capacities. Data aggregation is a technique used to conserve battery power in wireless sensor networks (WSN) [1]. When securing such a network, it is important that we minimize the number of computationally expensive security operations without compromising on the security. An encryption algorithm for data confidentiality which will allow us to aggregate encrypted data in a wireless sensor network.An aggregate digital signature algorithm to preserve data integrity which allows us to aggregate digital signatures. An implementation of these algorithms which is efficient in computational and communicational aspects in energy constrained environments.

Sensor nodes come in various shapes and forms, however, they are generally assumed to be resource- limited with respect to computation power, storage, memory and, especially, battery life. At the same time, WSNs are often deployed in public or otherwise untrusted and even hostile environments, which prompts a number of security is- sues. These include the usual topics, e.g., key management, privacy, access control, authentication and DoS-resistance, among others. [2] What exacerbates and distinguishes security issues in WSNs is the need to miniaturize all security services so as to minimize security- induced overhead.

A fully functional identity-based encryption scheme. The performance of our system is comparable to the performance of ElGamal encryption in F*p [7]. The security of our system is based on a natural analogue of the computational Diffie-Hellman assumption. Based on this assumption we show that the new system has chosen cipher text security in the random oracle model. Second, while mounting a chosen cipher text attack on ID we allow the attacker to obtain from the PKG the private key for any public key of her

Cite this article as: T Yawanikha, R Meyanand, M Appavu, M Dinakar, S Karthickagilan. "An Secure Data Collection in Cluster Wireless Sensor Networks Based on Anchor Point Selection Algorithm". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 357-364. Print.

choice, other than the private key for ID. This models an attacker who obtains a number of private keys corresponding to some identities of her choice and then tries to attack some other public key ID of her choice.

A signature scheme whose length is approximately 160 bits and provides a level of security similar to 320-bit DSA signatures. Our signature scheme is secure against existential forgery under a chosen message attack (in the random oracle model) assuming the Computational Diffie-Hellman problem (CDH) is hard on certain elliptic curves over a finite field of characteristic three. Generating a signature is a simple multiplication on the curve [11]. We call such groups Gap Diffie-Hellman groups, or GDH groups for short. Okamoto and Point cheval commented that a Gap Diffie-Hellman group gives rise to a signature scheme. However, most Gap Diffie-Hellman groups are relatively long and do not lead to short signatures. We prove the security of signatures schemes derived from GDH groups and show how they lead to very short signatures.

Many real-world applications involve signatures on many deferent messages generated by many different users. For example, in a Public Key Infrastructure (PKI) of depth n, each user is given a chain of n certificates. The chain contains n signatures by n Certificate Authorities (CAs) on n distinct certificates. Similarly,in the Secure BGP protocol (SBGP) each router receives a list of n signatures attesting to a certain path of length n in the network[9].A router signs its own segment in the path and forwards the resulting list of n + 1 signatures to the next router. As a result, the number of signatures in routing messages is linear in the length of the path. Both applications would benefit from a method for compressing the list of signatures on distinct messages issued by distinct parties.X.509 certificate chains could be shortened by compressing the n signatures in the chain into a single signature. Fig 1.1 shows the cluster WSN architecture to describe the sensor network transferring the data securely using redundancy elimination.

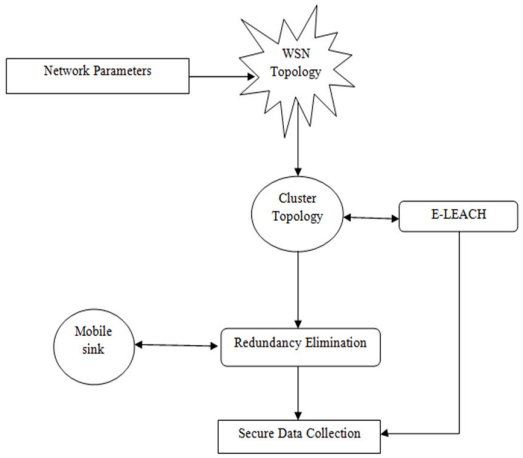

Fig1.1: Cluster WSN Architecture

This signature scheme works in any group where the Decision Diffie- Hellman problem (DDH) is easy, but the Computational Diffie-Hellman problem (CDH) is hard. We refer to such groups as gap groups. Recently there have been a number of constructions using such gap groups. Surprisingly, general gap groups are insufficient for constructing efficient aggregate signatures. Instead, our construction uses a pair of groups G1, GT and a bilinear mape: $G1 \times G1 \rightarrow GT$ where CDH is hard in G1. Joux and Nguyen showed that the map] can be used to solve DDH in G1, and so G1 is a gap group. It is the extra structure provided by the bilinear map that enables us to construct an efficient aggregate signature scheme. These signatures enable user Alice to give Bob a signature on a message M encrypted using a third party's public key and Bob to verify that the encrypted signature is valid. Verifiably encrypted signatures are used in optimistic contract signing protocols to enable fair exchange. Previous constructions require zero knowledge proofs to verify an encrypted signature. The verifiably encrypted signatures are short and can be validated efficiently [5]. We note that the resulting contract signing protocol is not abuse-free in the sense of.

2 Related Works

2.1 Elliptic Curves Algorithm

An elliptic curve can serve as the basis for a GDH signature scheme if we can use it to construct some group G with large prime order on which Computational Diffie-Hellman is difficult, but Decision Diffie-Hellman is easy. First, we characterize a necessary condition for CDH intractability on a subgroup of E [8].Let p be a prime, l a positive exponent, and E an elliptic curve over Fpl with m points.

Cite this article as: T Yawanikha, R Meyanand, M Appavu, M Dinakar, S Karthickagilan. "An Secure Data Collection in Cluster Wireless Sensor Networks Based on Anchor Point Selection Algorithm". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 357-364. Print.

Let P in E be a point of prime order q where q2 - m. We say that the subgroup hPi has a security multiplier α, for some integer α > 0, if the order of pl in F* q is α. In other words: q | plα −1 and q - plk −1 for all k = 1,2,…,α−1 It is well known (as shown below) that for CDH to be hard in the subgroup hPi we must have that the security multiplier, α, for this subgroup is not too small.[6][1]. On the other hand, to get an efficient Decision Diffie-Hellman algorithm in hPi we need that α is not too large. Therefore, the problem in constructing short signatures is to find curves for which α is sufficiently large for security, but sufficiently small for efficiency. Using current security parameters, α= 6 is sufficient for obtaining short signatures. It is an open problem to build elliptic curves with slightly higher α, say α = 10.

Discrete-log on elliptic curves: Let hPi be a subgroup of E/Fpl of order q with security multiplier α. We briefly discuss two standard ways for computing discrete-log in hPi.Use an efficiently computable homomorphism, as in the Menezes- Okamoto-Vanstone reduction, to map the discrete log problem in hPi to a discrete log problem in some extension of Fpl, say Fpli. We require that the image of hPi under this homomorphism is a subgroup of F*pliof order q[12]. Thus we have q|(pil−1), which by the definition of α implies that i ≥ α. Hence, the MOV method can, at best, reduce the discrete log problem in hPi to a discrete log problem in a subgroup of F*plα. Therefore, to ensure that discrete log is hard in hPi we want curves with large α.2. Generic: Generic discrete log algorithms such as the Baby-Step-Giant-Step and Pollard's Rho method have a running time proportional to $\sqrt{q}$. Therefore, we must ensure that q is sufficiently large. Decision Diffie-Hellman on elliptic curves: Let P ∈ E/Fpl be a point of prime order q. Suppose the subgroup hPi has security multiplier α. We assume q - pl−1. A result ofKoblitzshows that E/Fplα contains a point Q that is linearly independent of P. Such a point Q ∈ E/Fplα can be efficiently found [3][7].Note that linear independence of P and Q can be verified via the Weil pairing described below. With two linearly independent points P ∈ E/Fpl and Q ∈ E/Fplα, each oforder q, we can use the Weil pairing to answer certain questions that will allow. To construct a DDH oracle. Let E[q] denotes the subgroup of E/Fplα generated by P and Q. The Weil pairing is a map e : E[q]×E[q] → F*plα with the following properties: 1. Identity: for all R ∈ E[q], e(R,R) = 1. 2. Bilinear: for all R1,R2∈ E[q] and a,b∈ Z we have that e(aR1,bR2) = e(R1,R2)ab. 3. Non-degenerate: if for R ∈ E[q] we have e(R,R0) = 1 for all R0 ∈ E[q], then R = O.4. Computable: for all R1,R2∈ E[q], the pairing e(R1,R2) can be computed efficiently

That e(R1,R2) = 1 if and only if R1 and R2 are linearly dependent. For the linearly independent points P and Q, both of order q, the Weil pairing allows us to determine whether the tuple (P,aP,Q,bQ) is such that a = b mod q; indeed, a = b mod q ⇐⇒ e(P,bQ) = e(aP,Q). Suppose we also have a computable isomorphism φ from hPi to hQi. Necessarily, φ is such that, for all a,

φ(aP) = axQ, where xQ = φ(P). In this case, the Weil pairing allows us to determine whether the tuple (P,aP,bP,cP) is such that ab = c mod q: ab = c mod q⇐⇒e(P,φ(cP)) = e(aP,φ(bP)). With the isomorphism φ, the Weil pairing provides an algorithm for Decision Diffie-Hellman. Note that the algorithm for DDH requires two evaluations of the Weil pairing for points over Fplα.

2.2 Aggregation in WSN

Aggregation techniques are used to reduce the amount of data communicated within a WSN and thus conserves battery power. Periodically, as measurements are recorded by individual sensors, they need to be collected and processed to produce data representative of the entire WSN, such as average and/or variance of the temperature or humidity within an area. One natural approach is for sensors to send their values to certain special nodes, i.e., aggregators. Each aggregator then condenses the data prior to sending it on. In terms of bandwidth and energy consumption, aggregation is beneficial as long as the aggregation process is not too CPU-intensive[2][7]. The aggregators can either be special (more powerful) nodes or regular sensors nodes. In this paper, we assume that all nodes are potential aggregators and that data gets aggregated as they propagate towards the sink. In this setting, since sensors have very limited capabilities, aggregation must be simple and not involve any expensive or complex computations. Ideally, it would require only a few simple arithmetic operations, such as additions or multiplications. We note that aggregation requires all sensors to send their data to the sink within the same sampling period. This either requires the sensors to have (at least loosely) synchronized clocks or the ability to respond to explicit queries issued by the sink. One natural and common way to aggregatedata is to simply add up values as they are forwarded towards the sink [8]. Of course, this type of aggregation is useful when the sink is only interested in certain statistical measurements, e.g., the mean or variance of all measured data, some WSN applications require all sensor data and therefore cannot benefit from aggregation techniques. Similarly, applications requiring boundary values, e.g., min and/or max, are obviously not a good match for additive aggregation.

With additive aggregation, each sensor sums all values, xi, it receives from its k children (in the sink- rooted spanning tree) and forwards the sum to its par- ent. Eventually, the sink obtains the sum of all values sent by all n sensors. By dividing the sum by n, i.e., the total numbers of sensors, it computes the average of all measured data. This simple aggregation is very efficient since each aggregator only performs k arithmetic additions. It is also robust since there is no requirement for all sensors to participate as long as the sink gets the total number of sensors that actually provided a measurement. Additive aggregation can be also used to compute the variance, standard deviation and any other moments on the measured data. For example, in case of variance, each aggregator not only

Cite this article as: T Yawanikha, R Meyanand, M Appavu, M Dinakar, S Karthickagilan. "An Secure Data Collection in Cluster Wireless Sensor Networks Based on Anchor Point Selection Algorithm". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 357-364. Print.

computes the sum, S = Pk i=1 xi, of the individual values sent by its k children, but also the sum of their squares: V = Pk i=1 x2 i . Eventually, the sink obtains two values: the sum of the actual samples which it can use to compute the mean and the sum of the squares whichit can use to compute the variance:

Var = E(x2 −E(x)2; where E(x2) = (Pn i=1 x2 i)/n and E(x) = (Pn i=1 xi)/n[2][1]

2.3 Additively Homomorphic Encryption

Describe the notion of homomorphic encryption and provide an example. We then proceed to present our additively homomorphic encryption scheme along with its security analysis. This encryption technique is very well-suited for privacy-preserving additive aggregation. A varant of ElGamal encryption scheme [11] defined on an elliptic curve , to reduce energy consumption of our SDA scheme. The cipher text encrypted under the public key can be decrypted only by the BS. The CH's perform aggregation of collected sensor data's send them to BS directly. All sensor nodes are stationary after deployed and can be identified.

2.4 Homomorphic Encryption

A homomorphicencryption scheme allows arithmetic operations to be performed on ciphertext. One example is a multiplicatively homomorphic scheme, whereby the multiplication of two ciphertexts followed by a decryption operation yields the same result as, say, the multiplication of the two corresponding plain text values. Homomorphic encryption schemes are especially useful in scenarios where someone who does not have decryption keys needs to perform arithmetic operations on a set of cipher texts. A more formal description of homomorphic encryptions schemes is as follows [13]. Let Enc() denote a probabilistic encryption scheme. Let M be the message space and C the ciphertext space such that M is a group under operation $\oplus$ and C is a group under operation $\otimes$. Enc() is a homomorphic encryption scheme if for any instance Enc() of the encryption scheme, given c1 = Enck1(m1) and c2 =Enck2(m2), there exists a key k such thatc1 $\otimes$ c2 = Enck(m1 $\oplus$ m2)

In other words, the result of the application of function $\oplus$ on plaintext values may be obtained by decrypting the result of $\otimes$ applied to the corresponding encrypted values. A good example is the RSA cryptosystem which is multiplicatively homomorphic. The RSA encryption function is Enc(m) = me = c (mod n) and the corresponding decryption function is Dec(c) = cd = m (mod n) where n is a product of two suitably large primes (p and q), e and d are encryption and decryption exponents, respectively, such that e ∗ d = 1 (mod (p − 1)(q − 1)). Given two RSA ciphertexts c1 and c2, corresponding to respective plaintexts m1 and m2, it is easy to see that c1c2 ≡ me 1me 2 ≡ (m1m2)e (mod n) [1][7]. Hence, one can easily compute the multiplication of the ciphertexts (c1c2) to obtain the ciphertext corresponding to the plaintext m = m1m2 (mod n).

2.5 Proposed Encryption Scheme

A simple additivelyhomomorphic encryption technique. Its security analysis is provided in Appendix A. The main idea of our scheme is to re- place the (Exclusive-OR) operation typically found in stream ciphers with modular addition (+).Additively Homomorphic Encryption Scheme.Encryption: Represent message m as integer m ∈ [0, M − 1] where M is large integer. 2. Let k be a randomly generated keystream, where k ∈ [0, M − 1] 3. Compute c = Enc(m,k,M) = m + k (mod M) Decryption [4][5]: 1. Dec(c,k, M) = c − k (mod M) Addition of Ciphertexts. Let c1 =Enc(m1,k1,M) and c2 = Enc(m2,k2,M) 2. For k = k1 + k2, Dec(c1 + c2,k,M) = m1 + m2.We assume that 0 ≤ m < M. Due to the commutative property of addition, the above scheme is additively homomorphic. In fact, if c1 = Enc(m1,k1,M) and c2 = Enc(m2,k2,M).

Then c1 + c2 = Enc(m1 + m2,k1 + k2,M). Note that if n different ciphers ci are added, then M must be larger than Pn i=1 mi, otherwise correctness is not provided. In fact if Pn i=1 mi is larger than M, decryption will results in a value m0 that is smaller than M. In practice, if p = max(mi) then M should be selected as M = 2dlog2(p∗n)e. The keystream k can be generated by using a stream cipher, such as RC4, keyed with a node's secret key si and a unique message id. This secret key pre-computed and shared between the node and the sink, while the message id can either be included in the query from the sink or derived from the time period in which the node is sending its values assuming some form of synchronization.

2.6 Identity-Based Encryption with Chosen Cipher Text Security

A technique due to Fujisaki-Okamoto to convert the Basic dent scheme of the previous section into a chosen ciphertext secure IBE system (in the sense of Section 2) in the random oracle model. Let E be a probabilistic public key encryption scheme.

The following theorem shows that FullIdent is a chosen ciphertext secure IBE (i.e. IND-ID- CCA), assuming BDH is hard in groups generated by G. Let the hash functions H1,H2,H3,H4 be random oracles. Then FullIdent is a chosen ciphertext secure IBE (IND-ID-CCA) assuming BDH is hard in groups generated by G. Concretely, suppose there is an IND-ID-CCA adversary A that has advantage (k) against the scheme FullIdent and A runs in time at most t(k). Suppose A makes at most qE extraction queries, at most qD

Cite this article as: T Yawanikha, R Meyanand, M Appavu, M Dinakar, S Karthickagilan. "An Secure Data Collection in Cluster Wireless Sensor Networks Based on Anchor Point Selection Algorithm". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 357-364. Print.

decryption queries, and at most qH2,qH3,qH4 queries to the hash functions H2,H3,H4 respectively. Then there is a BDH algorithm B for G with running time t1(k) where: AdvG,B(k) ≥ 2FOadv((k) e(1+qE+qD), qH4, qH3, qD)/qH2 t1(k) ≤ FOtime(t(k),qH4,qH3).

Where the functions FOtimeand FOadv are defined. The proof is based on the following result of Fujisaki and Okamoto [9]. Let BasicPubhy be the result of applying the Fujisaki-Okamoto transformation to BasicPub.(Fujisaki-Okamoto). Suppose A has running time t(k), makes at most qD decryption queries, and makes at most qH3,qH4 queries to the hash functions H3,H4 respectively[2]. Then there is an IND-CPA adversary B against BasicPub with running time t1(k) and advantage 1(k) where,

1(k) ≥ FOadv((k),qH4,qH3,qD) =1 2(qH4 + qH3)[((k) + 1)(1 − 2/q)qD − 1]t1(k) ≤FOtime(t(k), qH4,qH3) = t(k) + O((qH4 + qH3) • n)

Here q is the size of the groups G1,G2 and n is the length of σ. In fact, Fujisaki-Okamoto prove a stronger result: Under the hypothesis, BasicPubhy would not even be a one-way encryptionscheme. For our purposes the result in is sufficient. To prove we also need the following lemma to translate between an IND-ID-CCA chosen ciphertext attack on FullIdent and an IND-CCA chosen ciphertext attack [9]. Let A be an IND-ID-CCA adversary that has advantage (k) against FullIdent. Suppose A makes at most qE> 0 private key extraction queries and at most qD decryption queries. Then there is an IND-CCA adversary B that has advantage at least (k) e(1+qE+qD) against BasicPubhy. Its running time is O(time(A)).

3 Aggregate Signature Security

Aggregate signatures and describe an aggregate signature scheme based on co-GDH signatures. Unlike the co-GDH scheme, aggregate signatures require the existence of a bilinear map. We define security models and provide proofs of security for aggregate signatures [5]. Consider a set U of users. Each user u ∈ U has a signing key pair (PKu,SKu). We wish to aggregate the signatures of some subset U ⊆ U. Each user u ∈ U produces a signature σu on a message Mu of her choice. These signatures are then combined into a single aggregate σ by an aggregating party. The aggregating party, who can be different from and untrusted by the users in U, has access to the users' public keys, to the messages, and to the signatures on them, but not to any private keys. The result of this aggregation is an aggregate signature σ whose length is the same as that of any of the individual signatures. This aggregate has the property that a verifier given σ along with the identities of the parties involved and their respective messages is convinced that each user signed her respective message.

3.1Aggregate Signature Security

Informally, the security of aggregate signature schemes is equivalent to the nonexistence of an adversary capable, within the confines of a certain game, of existentially forging an aggregate signature. Existential forgery here means that the adversary attempts to forge an aggregate signature, on messages of his choice, by some set of users. We formalize this intuition as the aggregate chosen-key security model,We give the adversary power to choose all public keys except the challenge public key. The adversary is also given access to a signing oracle on the challenge key. His advantage thathas defined to be his probability of success in the following game. The following claims give a lower bound for each of these terms. The probability that algorithm C does not abort as a result. .

Signatures on ciphertext received from the member nodes. The security of elliptic curve cryptography methods is based on the discrete logarithm problem (finding a knowing pandis computationally very difficult).An End-To-EndConfidentiality In our scheme, the intermediated nodes, CHs, perform the batch verification with BQS of signatures on ciphertext received from their member nodes, the aggregation of the ciphertexts, and a signature generation on the aggregated ciphertext without decrypting of the ciphertexts. The ciphertexts encrypted under the BS's public key can be decrypted by only the BS with its decryption key x. End-to-end confidentiality of our scheme is reduced to the security of the underlying HE scheme, EC-ElGamalþAlthough elliptic curves can be studied in any finite field, for, cryptographic purposes fields with finite number of elements are used.Fig 3.1 shows the keygeneration architecture to describe how the key to be generated.

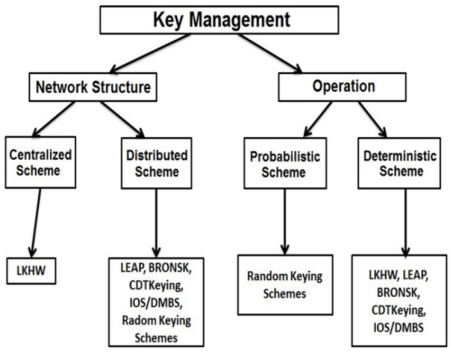

Fig3.1: Networking Management

Cite this article as: T Yawanikha, R Meyanand, M Appavu, M Dinakar, S Karthickagilan. "An Secure Data Collection in Cluster Wireless Sensor Networks Based on Anchor Point Selection Algorithm". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 357-364. Print.

In this model, the adversary is given a single public key. His goal is the existential forgery of an aggregate signature on network.

4 The Proposed Schemes

The energy level of the node depends on some factors such as sleep/wake up schedule and amount of data received and transmitted. For a node to be a cluster head, it has to locate at the centre of a cluster. Once a node is selected to be a cluster head, it broadcasts a message in the network and invites the other nodes to join its cluster. The other nodes will choose their own cluster heads and send join messages according to the power of the many received broadcast messages. When the cluster head receives the join message from its neighbour node, it assigns the node a time slot to transmit data. When the first round is over and the primal cluster topology is formed, the base station is no longer responsible for selecting the cluster head. The task of cluster formation is shifted from the base station to the sensor nodes [3] [7]. The decision to become a new cluster head is made locally within each cluster based on the node's weight value. The proposed modules are followed by

4.1 Network Model
4.2 The Cluster Topology using LEACH Protocol
4.3 Path Planning Algorithm using TSP
4.4 Secure Data Collection Using Elliptic Curve Algorithm.

4.1 Network Model

The sensor nodes are actively involved in detecting events and transmitting the information regarding the events. These activities lead to the death of the node faster than other nodes which are not actively involve d. Under this condition, CHN experiences high energy consumption. To overcome this problem, our proposed mathematical model helps to determine the energy of each node in order to select CHN on the basis of maximum energy ofsensor node in each cluster. Each sensor node determines its residual energy based upon consumed energy so far used in detecting events and transmitting its information.

This residual energy value determines whether the node should be considered as CHN candidate or not. The algorithm depends on calculating the residual energy of the sensor node and its distance from the base station if it is selected as CHN. The Non cluster head node (NCHN) detects CHN in its neighbor on the basis of multiple operations of WSNs using multiple rounds. The advantage of this approach is to provide enough flexibility to each NCHN to choose nearest CHN to reduce the energy consumption. Additionally, the process of choosing the CHN encompasses several steps. The base station broadcasts a short preamble message to each node of the WSN. Each node computes its distance from the base station based on the signal strength.

The node that gets a short preamble message becomes a candidateCHN. Each node waits until it gets an alert from another node of the cluster to compare its radio range and residual energy. If no message is received by another node that is supposed to be candidate node, then this node is elected as CHN. The elected CHN sends a multicasting message to its neighbour nodes in order to let them know about its election as the new CHN.

4.2 The Cluster Topology Using Leach Protocol

Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol. LEACH is representative cluster-based of routing protocols. It is also the first proposed in wireless sensor network and can reduce power consumption on avoiding the communication directly between sink and sensor nodes. In a sensor field, sensor node senses data and sends data to the sink that called round. The working procedure for LEACH will be finished in a round. Before gathering the sensed data at each round, the huge number of sensor nodes will divide into several clusters and choose a cluster head randomly by self organization. Each cluster head is in charge of gather the sensed data from the sensor nodes in the cluster. The cluster head will aggregate the received data, and then send to the sink directly. After sink received all the data from cluster heads, a round will be ending. There are two phases in each round about LEACH, Setup phase and Steady-state phase.

This phase consists of two major steps: cluster formation and cluster head selection. Once the base station forms the primal clusters, they will not change much because all sensor nodes are immobile, whereas the selected cluster head in the same cluster may be different in each round. During the first round, the base station first splits the network into two sub clusters, and proceeds further by splitting the sub clusters into smaller clusters that approach to be specified.

The base station repeats the cluster splitting process until the desired number of clusters is attained. When the splitting algorithm is completed, the base station will select a cluster head for each cluster according to the location information of the nodes. For a node to be a cluster head, it has to locate at the center of a cluster. Once a node is selected to be a cluster head, it broadcasts a message in the network and invites the other nodes to join its cluster. The other nodes will choose their own cluster heads and send join messages

Cite this article as: T Yawanikha, R Meyanand, M Appavu, M Dinakar, S Karthickagilan. "An Secure Data Collection in Cluster Wireless Sensor Networks Based on Anchor Point Selection Algorithm". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 357-364. Print.

according to the power of the many received broadcast messages. When the cluster head receives the join message from its neighbour node, it assigns the node a time slot to transmit data.

4.3 Path Planning Algorithm Using TSP

Travelling Salesman Problem (TSP) used to find a shortest path for visiting all Rendezvous points by a Mobile-Sink node.There are two types of sinks which one can be act as mobile element and other one act asBase Station. A mobile sink that preferentially visits areas of RP will prevent energy holes from forming in a WSN. In clustering purpose only all the sensor nodes send its data's to cluster head and cluster head sends the data's to appropriate rendezvous point and mobile sink node travel along the network and collect the data's from rendezvous point. This process to effectively save the energy of network. During simulation time the events are traced by using the trace files. The performance of the network is evaluated by executing the trace files. The events are recorded into trace files while executing record procedure. In this procedure, the events trace like packet received, Packets lost, Last packet received time etc.

4.4 Secure Data Collection Using Elliptic Curve Algorithm

Elliptic Curve Cryptography (ECC) has emerged as a suitable public-key cryptographic foundation that provides high security for relatively small key sizes (typically few hundred bits). Shorter key lengths ECC uses directly translate to energy savings because of the decreased number of emulated modulo instructions. Elliptic curve cryptography is an approach to public key cryptography based on the algebraic structure of elliptic curves over finite fields GF. An elliptic curve over binary finite field is the set of points (x, y) that satisfy the following equation:

y2 + xy= x3 + ax2 + b a,bxG. Together with the point at infinity.The product of a point and an integer is an operation, but it is very difficult and time consuming to reverse the operation, i.e. to find k knowing only P and Q; finding such an integer k is equivalent to calculating the elliptic curve discrete logarithm of the base P. This operation forms the basis of security in elliptic curve cryptosystems. A base point, G, is fixed for each curve. The random large integer, k, acts as a private key; while the result of multiplying k by the base point, G returns the corresponding public key, perform only aggregations on both ciphertext and signatures, that serves Private Key Generation(PKG).

5 Perfomance and Evaluation

To estimate energy consumption of each node, we assume that the HSN has C clusters with the same size N ¼ 16 or 64 and the ratio r of invalid signatures in a set of signatures is 10 or 30 percent. We investigate the total ECs of member nodes on MICAz and CHs on Tmote Sky in r ¼ 10 or 30 per- cent for N ¼ 16 or 64. Fig 5.1 represents the energy level changes that occur by using BQS scheme with nodes equal to the number of computations performed due to energy consumed..

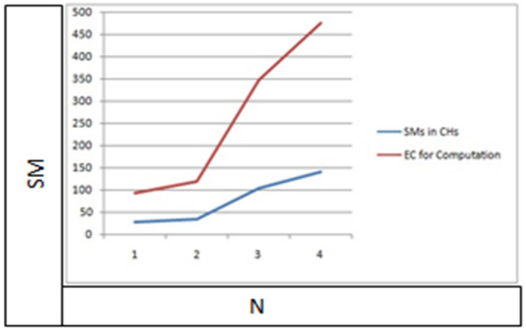

Fig 5.1: N-individual Signature Verification versus BQS

6 Conclusion and Future Work

An each cluster is split into two smaller cluster. Node's weight value allows to locally make a new cluster head. In heterogeneous clustered WSN's,Sen-SDA providesnew homorphic encryption scheme is proposed that allowsintermediate sensors to aggregate the encrypted data of decrypt them. In order to find invalid data scheme Sen-SDA, based on the combination of the HE scheme, EC-ElGamal and the pairing-free IBS scheme, mID-Scheme and the batch verification with BQS. In this signatureheterogeneous clustered Sen-SDA provides end to-end confidentiality and hop-by-hop authentication. We determined the size of a cluster depending the ratio of the number of invalid signatures to minimize the efficiency of CHs' batch verifications.

Cite this article as: T Yawanikha, R Meyanand, M Appavu, M Dinakar, S Karthickagilan. "An Secure Data Collection in Cluster Wireless Sensor Networks Based on Anchor Point Selection Algorithm". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 357-364. Print.

A mobile sink prevent energy holes from forming in a WSN collect data from random position.The events are recorded into trace files while executing record procedure. Further, we can implement by reducing the energy holes in each cluster nodes of a WSN network.

References

1. Kyung-Ah Shim, Cheol-Min Park "A Secure Data Aggregation Scheme Based On Appropriate Cryptographic Primitives in Heterogeneous Wireless Sensor Networks". Volume 26, No 8 , Aug 2015.
2. M. Bellare, J. Garay, and T. Rabin, "Fast batch verification for modular exponentiation and digital signatures," in Proc. Adv. Cryptol.Int .conf . Techn., 2004, pp.268-286.
3. D. Boneh and M. Franklin,"Identity-based encryption from the Weil pairing," SIAM J. Comput., vol. 32, no. 3, pp. 586–615, 2003.
4. D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in Proc. 22nd Int. Conf. Theory Appl. Cryptograph. Techn., 2003, pp. 416–432.
5. D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," in Proc. 7th Int. Conf. Theory Appl. Cryptol. Inf. Secu- rity, 2002, pp. 514–532.
6. C. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient aggregation of encrypted data in wireless sensor network, MobiQuitous '05," pp. 1–9, 2005.
7. R. Chandramouli, S. Bapatla, and K. P. Subbalakshmi, "Battery power-aware encryption," ACM Trans. Inf. Syst. Security, vol. 9, pp. 162–180, 2006.
8. C.-M. Chen, Y.-H. Lin, Y.-C. Lin, and H.-M. Sun, "RCDA: Recov- erable concealed data aggregation for data integrity in wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 4, pp. 727–734, Apr. 2012.
9. Crossbow datasheet on MICAz [Online]. Available: http:// www.openautomation.net/ uploadsproductos/ micaz_ datasheet.pdf, 2009.
10. J.Domingo-Ferrer, "A provably secure additive and multiplica- tive privacy homomorphism," in Proc. 5th Int. Conf. Inf. Security, 2002, pp. 471–483.
11. T. El Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. Inf. Theory, vol. IT-31, no. 4, pp. 469–472, Jul. 1985.
12. J. Girao, D. Westhoff, and M. Schneider, "CDA: Concealed data aggregation for reverse multicast traffic wireless sensor networks," in Proc. IEEE Int. Conf. Commun., 2005, pp. 3044–3049.
13. V. C. Gungor, B. Lu, and G. P. Hancke, "Opportunities and chal- lenges of wireless sensor networks in smart grid," IEEE Trans. Ind. Electron., vol. 57, no. 10, pp. 3557–3564, Oct. 2010.

Cite this article as: T Yawanikha, R Meyanand, M Appavu, M Dinakar, S Karthickagilan. "An Secure Data Collection in Cluster Wireless Sensor Networks Based on Anchor Point Selection Algorithm". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 357-364. Print.