ISSN:0975-9646

Comparative Study between Leach, Leah-E-Genetic Algorithm and Elliptic Curve Cryptography Techniques to Secure Against Sybil Attack In WSN

Omar Badeea Baban[#1]

[#] Department of Computer Engineering
Sinhgad College of Engineering, Pune-41,Pune, India

***Abstract*— Wireless Sensor Networks (WSNs) can be defined as a self-configured and infrastructure-less wireless networks to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, and motion. A Wireless Sensor Network (WSN) contains a large number of sensor nodes. The sensor nodes can communicate among themselves using radio signals. A wireless sensor node is equipped with sensing and computing devices, radio transceivers and power components. The sensor nodes depend upon battery power. Sensor nodes utilize more energy compared to a normal node.**

Typically in WSN, sensor nodes are attached to one or more base stations. As Wireless sensor networks continues to grow, they become vulnerable to attacks and hence they need for effective security mechanisms, The Sybil attack is one of the dangerous attacks against sensor and ad-hoc networks, where a node illegitimately claims multiple identities. Identification of suitable cryptography for wireless sensor networks is an important challenge due to limitation of energy, computation capability and storage resources of the sensor nodes. Symmetric based cryptographic schemes do not scale well when the number of sensor nodes increases. Hence public key based schemes are widely used.

To keep away from various vulnerable attacks, we propose a novel encryption schema based on Elliptic Curve Cryptography (ECC) and homomorphic encryption to secure data transmission in WSN , The proposed encryption schema takes less memory, reduces the computation time, provides great security and flawlessly suitable for low power devices like mobile nodes. The aim of this work is to provide security to the wireless sensor network using elliptical curves cryptography along with genetic algorithm.

Keywords*— *Wireless Sensor Networks, Sybil attacks, Genetic Algorithm, Leach-e, Leach-e-ga, Cluster head, Base Station, Elliptic Curve Cryptography.

I. INTRODUCTION

A wireless Sensor Network (WSN) is a distributed network of small sensor nodes deployed in large numbers to monitor the environment or other systems by the measurement of physical parameters such as temperature, pressure, or relative humidity.

These nodes by monitoring, collect detailed information about the physical environment in which they are installed, and then transmit the collected data to the Base Station (BS). BS is a gateway from sensor networks to the outside world.

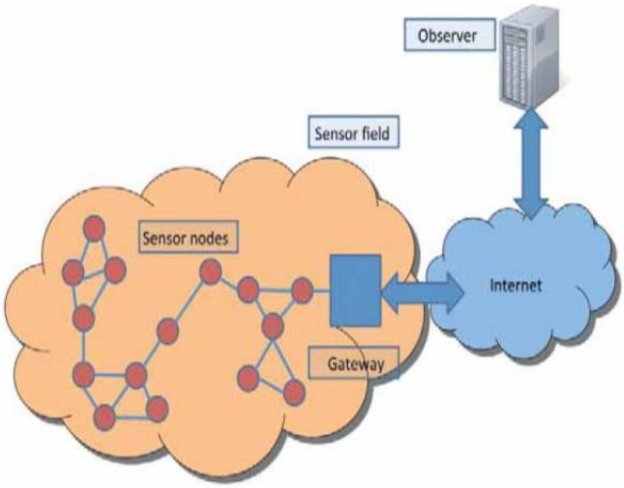


Fig.1 Wireless Sensor Networks [5]

The BS has a very large storage and large data processing capabilities. It passes the data it receives from sensor nodes to the server from where end-user can access them.

Security in WSN is a greater challenge due to the processing limitations of sensor nodes and nature of wireless links. Extensive use of WSNs is giving rise to different types of threats. To defend against the threats proper security schemes are required. Traditionally security is implemented through hardware or software and is generally achieved through cryptographic methods. Limited area, nature of links, limited processing, power and memory of WSNs leads to strict constraints on the selection of cryptographic techniques.

In this paper, we propose a novel encryption schema based on Elliptic Curve Cryptography (ECC) and homomorphic encryption to secure data transmission in WSN. The proposed encryption schema is built upon GASONeC algorithm (Elhoseny et al., 2014) that uses genetic algorithm

to build the optimum network structure in the form of clusters.

ECC is used to exchange public and private keys due to its ability to provide high security with small key size. The proposed encryption key is 176-bit and is produced by combining the ECC key, node identification number, and distance to its cluster head (CH).

Several energy conserving security architectures have been proposed in wireless sensor networks where Key distribution and Key management mechanisms are basic problem of them. RSA, DSA and Elliptic curve cryptography (ECC) are three most widely adopted cryptosystems. ECC is considered as the one which has the highest security quality in per bit key among current public key cryptosystems. compared with the other mechanisms Elliptic Curve Cryptography (ECC) is the best due to its smaller key size. High security despite of smaller key size results in area and power efficient cryptosystems.

The major characteristics of the sensor node used to evaluate the performance of WSN are:

1. Fault tolerance: Each node in the network is prone to unanticipated failure. Fault tolerance is the capability to maintain sensor network functionalities without any break due to sensor node failures.

2. Mobility of nodes: In order to increase the communication efficiency, the nodes can move anywhere within the sensor field based on the type of applications.

3. Dynamic network topology: Connection between sensor nodes follows some standard topology. The WSN should have the capability to work in the dynamic topology.

4. Communication failures: If any node in the WSN fails to exchange data with other nodes, it should be informed without delay to the base station or gateway node.

5. Heterogeneity of nodes: The sensor nodes deployed in the WSN may be of various types and need to work in a cooperative fashion.

6. Scalability: The number of sensor nodes in a sensor network can be in the order of hundreds or even thousands. Hence, WSN designed for sensor networks is supposed to be highly scalable.

7. Independency: The WSN should have the capability to work without any central control point.

8. Programmability: The option for reprogramming or reconfiguring should be available for the WSN to become adaptive for any dynamic changes in the network.

9. Utilization of sensors: The sensors should be utilized in a way that produces the maximum performance with less energy.

10. Impracticality of public key cryptosystems: The limited computation and power resources of sensor nodes often make it undesirable to use public key algorithms.

11. Lack of a prior knowledge of post-deployment configuration:

If a sensor network is deployed via random distribution, the protocols will not be aware of the communication status between each node after deployment.

The following metrics are used to evaluate the performance of a WSN: network coverage, node coverage, efficiency in terms of system lifetime, effortless deployment, data accuracy, system response time, fault tolerance, scalability, network throughput, sample rate, security, the cost of the network and network architecture used. The individual sensor node in the WSN is evaluated using flexibility, robustness, computation, communication, security, synchronization, node size and cost.

In comparison with sensor networks, Ad Hoc networks will have less number of nodes without any infrastructure. The differences between WSN and Ad hoc Networks are presented in the Table 1. [9]

Table 1. Wireless Sensor Networks Vs Ad hoc Networks [9]

Parameters	**Wireless Sensor Networks**	**Ad Hoc Networks**
Number of sensor nodes	Large	Medium
Deployment	Densely deployed	Scattered
Failure rate	Prone to failures	Very rare
Topology	Changes very frequently	Very rare
Communication paradigm	Broadcast communication	Point-to-Point communications
Battery	Not replaceable / Not rechargeable	Replaceable
Identifiers	No unique identifiers	Unique identifiers
Centric	Data centric	Address centric
Fusion / aggregation	Possible	Not suitable
Computational capacities, and memory	Limited	Not limited
Data rate	Low	High
Redundancy	High	Low

II. REVIEW OF LITERATURE

Wireless sensor networks (WSNs) are consist of a large number of sensor devices that can communicate with each other via wireless channels, with limited energy and computing of such environment is a challenging algorithmic and technological task. These WSNs are powerful in that they are amenable to support a lot of very different real-world applications; they are also a challenging research and engineering problem because of this very flexibility. Accordingly, there is no single set of requirements that clearly classifies all WSNs, and there is also not a single technical solution that encompasses the entire design space. Research on sensor networks was originally motivated by

military applications. Early research was done by military using sensor networks for defence dealing with events at contiguous levels. Around 1980 modern research on sensor networks started with the distributed sensor networks program at the US Defence Advanced Research Projects Agency (DARPA). During this period Universities and Institutes did an intensive research in technology components for sensor networks about designing acoustic sensors, protocols to link processes of working on a common application in a network, self-location algorithms, distributed software and developing test beds.

In 1990s there was an important shift of sensor network research due to advances in computing and communications. Small size, low cost sensors are designed to be based upon Micro Electro Mechanical Systems (MEMS) technology, wireless networking and low power processors, which make sensors possible to be deployed in a wireless fashion. This leads and influences the latest research on networking and information processing techniques of sensor networks.

A WSN can be generally described as a network of nodes that cooperatively sense and may control the environment enabling interaction between persons or computers and the surrounding environment. Today, Wireless Sensor Networks are widely used in the commercial and industrial areas such as for e.g. environmental monitoring, habitat monitoring, healthcare, process monitoring and surveillance. For example, in a military area, we can use wireless sensor networks to monitor activity. If an event is triggered, these sensor nodes sense it and send the information to the sink node by communicating with other nodes. The use of WSNs increasing day by day and at the same time it faces the problem of energy constraints in terms of limited battery lifetime. As each node depends on energy for its activities, this has become a major issue in WSNs. The failure of one node can interrupt the entire system or application. Every sensing node can be in active (for receiving and transmission activities), idle and sleep modes. In active mode nodes consume energy when receiving or transmitting data. In idle mode, the nodes consume almost the same amount of energy as in active mode, while in sleep mode, the nodes shutdown the radio to save the energy. [14]

In order to design a completely secure wireless sensor networks, security must be integrated to every node of the system. The reason is that a component implemented without any security could be easily become a point of attack. It indicates that a security must permeate through every aspects of design of wireless sensor networks. Wireless sensor networks (WSNs) are subject to various attacks because of the vulnerable environment, limited recourse, and open communication channel. Wireless networking has witnessed a strong interest in the recent past due to the applications in mobile and personal communications. Wireless network architectures can be categorized into infrastructure wireless network architectures and ad hoc wireless network architectures. Sometimes wireless networks are extended from existing wired network. As per the research studies, Wireless sensor networks are becoming very popular now a day as they offer economically feasible and real-time monitoring solutions. While establishing the Wireless Sensor Network, the sensor nodes can be easily deployed in the unreceptive environments. [11]

Many routing protocols based on clustering method for WSNs have appeared in the literature, In the LEACH and LEACH-E (AlakeshBraman et al. 2014) protocols, the communication between cluster heads and the base station requires more energy than the non-cluster nodes. This means increasing the number of clusters-heads can increase the energy consumption of the whole network and shorten the network lifetime. Therefore, it is necessary to select the optimal number of cluster heads to make the energy consumption minimum. The original LEACH-E algorithm, selects the cluster heads at random with fixed round time for the selection. It considers the remnant power of the sensor nodes in order to balance network loads and changes the round time depending on the optimal cluster size. In LEACHC (Shuo Shi et al. 2012;Petre-CosminHuruial et al. 2010; Raed M. Bani Hani andAbdalraheem A. Ijjeh. 2013) protocol, each node transmits its information to the corresponding base station and the sink node makes the choice of selecting the cluster head and how to divide clusters. Then the cluster head sends this information to BS. In Hierarchy routing protocol a CH collect a data from its cluster members, aggregates all data and forward to the BS that might be located far away from it. If the CH is compromised then it will be dropped. The compromised CH will become ineffective, because the data aggregated by cluster head will never reach the base station.

V-LEACH (BaniYassein. M et al. 2009) protocol, besides having a CH in the cluster, also has a vice-CH that takes the role of the CH when the CH is dropped/compromised. The vice-cluster nodes forward data directly to the BS. Messy GAs solve (Goldberg . D et al.1989) problems of coverage of local maxima by the optimal search. To choose the best CH, minimizing the energy consumption and latency is obtained by choosing the best nodes in the network. A genetic algorithm is executed on a central BS and the results are send to the nodes (Goldberg . D et al.1989).

Hierarchical routing protocol (Vikram Mehta andDr.Neena Gupta. 2012) due to a battery replacement or recharging is not realistic.

Choosing the routing protocol is, it must be energy-efficient to improve the network lifetime (Yang Yu et al 2006; Manimozhi. B , Santhi.B.2013). The optimal set of protocols is proposed to show the optimization in genetic algorithm metrics for WSNs with the QoS requirements (JiaXu,Ning et al. 2012). Cluster-based LEACH routing protocol in WSN has greater energy efficiency and the information such as nodes residual energy and geometric distance send to BS, to elect CH nodes. The CH node is one hop to the BS to consume less energy than other nodes because communication of data consumes the more energy. CH nodes not only consider the residual energy of the nodes and also distance between the CH and BS also examined (Jin Fan and Parish D .J. 2007). Trust-based LEACH protocol in (Nguyen

Duy Tan et al. 2012) discussed the cluster-head-assisted monitoring control.

Basic classification of routing protocols in WSNs (Petre-CosminHuruial et al. 2010) has named LEACH as the most energy efficient protocol giving its advantages and disadvantages. [17]

Choi et al. [4] investigated the feasibility of various cryptographic algorithms, AES, Blowfish, DES, IDEA, MD5, RC4, RC5, SEED, SHA-1 and SHA-256, for their use in WSN utilising MICAz type motes running TinyOS. The usage of resources including memory, computation time and power for each cryptographic algorithm were experimentally analysed. As a result, RC4 and MD5 turned out as the most suitable algorithms for MICAz-type motes.

Gura et al. [12] Implemented ECC on an 8 bit microcontroller by using elliptic curves GF(p) over prime integer field. They selected Elliptic Curves GF(p) over prime integer fields since binary polynomial field arithmetic specifically multiplication is insufficiently supported by current microprocessors and would thus lead to lower performance. The point multiplication of an integer and point on an elliptic curve decomposed into sequence of point additions and point doublings.

Wander et al. [25] quantified the energy cost of authentication and key exchange based on public-key cryptography; RSA and ECC on an 8-bit microcontroller platform; Atmel ATmega128 processor. A comparison has been presented on two public key algorithms, RSA and Elliptic Curve Cryptography (ECC), and considers mutual authentication and key exchange between two un-trusted parties such as two nodes in a wireless sensor network. The ECC-based signature is generated and verified with the Elliptic Curve Digital Signature Algorithm (ECDSA). The results have shown that ECDSA signatures are significantly cheaper than RSA signatures. The experiments were conducted on the Berkeley/Crossbow motes platform, specifically on the Mica2dots. The implementation of RSA and ECC cryptography on Mica2 nodes further proved that a public key-based protocol is viable for WSNs.

Batina et al. [3] proposed a low cost public key cryptography scheme for sensor networks providing service such as key distribution and authentication. They proposed a custom hardware assisted approach to implement Elliptic Curve Cryptography (ECC) in order to obtain stronger cryptography as well as to minimize the power. The low-power ECC processor contains a modular arithmetic logical unit (MALU) for ECC field arithmetic.

Szczechowiak et al. [22] presented results on implementing ECC, as well as the related emerging field of Pairing-Based Cryptography (PBC), on two of the most popular sensor nodes MICA2 and Tmote Sky. They showed that ECC over prime field is not always the best option as pairings over GF (2m) seem to be more efficient on this type of architecture. They argued that fast pairing computation enables Identity Based Encryption and thus opens new ways for achieving security in sensor networks which was also argued by Oliveira et al., 2007.

Yeh et al. [27] proposed ECC-based user authentication protocol that resolves some weaknesses. The proposed protocol provide mutual authentication to protect inside security and outside security. Also, it not only inherits the merits of ECC based mechanism but also enhances the WSN authentication with higher security than other protocols. Therefore, the proposed protocol is more suited to WSNs environments. [10]

III. SYSTEM ARCHITECTURE

Wireless sensor networks are dynamic in nature and data transmitted through various numbers of intermediate nodes.
Due to the mobility and dynamic nature of the sensor nodes, the intermediate nodes may change after route discovery and route-link failure occurs. Also, any intruders can join as the intermediate node in the route. Clustering is an important mechanism in large multihop wireless sensor networks for obtaining scalability, reducing energy consumption and achieving better network performance.
Most of the research in this area has focused on energy-efficient solutions, but has not thoroughly analyzed the network performance, e.g. in terms of data collection rate and time. It is evident that by organizing the sensor nodes in groups i.e., clusters of nodes, we can reap significant network performance gains.
LEACH is the first network protocol that uses hierarchical routing for wireless sensor networks to increase the life time of network.
All the nodes in a network organize themselves into local clusters, with one node acting as the cluster-head. All non-cluster-head nodes transmit their data to the cluster-head, while the cluster-head node receive data from all the cluster members, perform signal processing functions on the data (e.g., data aggregation), and transmit data to the remote base station. Therefore, being a cluster head node is much more energy-intensive than being a non-cluster head node. The biggest challenge for the LEACH-E protocol is that they go through topological changes in the networks and thereby their energy gets drained. To conserve energy and increase network lifetime, the node should minimize the energy dissipation and optimize communication. Changing behaviour of the node is identified by the proposed LEACH-E Genetic Algorithm using its fitness functions and thus makes the node as a trustable node. Once the nodes trustiness is identified, the transmission takes place efficiently in a secured manner.

A- Sybil Attack

Sybil node is the process of creating two or more duplicate nodes with similar identity i.e. same node id as shown in Figure 2.
Particularly, wireless sensor networks are more prone to Sybil attack because of the open and broadcast communication medium and the same frequency is being shared among all nodes. In Sybil attack, attacker makes multiple illegitimate identities in sensor networks either by fabricating or stealing the identities of legitimate nodes. So the base station cannot distinguish the legitimate and the forged node. This confuses the base station and other nodes and the network performance degrades. It is very important to know about the different forms of
Sybil attack, which have targeted the network to get confused or damaged. Sybil attack Taxonomy is three dimensional taxonomy:
1. Direct vs. Indirect Communications
2. Fabricated vs. Stolen Identities.
3. Simultaneity.
In direct method of Sybil attack, legitimate nodes communicates directly with nodes however in case of indirect method, communication in between legitimate node and nodes is done via malicious nodes. Sybil attack may also include fabricated and stolen identities.

In case of fabricated identity, nodes create similar fabricated ID for it on the basis of structure of legitimate nodes ID. nodes may also steal the legitimate nodes ID and can use it as its own ID.
Such attacking nodes will not be identified till stolen ID is destroyed. If the Sybil attack is simultaneous, all identities will participate in network at same time. In non simultaneous Sybil attack, attacker presents a large number of identities over a period of time.

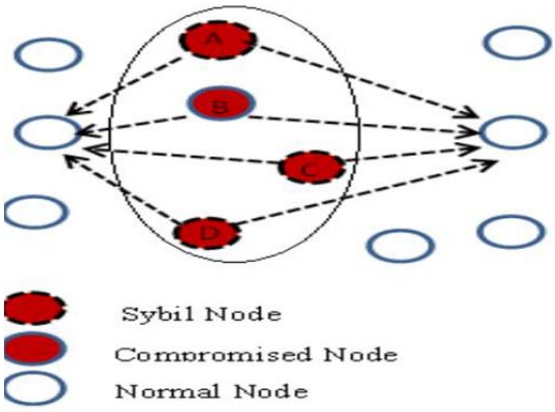


Fig.2 Sybil Attack [16]

Main types of Sybil attacks are Distributed Storage, Routing, Data Aggregation, Voting, Fair Resource Allocation and Misbehaviour Detection. In case of Distributed Storage, there is Sybil attack on replication and fragmentation mechanism.
Sybil attack on routing can also results multipath or disparity routing in, seemingly disjoint paths can go through a single malicious node presenting identities. Data Aggregation Sybil attack affect on some sensor network protocols to aggregate the reading of sensors in order to conserve energy rather than returning individual readings. Fair Resource Allocation Sybil attack can be used in fair resource allocation which will allow a malicious node to obtain unfair share of resources. In Misbehaviour Detection nodes can be used to spread the blame in a misbehaviour detection network.

B. Existing Detection Methods

A. Radio Resource Testing This method is based on the radio capability of each node of the network which already have got assigned a single radio randomly to broadcast and listen. Let's assume that in network any physical device has only one radio and radio is incapable of simultaneously sending or receiving on more than one channel. Now every node is assigned a different channel to broadcast and different channel to listen. If the neighbour with assigned channel is legitimate then:
let s is the total number of nodes and n is number of nodes then:
Prob. of detection = s/n
Prob. Of non-detection = (n-s)/n
For r rounds: Prob. of non-detection = ((n-s)/n)r
In case there are no enough channels for assignment to the nodes then this method can face problem.

B. Registration Registration may be one of the effective solutions to prevent from Sybil attack. There may be one trusted central authority to know the nodes identity. This can help in identifying the legitimate node as it to be checked in known good list. But registration list which contains known identities has to be protected from malicious nodes. If any attacker could add its identity in this list then identity will be treated as known-good.

C. Position Verification In this method it is assumed that the nodes are immobile and will not be changing their position. This is one of the effective method for detecting Sybil attack. If any such attack is created by a malicious node, corresponding position of the node will be changed and will be detected as Sybil attack as network had already recorded nodes initial positions.

D. RSSI Based In this method, localization algorithm is used. By having the position of nodes on signal strength, presence of attack in network can be calculated. Upon receiving a message, the four detector nodes compute the location of sender and associate this location with the sender-ID included in the message. But location calculation is costly.

C. Disadvantages of the Detection Methods

Each of the defenses against the Sybil attack that we have examined has different tradeoffs. Most defenses are not capable of defending against every type of Sybil attack. Additionally, each defense has different costs and relies on different assumptions. The radio resource verification defense may be breakable with custom radio hardware, and validation may be expensive in terms of energy. Position verification can only put a bound on the number of Sybil nodes an attacker can generate unless it is able to very precisely verify node positions. Node registration requires human work in order to securely add nodes to the network, and requires a way to securely maintain and query the current known topology information. [19]

Table 2: Comparative analysis of the techniques to prevent and mitigate the Sybil attack and their disadvantages [18].

Technique to mitigate Sybil attack	Disadvantages / Limitations
Message Authentication and Passing Method	• The message authentication and passing method is applied in order to check the trustworthiness or otherwise for a Sybil node or otherwise for a Sybil node. • If a node does not have any authorization from the network or from the base station, it can't communicate with any other node in the network. • The message authentication and passing method is known for more time consuming as compare to any other method.
TDOA method	• It is an algorithm for Sybil attack detection based on Time difference of Arrival (TDOA) localization method. • This method detects the malicious behavior of head node and member nodes in a cluster based network. • TDOA has achieved a detection rate of 96% along with very low false positive rate of 4%. • It doesn't require any computational overhead to sensor nodes. • Minimize the nodes consumption of energy during an attack.
Random password comparison method	• This method facilitates deployment and control of the positions of the nodes and thereby it prevent the occurrence of Sybil attack in WSN, the RPC method is dynamic as well as accurate in detecting the Sybil attack. • RPC algorithm discovers a valid route in The sensor network by checking each node is a trustable node or a Sybil node so that the data can be transmitted very safely. • The Sybil nodes are detected and data leakage is avoided completely by using RPC.
Neighbourhood RSS based approach	• This lightweight scheme use of neighbourhood RSS to differentiate between the legitimate and Sybil identities. • This scheme has a high level of accuracy with detection process gives us the high true positive rates up to 80% with low false positive rates that ranges to 16%.
SYBILSECURE technique	• Experimental results show that Sybilsecure consumes less energy as compare to the existing defences mechanisms. • Sybilsecure is based on sending and acknowledging the query data packets. • The proposed solution is basically based on sending to and responding from the query sent by the cluster head. The cluster head has a list of its sub nodes parameters, these parameters are identities and their locations. The cluster head broadcasts query packet to all sub- nodes in such a way that it expects a reply from all the sub nodes, so that they must send their id and location.
Two-hop messages approach	• This algorithm is based on broadcasting two-hop messages • In this algorithm by sending two hop messages, each node finds its two hop neighbours and common neighbours between itself and each of its two hop neighbours. The number of common neighbours is one of the good indicator to detect Sybil nodes. • Experimental results by authors show that the proposed algorithm outperforms similar other existing algorithms with respect to true and false detection rates.
PDAP approach	• This algorithm is used in Vehicular adhoc networks (VANETs), In VANETs; most privacy-preserving schemes are vulnerable to Sybil attacks, in which a malicious user can pretend to be multiple vehicles. • In the proposed scheme, malicious node can be detected in a distributed manner. This is done through passive overhearing by set of fixed nodes called road-side boxes (RSBs). The detection of Sybil attacks does not require any vehicle to disclose its identity in the network; hence privacy is preserved for at all times.
TIME-TOTIME MESSAGE model	• Every node in the WSN will maintain the observation table, used for storing node id along with location to detect the Sybil node. • The simulation results by author showed that the detection of Sybil attack is high in sensor network. The communication overhead is also less as compared with other existing algorithms.

Compare and Match Approach	• This approach is used to verify the position to prevent Sybil attacks. • A malicious node can be a Sybil node if and only if it knows the complete information about the other nodes. A Sybil node can have any duplicate ID and duplicate information after obtaining this information. • A node can only communicate with other nodes after authorization by the network or from base station. According to authors, CAM is very effective and efficient as compare to other existing methods.
Threshold Elgamal Key Management Scheme	• To defend against the Sybil attack Proposed scheme validate each node identity to the only identity presented by the corresponding physical node, There are basically two ways to validate an identity. The first type is the direct validation in which a node directly tests another node identity. The second type is indirect one in which already verified nodes allowed to vouch for or refute other nodes. • In the proposed approach Elgamal based key management scheme is used. The Elgamal encryption scheme is an asymmetric key encryption algorithm used for public-key cryptography, which is based on the Diffie– Hellman key exchange. • A Threshold ElGamal-based key management scheme is used in this paper for protection against Sybil attack.
Optimized secure routing protocol	• The mechanism used in the paper is set up to detect Sybil attack based on the distance and hop count between the nodes. • The prevention is done based on Encryption technique which uses unique identities of the nodes. • The authors also calculate performance parameters energy consumption. The results shows the efficiency of the proposed protocol. • The proposed work help in preventing the wireless sensor network from the security risk due to Sybil attack. The encryption technique used in the paper is based on the binomial distribution.
Energy and Hop based Detection	• The detection of malicious node is done in three phases, where in the first phase of method the node energies are compared with the threshold value. In the second phase the distance between suspected Sybil nodes is calculated and finally, the route followed by the packets are checked for confirmation of a Sybil node. • It is observed from the results that, the proposed scheme increase the Packet delivery ratio along with throughput of the network.
Channel-Based Detection	• An enhanced physical-layer authentication scheme to detect Sybil attacks is proposed in. • This exploits the spatial variability of radio channels in the environments with rich scattering. Authors build a hypothesis test in order to detect Sybil clients for both narrowband and wideband wireless systems, Based on existing channel estimations mechanisms, proposed method can be easily implemented with low overhead. This can be done either independently or combined with other physical-layer security methods. • The performance of proposed Sybil detector in the paper is verified, via both a propagation modelling software. A field measurement using a vector network analyzer is also used for typical indoor environments. Authors claim that their evaluation examines numerous combinations of system parameters such as bandwidth, number of channel estimates, signal power, number of total clients, number of Sybil clients, and number of the access points. According to authors, both the false alarm rate and the miss rate of Sybil attacks are below 0.01, pilot power of 10 mW, with three tones, and a system bandwidth of 20 MHz.
UWB ranging based information	• This scheme proposes development of a defences scheme against direct, simultaneous Sybil attacks with derivation of a rigorous analytic framework for the determination of the system performance. • This scheme focuses on a rule-based anomaly detection system. This system is called RADS, which monitors and timely detects Sybil attacks in large-scale WSNs. The proposed expert system relies on an ultra-wideband (UWB) ranging-based detection algorithm. This algorithm usually operates in a distributed manner that require no information sharing or cooperation between the sensor nodes in order for performing the anomaly detection tasks.

D. System Overview

1. Leach-E Protocol

LEACH-E protocol improves the CH selection procedure. Sensor node's residual energy is the main concern, which decides whether the node become a CH or not after the first round (BaniYassein .M et al2009). Like LEACH protocol, LEACH-E is divided into rounds (Shankar .M et al. 2012). In the first round, all the nodes have the same probability of being a CH. At the end of the first round, the node, which has more residual energy, is elected as CH. LEACH–E protocol improves the cluster head selection procedure.

2. Leach-E-GA (Leach-Energy-Genetic Algorithm)

This work uses the LEACH—E-Genetic algorithm (GA) that would enhance the WSN response time, network life and minimize the delay. The Genetic algorithm proposed by (Goldberg et al in 1975; Wu Xinhua and Wang Sheng. 2010) improves the cluster heads selection process. Selecting the minimum number of cluster heads in the WSN is determined based on the square root of the total number of sensor nodes, to minimize the total energy consumption. The LEACH-E Genetic algorithm is shown in figure 3 selects an unsupervised node, which allows the network to achieve maximum coverage distance with minimum energy consumption.

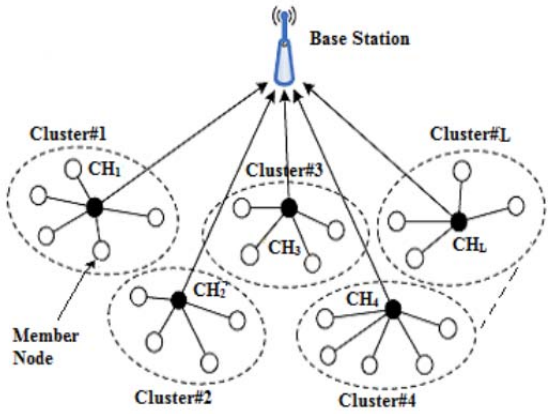


Fig. 3 GA Hierarchical Clustering [21]

Genetic algorithm optimizes the behaviour of the node based on its request and response, energy level, mobility and comparison with its record of previous transmissions. A node, whose behaviour is changed and not fit to the fitness function, is considered to be the Sybil node. The node is dropped from the network to improve the quality of the network for future communication. (Wu Xinhua Wang Sheng. 2010) enhanced the HCR protocol using GA, which determines the clusters, CHs, Cluster-members and the schedules for transmission. In Leach-E-GA protocol the GA can be used at any place in the network like base station CH, or in administration and it provides more energy efficiency by identifying the Sybil nodes to the optimizer. In each round of routing discovery, GA is applied. The optimizer chooses the best trusted neighbour nodes using the GA fitness function. The fitness function is based on the node behaviour, direct distance to destination node, and energy and trust value of the nodes in the route. LEACH-E is enhanced by GA at the base station. GA creates the energy efficient clusters for more numbers of transmissions. In terms of GA representation, nodes are called [assigned] as chromosomes.

Genetic Algorithm ( )

- Initialize population and Objective Function Value- [OFV].
- Define the Fitness function.
- Selection.
- Cross over.
- Mutation.
- Repeat the above steps until reaching the solution.

A population contains a group of individuals named chromosomes, which represents a finished solution for a derived problem. Each chromosome is a sequence of values of the attribute [node-energy, node-trust value, and node-distance]. [17]

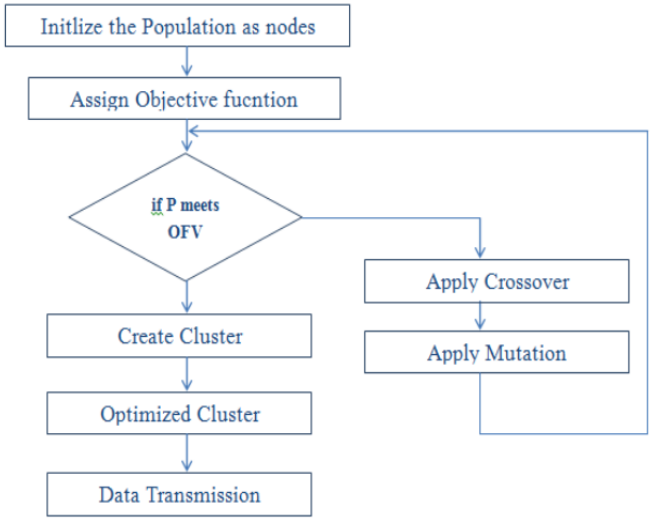


Fig. 4 GA Flowchart used for WSN [17]

Once an initial population is randomly generated, the algorithm evolves through three operators:
A. Selection: This equates to survival of the fittest.
B. Crossover: This represents mating between individuals.
C. Mutation: This introduces random modifications.

A. Selection Operator

- Give preference to better individuals, allowing them to pass on their genes to the next generation.
- The goodness of each individual depends on its fitness.
- Fitness may be determined by an objective function or by a subjective judgment.

B. Crossover Operator

Crossover is a significant operator of the GA. The primary aim of Crossover is to reorganize the information of two different individuals and create a new one. It is a structured, yet randomized method of exchanging formation between strings. It encourages the exploration of new fields in search space. Cross swapping operator is used on the chosen individuals. Here, two different cross sites of parent chromosomes are selected randomly. The cross over operation is finished by exchanging the middle substring between strings.

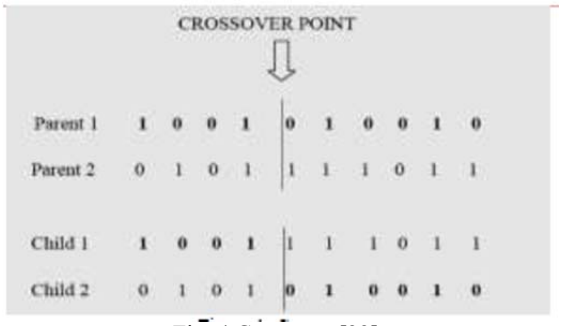


Fig. 4 Crossover [22]

C. Mutation Operator

Mutation consists of securing the procedure of reproduction and Crossover efficiently without much loss of the potentially helpful genetic material. Mutation is by itself a random walk through the string space and offers for occasional interference in the crossover operation by introducing one or more genetic elements during reproduction. This operation assures diversity in the genetic strings over large period of time and prevents stagnation in the emergence of optimal individuals. Bit wise mutation changes 1 to 0 and vice versa. The above specified operations of selection, crossover and mutation are repeated until the best individual is detected.

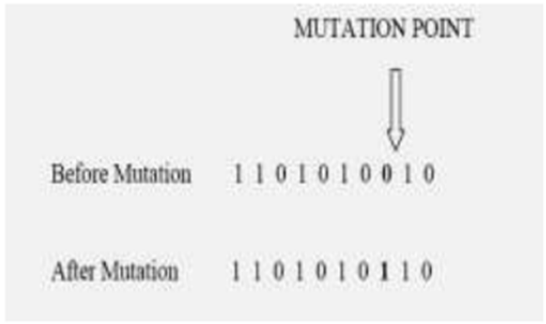


Fig.5 Mutation [22]

3. ECC Cryptography

Elliptic Curve Cryptography was first projected by victor Miller and independently by Neal Koblitz in the mid-1980s and has evolved into a mature public-key cryptosystem. Compared to its traditional counterparts, ECC offers the equal level of security using much smaller keys. This result in faster computations and reserves in memory, power and bandwidth those are especially important in constrained environments. More significantly, the advantage of ECC over its competitor's increases, as the security needs increase in excess of time. ECC operates over a group of points on an elliptic curve defined over a finite field.

Algorithm:

1. At first we will take a curve in the form y2 = x3+ax+b
Where, a and b are curve parameters.
2. Choose a prime number.
3. Using point adding and point doubling we compute the points on the curve.
4. Select a generating point out of those points whose order should be large.
5. Take a random number less than order of generating point as a private number for each entity. This will be a secret key.
6. Generate its public key by multiplying the generating number with the secret number and will publish the point.

Encryption: The first task in this system is to encode the plaintext message m to be sent as an x-y point Pm. It will be the point Pm that will be encrypted as a cipher text and subsequently decrypted. As with the key exchange system, an encryption and decryption system requires a point G and an elliptic group Ep (a, b) as parameters.
1. Each user A selects a private key nA and generates a public key PA= nAXG.
2. To encrypt and send a message Pm to B, A chooses a random positive integer x and produces the cipher text Cm consisting to the pair of points.
3. Cm= xG,Pm+xPB (A uses Bs public key PB to encrypt the message.)

Decryption: To decrypt the cipher text, B multiplies the first point in the pair by B's secret key and subtracts the result from the second point:
Pm+xPB - nB(xG)
Pm+xBG - nB(*xG)
Pm, which is the original message or plaintext. [11]

PROPOSED WORK FLOW

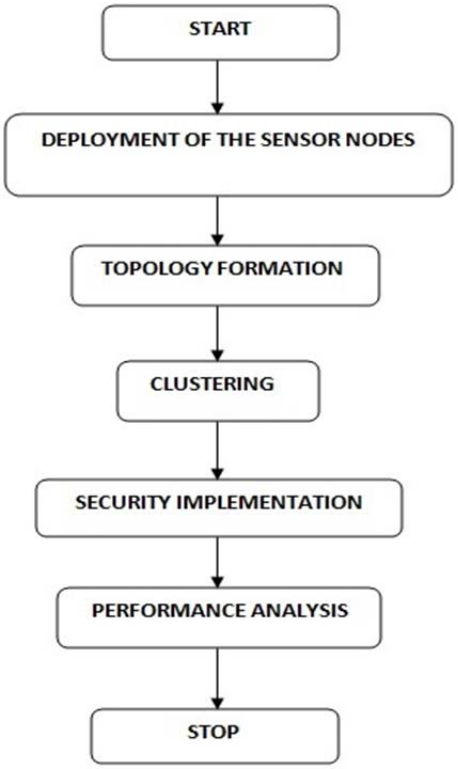


Fig. 6 Work flow [11]

The proposed methodology has implemented to provide the security in the wireless sensor network using Genetic Algorithm first and then elliptical curves cryptography. We have implemented the project using NS2 platform. Network Simulator-2, NS2 Network simulator is the part of software that predicts the performance of the network without a real network being there. It is a vital simulation tool for networks which contains, Lists of events and executes one event after another; Single thread of control so no blocking or race conditions, Otcl adds object orientation to TCL, Transport layer protocols like TCP and UDP as a Traffic Agent.
As we know for the simulation it offers various benefits like:
• Provides a graphic interface.
• Compatible with many platforms.

The project has gone through the following phases:

1. Deployment of the Sensor Nodes: In this, we have created the wireless sensor nodes which are randomly generated.

2. Topology Formation: These nodes are scattered randomly and have formed the structure, we can call it as topology.

3. Clustering: After deployment of random nodes, we have created clusters of the nodes.

We use LEACH-E Genetic algorithm (GA) for our network architecture to provide the security to the network as it is used to identify the node best trusted neighbours for communication using its optimization capability which would enhance the WSN response time, network life and minimize the delay. The Genetic algorithm improves the cluster heads selection process. Selecting the minimum number of cluster heads in the WSN is determined based on the square root of the total number of sensor nodes, to minimize the total energy consumption.

4. Security Implementation: For security implementation in the network, we have used elliptical curve cryptography to encrypt the messages sent from the sender to the receiver side. After deployment and clustering of the wireless sensor network, we have implemented the security among the each node to be communicated. Each sensor node will have routing table. Each sensor node is having their id and some relevant information like their public key which has been used in the process of encrypting the data or message to be transmitted.

The private keys are randomly generated which are used to decrypt the message at the receiver side.

Consider the standard elliptic curve equation as,

$$y2 = x3 + ax + b \qquad \text{(E.q. 1)}$$

Ex:

E = y^2 = x^3 + 4x + 20, defined over F29 with the constants where, a = 4 and b = 20 which have been checked to satisfy that E is an elliptic curve.

The 37 randomly generated points in E (F29) are as following:

{O, (0, 7), (0, 22), (1, 5), (1, 24), (2, 6), (2, 23), (3, 1), (3, 28), (4, 10), (4, 19), (5, 7), (5, 22), (6, 12), (6, 17), (8, 10), (8, 19), (10, 4), (10,25), (13, 6), (13, 23), (14, 6), (14, 23), (15, 2), (15, 27), (16, 2), (16, 27), (17, 10), (17, 19), (19, 13), (19, 16), (20, 3), (20, 26), (24, 7), (24, 22), (27, 2), (27, 27)}.

These points can be represented on the elliptical curve are as follows:

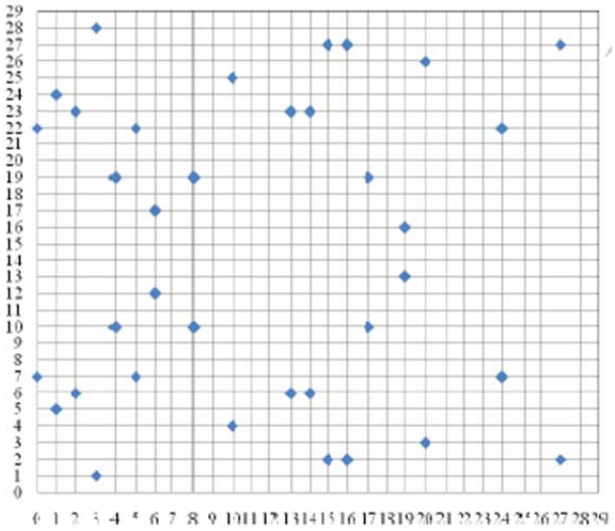


Fig. 7 Elliptic Curve Point Representation [11]

Consider the points,

1).The point (x=1, y=5) in E (F29) satisfies the equation elliptic curve as:

y2 mod p = x3 + 4x + 20 mod p

25 mod 29 = 1 + 4 + 20 mod 29

25 = 25 this satisfies the equation of EC.

2) The point (x=3, y=1) in E (F29) satisfies the equation elliptic curve as:

y2 mod p = x3 + 4x + 20 mod p

1 mod 29 = 27 + 12+ 20 mod 29

1 = 1 this satisfies the equation of EC.

3) The point (x=15, y=2) in E (F29) satisfies the equation elliptic curve as:

y2 mod p = x3 + 4x + 20 mod p

4 mod 29 = 3375 + 60+ 20 mod 29

4=4, this satisfies the equation of EC. [11]

i. Numerical Illustration

Population of Nodes

All nodes in the network are considered as chromosomes. The CH and CM nodes are represented as X and Y respectively. The fitness of a chromosome is evaluated by many parameters, such as node energy, distance, node trust value. Population P consists of several chromosomes. For example, the population P is initialized as P =50 and it is generated randomly. According to the fitness the population transforms into the future generation.

Fitness Parameters

$$DD = \sum_{i=1}^{N} dist_{i,BS}$$

$$C = \sum_{i=1}^{K} dist_{i,CH} + dist_{CH,BS}$$

$$\mu = \frac{\sum_{i=1}^{HS} dist_{cluster-i}}{CH}$$

$$SD = \sqrt{\sum_{i=1}^{CH} (\mu - dist_{cluster-i})^2}$$

$$TV = \sum_{i=1}^{N} TV(Node_i) \geq TV_{th}$$

$$Enry = \sum_{j=1}^{K} Enry_{Tx_{j,CH}} + K \times Enry_{Rx} + Enry_{Tx_{CH}}$$

Fitness Function

$$OBF = \sum_{i=1} (w_i \times f_i), \forall f_i \in \{C, DD, Enry, SD, TV\} \quad \text{..... (E.q. 1)}$$

Where all the attributes are used as notation in the above objective constrains to represent the fitness function and it is described in the following table-3. If the node satisfied in terms of OBF, then there will be a link provides between X, Y, where X represents the node and the Y represents the cluster. Each chromosome is evaluated according to the fitting parameters and update in each round, and it can be written as:

$\Delta fi = fi - (fi\text{-}1)$ .....(E.q 2)

δf denotes the changes in the fitness parameter values.

$wi = (wi\ -1) + ci\Delta fi$ .....(E.q 3)

Where, (ci = 1/1+exp – fi) Improves the weight value compared with the previous value.

Each time the nodes attribute are evaluated by the fitness function and check the arbitrary weight value. If the arbitrary weight value is the best OFV, then that chromosome is chosen as the best neighbour for transmitting data and grouped into clusters. If the node parameter has not satisfied the fitness constraints, then apply cross over on the chromosomes. Then apply mutations and compute the OFV. Repeat the same above fitness calculation until reaching the objective value.
Else, replace all the bad solution based chromosomes with the newly generated chromosomes randomly for the optimization process. Also, in this project, it is considered to minimize latency, which means minimizing travel time of data from the end nodes to BS (Goldberget al.,1989).When each CH node sends data directly using one hop to the BS, the time is reduced, but the node consumes more energy.
Minimizing energy consumption involves finding solutions where nodes communicate information on distances as short as possible and between as few nodes as possible. The results where cluster heads are equally spread, it is found that the energy consumption is uniformly distributed in the network. [17]

Table 3. Nomenclature [17]

Notation	Description
i	Index and ID of the node, cluster
K	Data size
DD	Distance
C	Cluster
$Enry$	Energy
SD	Cluster Distance with Dieviationμ
TV	Trust Value
$dist_{i,BS}$	Distance between Node i and BS
$dist_{i,CH}$	Distance between Node i and CH
$dist_{CH,BS}$	Distance between CH and BS
BS	Base station
CH	Cluster Head
$cluster - i$	I^{th} Cluster
$Enry_{Tx_{j,CH}}$	Energy Need for Transmitting from j^{th} node to CH
$Enry_{Rx}$	Energy Need for Receiving
$Enry_{Tx_{CH}}$	Energy Need for Transmitting to BS
w_i	Arbitrary Weight
f_i	Fitness parameter

ii. Mathematical Model

A mathematical model is an abstract model that uses mathematical language to describe the behaviour of the system. Set theory and mathematical model for A Mechanism of Preventing Sybil Attack in WSN by Using Elliptic Curve Cryptography with Genetic Algorithm is described.

1. Let, S be the system defined as-
S = {I, O, F}
2. I is main set of inputs of the system.
I = {S, BS, A}
3. S is main set of Normal Nodes like s1, s2, s3....
S = {s1, s2, s3, ……..., sn}
4. A is main set of Cluster Head nodes like a1, a2, a3....
A = {a1, a2, a3,…… ……., an}
5. O is main set of Accused Nodes or Attack Nodes like c1, c2, c3....
O = {c1, c2, c3, ……..., cn}
6. Let F be the set of processing function.
F = {Ffit, Fecc}
7. Ffit is Fitness function defined as:
Ffit = {C, DD, Entry, SD, TV}
8. Let C be the set of cluster.

$$C = \sum_{i=1}^{K} dist_{i,CH} + dist_{CH,BS}$$

9. Let DD be the set of distance.

$$DD = \sum_{i=1}^{N} dist_{i,BS}$$

10. Let Entry be the set of Energy.

$$Enry = \sum_{j=1}^{K} Enry_{Tx_{j,CH}} + K \times Enry_{Rx} + Enry_{Tx_{CH}}$$

11. Let SD be the set of cluster distance with deviation.

$$SD = \sqrt{\sum_{i=1}^{CH} (\mu - dist_{cluster-i})^2}$$

12. Let TV be the set of trust values of nodes.

$$TV = \sum_{i=1}^{N} TV(Node_i) \geq TV_{th}$$

13. Fecc is elliptic curve cryptography function defined as:

Fecc encrypt = $Cm = \{ xG, Pm + xPB \}$

Where, Cm is cipher text message.
Pm is plain text or original message.
x is random integer selected by the sender of the message, A sender.
G is a point of a,b.
PB is B's public key.

Fecc decrypt = Pm + xPB – nB(xG)
Pm + xBG – nB(xG)

nB is B's private key.

14. Fs is the successful case defined as-
Fs= Malicious nodes are detected and place them out of the network. In short, network contains no malicious node. Normal nodes are differentiated from malicious nodes using fitness function and elliptic curve cryptography.

15. Fi is the failure case defined as-
Fi = Network consist of malicious node.

Figure 8 shows Venn diagram for Sybil attack prevention system in WSN by using Elliptic Curve Cryptography with Genetic Algorithm.

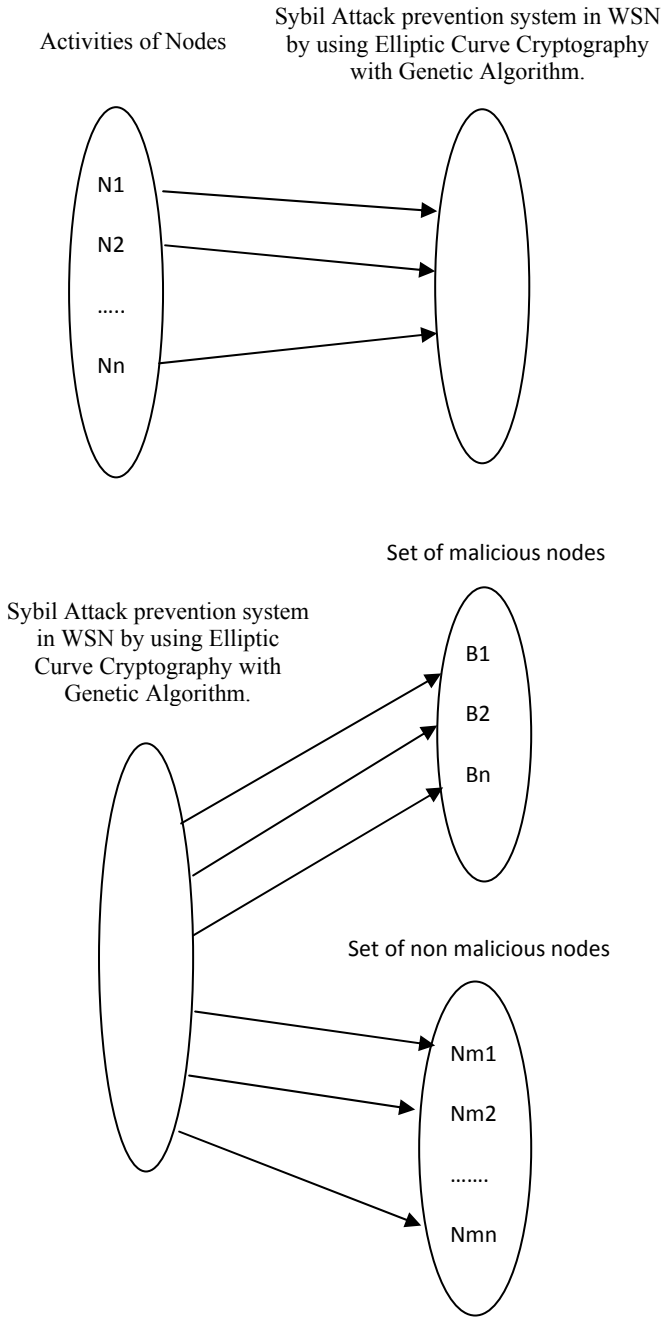


Fig. 8 Venn diagram

Algorithms

Cluster Formation Algorithm in NS2:

```
#Filename: sample18.tcl
#****************SENSOR NETWORK ************
#******************ENERGY MODEL **********88
#************Multiple node Creation and communication model using
UDP (User Datagram Protocol)and CBR (Constant Bit Rate)
*****************************88

# Simulator Instance Creation
set ns [new Simulator]
#Fixing the co-ordinate of simulation area
set val(x) 600
set val(y) 600
# Define options
set val(chan) Channel/WirelessChannel ;# channel type
set val(prop) Propagation/TwoRayGround ;# radio-propagation model

set val(netif1) Phy/WirelessPhy ;# network interface type
set val(netif2) Phy/WirelessPhy ;# network interface type
set val(mac) Mac/802_11 ;# MAC type
set val(ifq) Queue/DropTail/PriQueue ;# interface queue type
set val(ll) LL ;# link layer type
set val(ant) Antenna/OmniAntenna ;# antenna model
set val(ifqlen) 50 ;# max packet in ifq
set val(nn) 10 ;# number of mobilenodes
set val(rp) AODV ;# routing protocol
set val(x) 600 ;# X dimension of topography
set val(y) 600 ;# Y dimension of topography
set val(stop) 10.0 ;# time of simulation end
set val(energymodel) EnergyModel ;#Energy set up

# set up topography object
set topo [new Topography]
$topo load_flatgrid $val(x) $val(y)
# general operational descriptor- storing the hop details in the network
create-god $val(nn)
#Transmission range setup
#********************************* UNITY GAIN, 1.5m HEIGHT OMNI DIRECTIONAL ANTENNA SET UP **************
Antenna/OmniAntenna set X_ 0
Antenna/OmniAntenna set Y_ 0
Antenna/OmniAntenna set Z_ 1.5
Antenna/OmniAntenna set Gt_ 1.0
Antenna/OmniAntenna set Gr_ 1.0
#********************************* SET UP COMMUNICATION AND SENSING RANGE **********************************

#default communication range 250m
# Initialize the SharedMedia interface with parameters to make
# it work like the 914MHz Lucent WaveLAN DSSS radio interface
$val(netif1) set CPThresh_ 10.0
$val(netif1) set CSThresh_ 2.28289e-11 ;#sensing range of 500m
$val(netif1) set RXThresh_ 2.28289e-11 ;#communication range of 500m
$val(netif1) set Rb_ 2*1e6
$val(netif1) set Pt_ 0.2818
$val(netif1) set freq_ 914e+6
$val(netif1) set L_ 1.0
```

```
# Initialize the SharedMedia interface with parameters to make
# it work like the 914MHz Lucent WaveLAN DSSS radio
interface
$val(netif2) set CPThresh_ 10.0
$val(netif2) set CSThresh_ 8.91754e-10 ;#sensing range of
200m
$val(netif2) set RXThresh_ 8.91754e-10 ;#communication
range of 200m
$val(netif2) set Rb_ 2*1e6
$val(netif2) set Pt_ 0.2818
$val(netif2) set freq_ 914e+6
$val(netif2) set L_ 1.0
# configure the first 5 nodes with transmission range of 500m
$ns node-config -adhocRouting $val(rp) \
-llType $val(ll) \
-macType $val(mac) \
-ifqType $val(ifq) \
-ifqLen $val(ifqlen) \
-antType $val(ant) \
-propType $val(prop) \
-phyType $val(netif1) \
-channelType $val(chan) \
-topoInstance $topo \
-energyModel $val(energymodel) \
-initialEnergy 10 \
-rxPower 0.5 \
-txPower 1.0 \
-idlePower 0.0 \
-sensePower 0.3 \
-agentTrace ON \
-routerTrace ON \
-macTrace OFF \
-movementTrace ON

# Node Creation
set energy(0) 1000
$ns node-config -initialEnergy 1000 \
-rxPower 0.5 \
-txPower 1.0 \
-idlePower 0.0 \
-sensePower 0.3
set node_(0) [$ns node]
$node_(0) color black
# configure the remaining 5 nodes with transmission range of
200m
$ns node-config -adhocRouting $val(rp) \
-llType $val(ll) \
-macType $val(mac) \
-ifqType $val(ifq) \
-ifqLen $val(ifqlen) \
-antType $val(ant) \
-propType $val(prop) \
-phyType $val(netif2) \
-channelType $val(chan) \
-topoInstance $topo \
-energyModel $val(energymodel) \
-initialEnergy 10 \
-rxPower 0.5 \
-txPower 1.0 \
-idlePower 0.0 \
-sensePower 0.3 \
-agentTrace ON \
-routerTrace ON \
-macTrace OFF \
-movementTrace ON
for {set i 1} {$i < 3} {incr i} {
set energy($i) [expr rand()*500]
$ns node-config -initialEnergy $energy($i) \
-rxPower 0.5 \
-txPower 1.0 \
-idlePower 0.0 \
-sensePower 0.3
set node_($i) [$ns node]
$node_($i) color black
}
```

IV. SYSTEM ANALYSIS

The proposed schemes have been experimented in the simulation environment in NS2. The simulation parameters are shown in Table 4. All the parameters such as the size of the network, what kind of propagation is going to use in the routing protocol. Which MAC layer rules are applied and the type of the antenna is used in the network model. The time duration of the entire simulation and the nodes deployment method with the number of nodes and number of clusters mention in the simulation settings. Finally, the node initial energy, size of the data packet used in data transmission is given in Table 4.

Table 4 Simulation Parameters

Parameter	Level
Area	500m*500m
Propagation Model	Two-ray ground reflection
Number of Nodes	101
MAC	802.11
Antenna	Omni directional
Simulation Time	100 s
Placement	Random
Number of Cluster	13
Node Initial Energy	100 J
Equal energy (Start up)	Yes
Packet Size	1000

The network is deployed with 101 nodes and each of them communicates with each other by using Leach protocol.

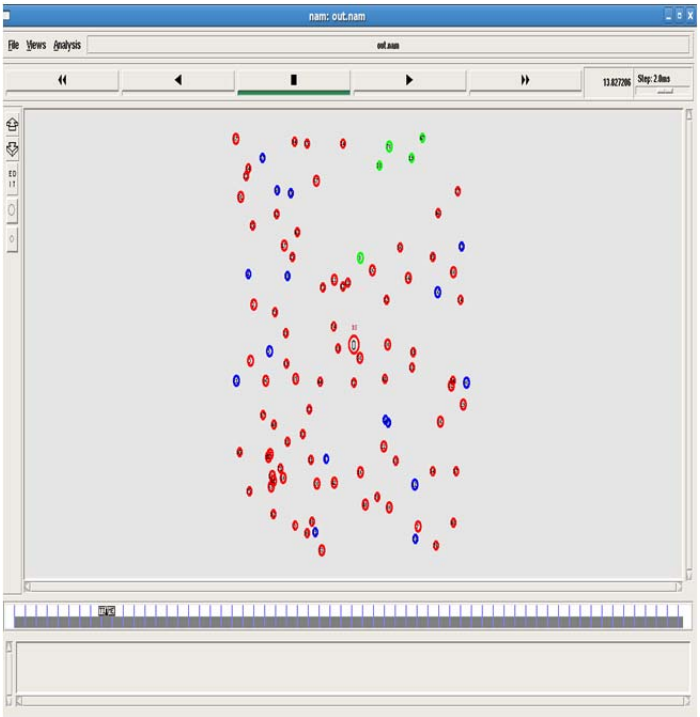


Fig. 9 The Leach protocol Network

Then Leach-e-ga algorithm is implemented, we have selected the Base Station, Cluster heads and the normal nodes of each cluster. The base station or sink node (BS) is shown by red colour and 13 cluster heads are shown by blue colour and remaining nodes for the respective nodes are acting as cluster members for their respective cluster heads. During the simulation Sybil Attack nodes will be detected and removed from the network by using Leach-e-ga algorithm. And this will provide the required security to the network.

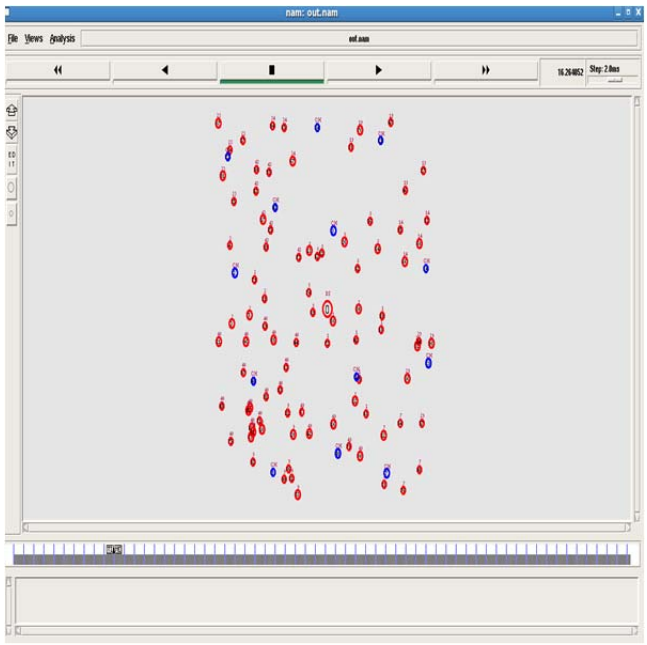


Fig. 10 Leach-e-ga algorithm

Then the transmission range is defined between the sensor nodes. And node 54 starts to communicate with node 93 and transfer the data.

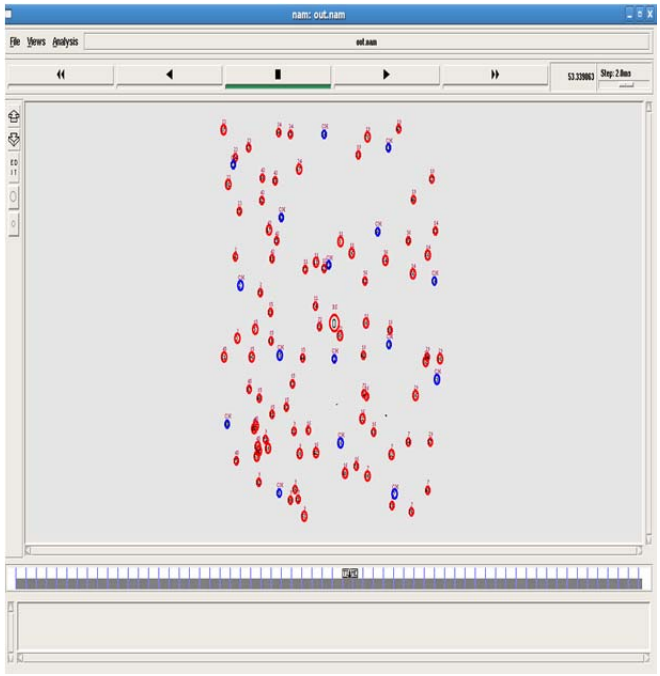
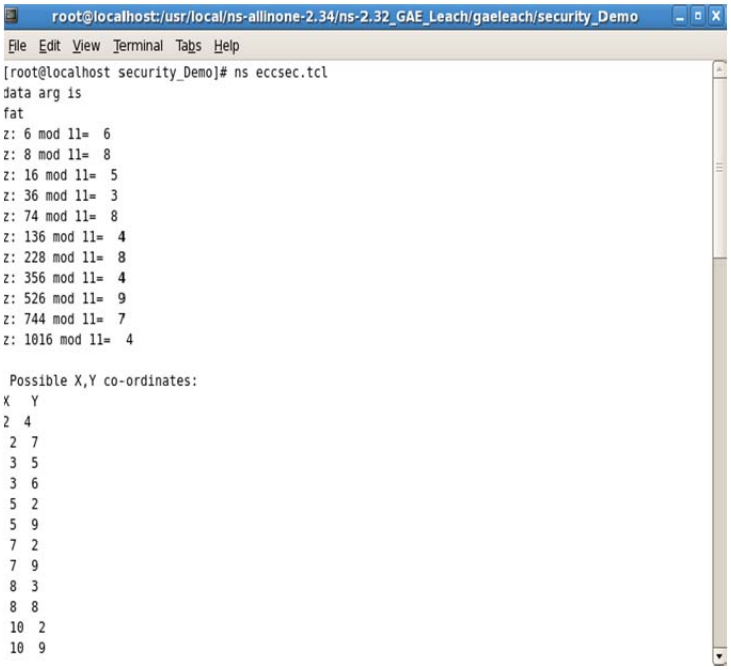
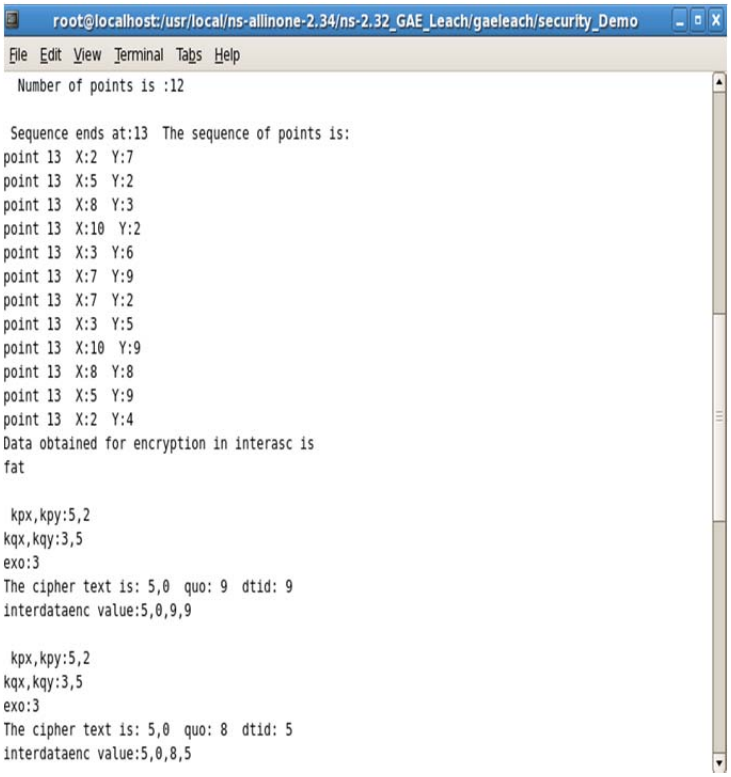
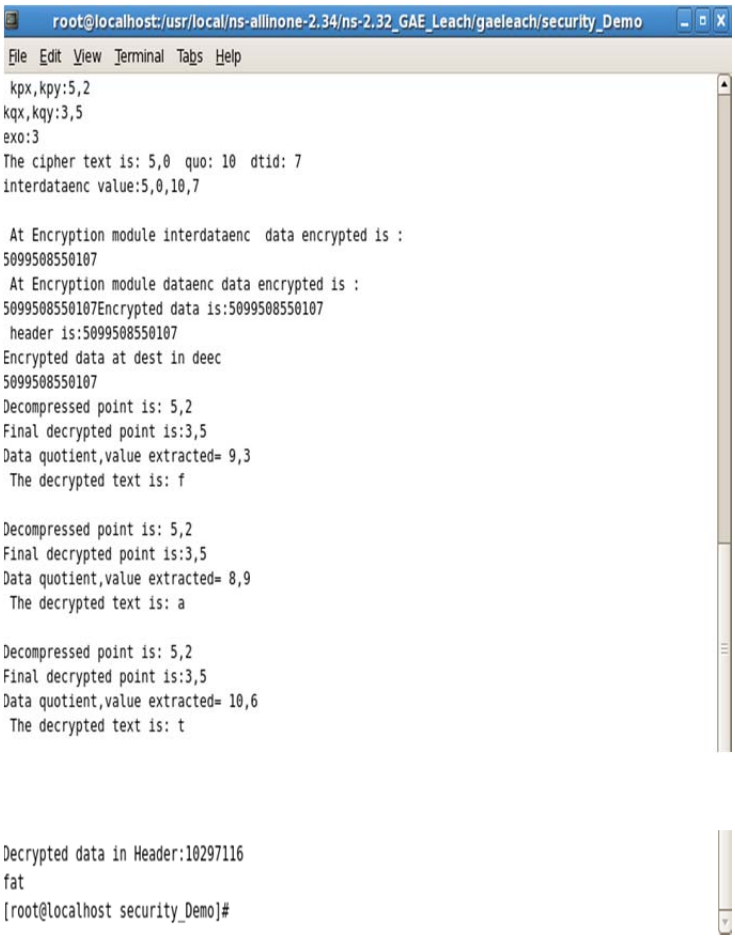


Fig. 11 Transmission range of sensor nodes

Then the Elliptic curve cryptography is implemented to secure data transmission between the sensor nodes and to provide more security to the network.







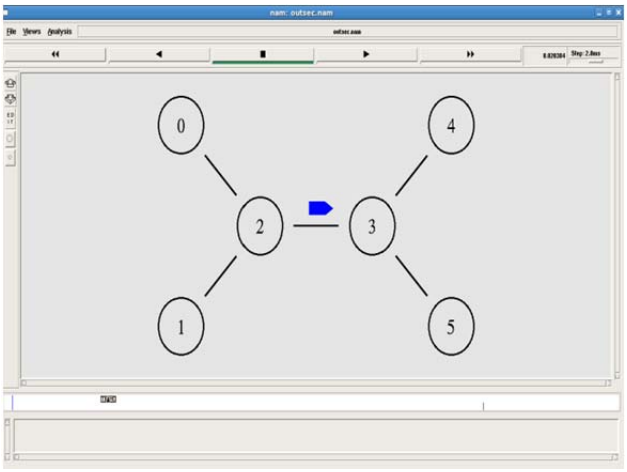


Fig. 14 Elliptic curve cryptography to communicate between the nodes

The following graphs show the improvements of network quality of service (Qos) parameters like Packet Delivery Ratio, Packet Drooping Ratio, Jitter, Throughput, Network Life Time and Security ratio using RSA and ECC.

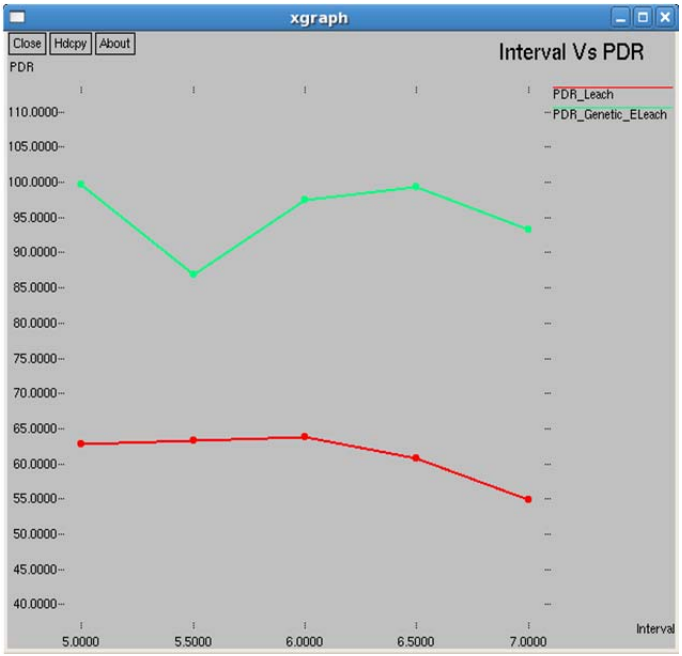


Fig. 15 Packet Delivery Ratio Vs Interval

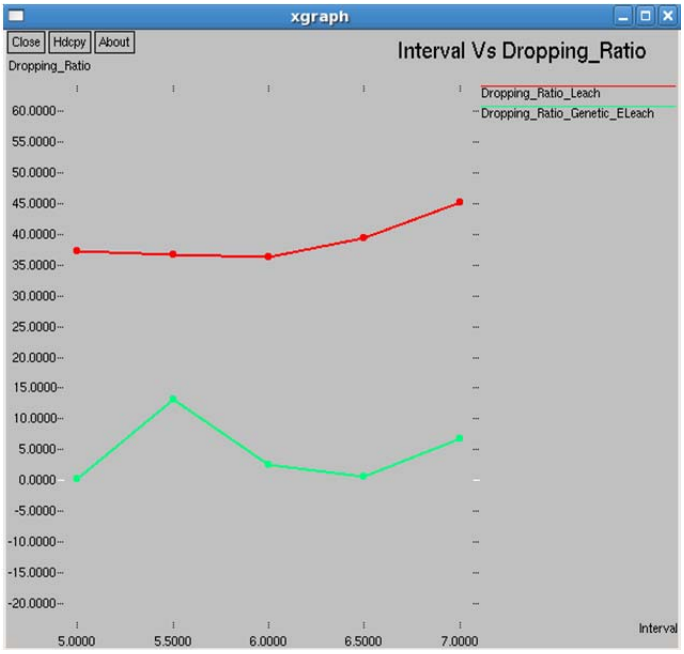


Fig. 16 Drooping Ratio Vs Interval

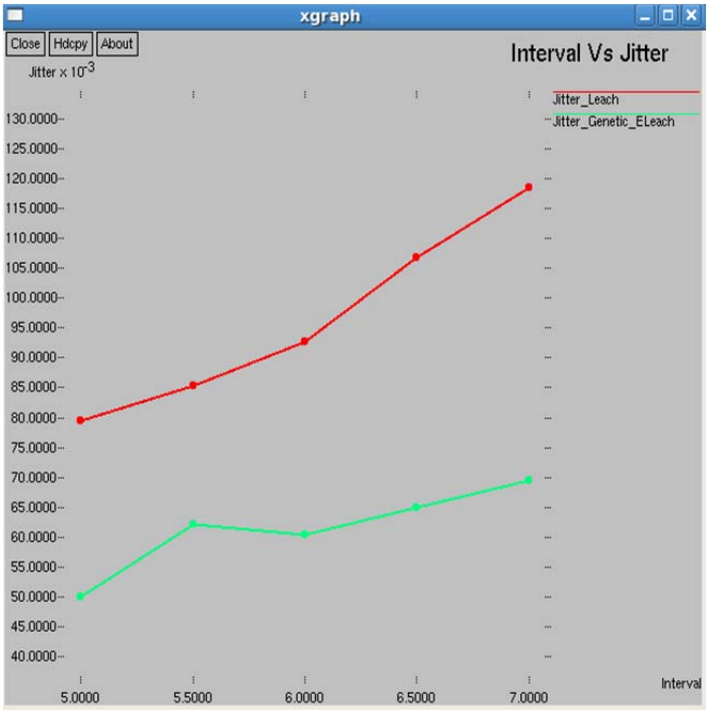


Fig. 17 Jitter Vs Interval

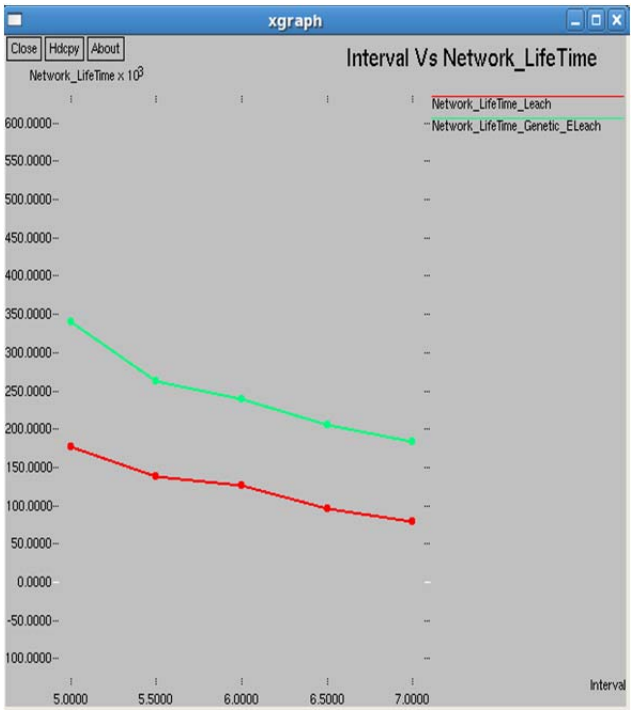


Fig. 19 Network Life Time Vs Interval

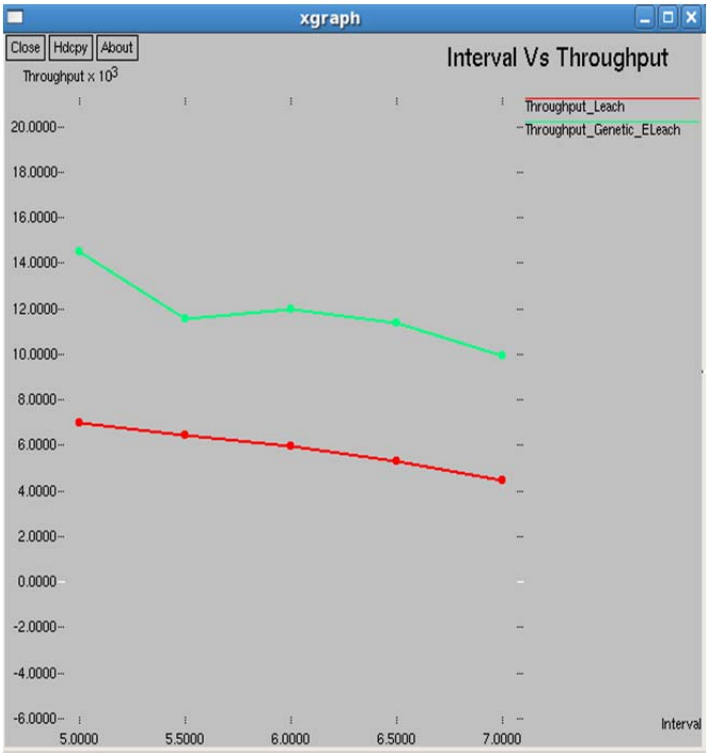


Fig. 18 Throughput Vs Interval

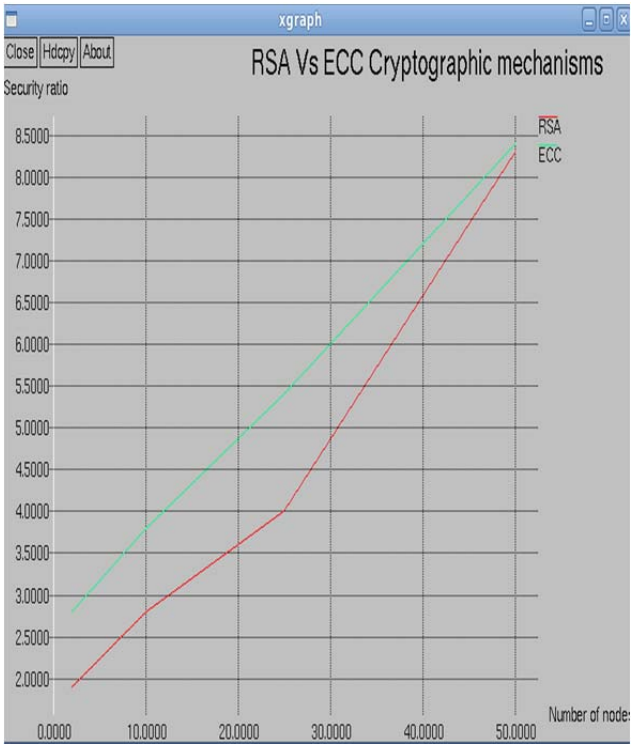


Fig. 20 Number of nodes Vs Security ratio using RSA and ECC

Fig. 15 represents the graph plotted against Packet Delivery Ratio Vs interval considering the implemented methodologies. Fig. 16 represents the graph plotted against Drooping Ratio Vs interval, Fig. 17 represents the graph plotted against jitter Vs interval, Fig. 18 represents the graph plotted against Throughput Vs interval, Fig. 19 represents the graph plotted against Network Life Time Vs interval and Fig. 20 represents the graph plotted against Number of nodes Vs Security ratio using RSA and ECC for the implemented methodology.

The comparison between the ECC and RSA is represented in the following table 5:

Table 5 Comparison of RSA and ECC

Sr. No.	Parameters	RSA	ECC
1.	Key Size	Large	Small
2.	Security	Weak	Strong
3.	Key	Generation	Fast
4.	Encryption	Fast	Slow
5.	Decryption	Slow	Fast
6.	Power Usage	High	Low
7.	Throughput	Average	High
8.	Response	Time	Average
9.	Latency	High	Low
10.	Protocol	Performance	Average

EXPECTED OUTCOME

Random Password Comparison [RPC] technique is added to leach-e-GA to provide more accuracy and thereby improve data transmission in the network also it will increase the throughput. RPC algorithm discovers a valid route in the sensor network by checking each node is a trustable node or a Sybil node so that the data can be transmitted very safely. The Sybil nodes are detected and data leakage is avoided completely by using RPC. As the Sybil nodes are detected in the discovery stage of finding initial route, they enable continuation of further transmission without any fear of attack.

V. CONCLUSION

In wireless sensor networks, the energy limitations of nodes play a crucial role in designing any protocol for implementation. The wireless sensor networks continue to grow and become widely used in many applications. So, the need for security becomes vital. However, the wireless sensor network suffers from many constraints such as limited energy, processing capability, and storage capacity, etc. There are many ways to provide security, one is cryptography.

In this work, it is aimed to select nodes for clustering using LEACH-E-GA in order to improve the energy efficiency with trusted nodes. Before, clustering all the nodes are optimized by the Genetic Algorithm and LEACH-E do clustering and CH election. The nodes are optimized using their attributes such as energy value, distance, and trust value.

Then we apply our cryptography scheme to provide security services in WSNs. Public Key based cryptographic schemes were introduced to remove the drawbacks of symmetric based approaches. In this work, we have studied two schemes ECC and RSA. At the analysis, it is found that Leach-e-ga with ECC is more advantageous compared to normal leach in terms of Network Qos like Packet Delivery Ratio, Packet Drooping Ratio, Jitter, Throughput, Network Life Time and Security ratio using RSA and ECC.

ECC is more advantageous compared to RSA, due to low memory usage, low CPU consumption and shorter key size compared to RSA. Though, the operations in RSA are comparatively faster than ECC. In RSA key generation and encryption are faster whereas decryption is slower. On the other hand in ECC key generation and encryption are slower whereas the decryption is faster. From this conclusion RSA is faster but it is said that security wise ECC is stronger than RSA.

Vi . FUTURE WORK

Among varieties of routing schemes LEACH-E-GA along with ECC routing protocols offer better choices to researchers to achieve more improvements of Network efficiency and Network security. The best performance to provide security can be obtained by improving the existing system based on LEACH-E-GA with ECC for wireless sensor networks with the following approach of requirement of security level and selection of appropriate ECC parameters set, selection of cryptographic scheme and formats for network transfer of keys.

ACKNOWLEDGMENT

Foremost, I would like to express my sincere gratitude to lecturer J.E. Kamalasekaran for the continuous support during my work, for her motivation, enthusiasm, and immense knowledge. Her guidance helped me in all the time of research and writing of this research.

I would like to thank the Department of Computer Engineering SCOE, especially the management Prof. M. P. Wankhade, Head of Computer Engineering Department and those members of Seminar Review committee for their input, valuable discussions and accessibility. In particular, I would like to thank Prof. M. P. Wankhadeand Prof. D.D. Gatade for their support, expertise and patience, Prof. G.T.Chavan, ME Coordinator he has been always there for guidance and give advice. I am deeply grateful to him for his continuous encouragement and guidance. I thank all my fellow lab mates and my friends in the college.

Last but not the least; I would like to thank my family: my parents, my wife for supporting, encouraging me spiritually throughout my life.

REFERENCES

[1] Alakesh, B., & Umapathi, G. R. (2014). A Comparative Study on Advances in LEACH Routing Protocol for Wireless Sensor Networks. A survey International Journal of Advanced Research in Computer and Communication Engineering, 3(2).

[2] Bani, Y. M. et al. (2009). Improvement on LEACH Protocol of Wireless Sensor Network(VLEACH). International Journal of Digital Content Technology and its Applications, 3(2).

[3] Batina, L., Mentens, N., Sakiyama, K., Preneel, B., Verbauwhede, I, "Low-cost elliptic curve cryptography for wireless sensor networks" Lecture Notes in Computer Science, 4357: 6 17, 2006.

[4] Choi, K., Song, J., "Investigation of feasible cryptographic algorithms for wireless sensor network", 8th ICACT-2006, 2, 2006.

[5] Dr. Shu Yinbiao, Dr. Kang Lee, Mr. Peter Lanctot," Internet of Things: Wireless Sensor Network" White Paper 2014 International Electrotechnical Commission-IEC, China. (http://www.iec.ch).

[6] Elhoseny, M., Yuan, X., Yu, Z., Mao, C., El-Minir, H., Riad, A., 2014. Balancing energy consumption in heterogeneous wireless sensor networks using genetic algorithm. In: IEEE Commun. Lett. PP (99), 1.

[7] Fan, J., & Parish, D. J. (2007). Using a Genetic Algorithm to Optimize the Performance of a wireless Sensor Network. ISBN: 19025-6016-7 2007 PGNet.

[8] Goldberg, D. et al. (1989). Messy genetic algorithms: Motivation, analysis, and first results. The Clearing house for Genetic Algorithms (TCGA), Report 89003.

[9] http://shodhganga.inflibnet.ac.in/bitstream/10603/22912/7/07_chapter_01.pdf

[10] Jai Prakash Prasad and Dr. Suresh Chandra Mohan "Security Enhancement of N-Tier Grid Protocol Using Elliptical Curve Cryptography for WSN" International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol.5, No 6, December 2015, ISSN: 2250-3501

[11] Ms. Reena S. Satpute, Prof. R. S. Mangrulkar,and Prof. A. N. Thakare" Performance Analysis of Wireless Sensor Networks using Elliptical Curves Cryptography" B.D.C.O.E., Seagram Maharashtra, India- Pin Code-442001. International Journal of Engineering Research & Technology (IJERT) Vol. 3 Issue 7, July - 2014 ISSN: 2278-0181

[12] N. Gura, A. Patel, and A. Wander, "Comparing elliptic curve cryptography and RSA on 8-bit CPUs,"in Proceedings of the 2004 Workshop on Cryptographic Hardware and Embedded Systems (CHES), August 2004.

[13] Nguyen, D. T. et al. (2012). An Improved LEACH Routing Protocol for Energy-Efficiency of Wireless Sensor Networks. Smart Computing Review, 2(5).

[14] P. R. Gundalwar, Dr. V. N. Chavan," A literature review on Wireless Sensor Networks (WSNs) and its Diversified Applications" International Journal of Advanced Research in Computer Science (IJARCS 2012), Volume 3, No. 7, Nov-Dec 2012 ISSN No. 0976-5697

[15] Petre-Cosmin, H. et al. (2010). Hierarchical Routing Protocol based on Evolutionary Algorithmsfor Wireless SensorNetworks. 9th RoEduNet IEEE International Conference 2010.

[16] Prabhjotkaur, Aayushi Chada, Sandeep Singh," Review Paper of Detection and Prevention of Sybil Attack in WSN Using Centralizedids", International Journal of Engineering Science And Computing (IJESC), July 2016, Volume 6 Issue No. 7

[17] R. Amuthavalli and R. S. Bhuvaneswaran, "Genetic Algorithm Enabled Prevention of Sybil Attacks for LEACH-E", in Modern Applied Science Vol. 9, No. 9; 2015, Published by Canadian

[18] Rupinder Singh, Dr. Jatinder Singh, and Dr. Ravinder Singh," SYBIL ATTACK COUNTERMEASURES IN WIRELESS SENSOR NETWORKS", International Journal of Computer Networks and Wireless Communication, Vol.6, No 3, May-June 2016, ISSN: 2250-3501(IJCNWC 2016)

[19] S.Sharmila, G Umamaheswari. (2012). "DETECTION OF SYBIL ATTACK IN MOBILE WIRELESS SENSOR NETWORKS". INTERNATIONAL JOURNAL OF ENGINEERING SCIENCE ADVANCED TECHNOLOGY, Volume-2, Issue-2, 256, 262,ISSN: 22503676 (IJESAT 2012)

[20] Shankar, M. et al. (2012). Performance Evaluation of LEACH Protocol in Wireless Network. International Journal of Scientific & Engineering Research, 3(1).

[21] Shigenobu Sasaki, Sabah M. Ahmed, Mohammed Abo-Zahhad, and Nabil Sabor. "A New Energy-Efficient Adaptive Clustering Protocol Based on Genetic Algorithm for Improving the Lifetime and the Stable Period of Wireless Sensor Networks" International Journal of Energy, Information and Communications, Vol.5, Issue3 (IJEIC 2014)

[22] Shilpa Goyal, Ms. Nisha Pandey, Computer Science and Engineering Department Shri Ram College of Engg Mgmt Palwal, India, Detection and Mitigation of Sybil Attack by Implementing Extended Genetic Algorithm, in International Journal on Recent and Innovation Trends in Computing and Communication IJRITCC June 2016 Volume: 4 Issue:

[23] Szczechowiak, P., Oliviera, L., Scott, M., Collier, M., Dahab, R., "NanoECC: Testing the limits of Elliptic Curve Cryptography in Sensor Networks EWSN 2008', 4913: 305 320, LNCS, Springer- Verlag, 2008.

[24] Vikram, M., & Neena, G. (2012). Performance Analysis of QoS Parameters for Wimax Networks. International Journal of Engineering and Innovative Technology (IJEIT), 1(5).

[25] Wander, A., Gura, N., Eberle, H., Gupta, V., Shantz, S., "Energy analysis of public-key cryptography for wireless sensor networks," 3rd IEEE International Conference on Pervasive Computing and Communication, 2005.

[26] Wu, X. H., & Wang, S. (2010). Performance Comparison of LEACH and LEACH-C Protocols byNS2. Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science.

[27] Yeh, H., Chen, T., Liu, P., Kim, T., Wei, H., "A Secured Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography", Sensors, 4767-4779, 2011.

[28] Yu, Y., Viktor, K., & Prasanna, B. K. (2006). Introduction to Wireless Sensor Networks. Information Processing and Routing in wireless sensor networks, World Scientific Publishing Co.,Pte.Ltd. Retrieved from http://www.worldscibooks.com/compsci/6288.html

[3]

[4]

[12