inappropriate for dynamic sensor networks [6]. Both these schemes rely on flat sensor networks.

In 2003, Jolly et al. [8] proposed a low-energy key management(LEKM) protocol for sensor-to-gateway keys management. In this model, the sensor nodes are deployed in the areas of interest. There are sensor nodes, command nodes and gateways. The gateways have comparatively high storage, energy and processing power. The gateway nodes partition the network into different clusters. Each cluster is composed of a gateway node and number of sensor nodes. The sensor nodes sense the event and the gateway node aggregates the data from different sensors and sends them to the command node that controls the mission of the network. This is a Time Division Multiple Access (TDMA) based Media Access Control where the sensors will be in active mode only in the slot allotted to them. Other time they are sleeping.The key management in this scheme is such that a sensor node stores only two keys-one it shares with the gateway and the other it shares with the command node. The command node has high storage and is situated in a friendly area. So it stores keys of all nodes. The gateway node stores keys it shares with the members in its cluster and the key it shares with the command node. Since the gateway node is preloaded with m/n keys in the initialization phase, the compromise of it can breach the security

3. Hierarchical Sensor Networks

Compared with the flat network architecture hierarchical sensor networks (HSNs) are more often used in real applications because they can improve the network throughput and reduce the energy consumption [7].

A HSN is organized as a clustered network, which consists of different types of nodes with widely varying abilities and energy resources, for example, cluster head node (CH), sensor member node, and base station (BS). The communication system of a hierarchical sensor network can be divided into two levels namely Intra Cluster Communication and Inter Cluster Communication. Intra Cluster communication refers to the communication between the sensor member nodes that comes under the same cluster head (CH) whereas Inter Cluster Communication is the one between member sensor nodes that belongs to the different clusters.

4. Proposed Scheme

The proposed system is based on hierarchical wireless sensor networks, where nodes have varying capabilities. The hierarchical networks can help in providing different levels of security. The proposed considers a group of sensor node (called member sensor nodes) being headed by a group head (cluster head).A group of cluster heads headed by a super cluster head. The main types of communication that occur in these networks are:

- **Intra-Cluster Communication**:- This happens between the member sensor nodes within the same group or cluster.
- **Inter-Cluster Communication**:- This occurs between the sensor nodes that belong to different clusters. This can be between sensor nodes that belong to same or different super cluster heads.
- The proposed scheme offers mutual authentication in addition to key management. It is a major requisite since the wireless networks are always susceptible to attacks.
- The different phases in the proposed system are explained below:
- **Initialization:-** This phase is done prior to deployment of Wireless Sensor Nodes. The member sensor nodes, cluster heads and super cluster heads are pre-distributed with different values. The Super Cluster Heads are pre-distributed with an authentication key $K_{SCHAuth}$, a pair of public key/private keyK_{Pub} , K_{Pri} and a document signed by the base station. The public key of the base station is pre-distributed in the cluster head. The public private key pairs are created as follows:

An Elliptic Curve of the form

$$y^2 = x^3 + ax + b \ mod \ P$$

is selected. A base point, BP, on the curve is chosen. A random integer, S, is chosen and kept secret. S is the private key K_{Pri}. The public key K_{Pub} is calculated as S*BP is calculated. The * denotes the point multiplication.

The algorithm for Scalar Multiplication is as follows:

The binary representation of private key S

$$S = (k_{m-1}, k_{m-1}, \dots, k_0), \ k_m = 1$$

Compute Q=S*P
Q=P
For i=m-2 to 0
Q=2Q
If $k_i = 1$then Q = Q + P
End if
End For
Return Q

The signature for the digitally signed document is created by the following algorithm:

4.1 Signature Generation

Private keyd_A, Public key $Q_A=d_AP$.

1. Select a random k from [1, n-1]
2. Compute $kP = (x_1, y_1)$and $r = x_1 \ mod \ n$.if$r=0$ goto step 1
3. Compute e=H(m), where H is a hash functon, m is the message.
4. Compute $s = k^{-1}(e + d_A * r) mod \ n$ If s=0go to step 1.

(r, s) is Alice's signature of message m

4.2 Signature Verification

1. Verify that *r, s* are in the interval [1,*n*-1]
2. Compute $e=H(m)$, where *H* is a hash functon, *m* is the message.
3. Compute $w=s^{-1} \ mod \ n$
4. Compute $u_1=ew \ mod \ n$ and $u_2=rwmod \ n$.
5. Compute $X=u_1P+u_2Q_A=(x_1, y_1)$
6. Compute $v=x_1 \ mod \ n$
7. Accept the signature if and only if $v=r$

4.3 Bootstrapping Phase

During this phase the cluster heads and super cluster heads carry out mutual authentication in order to protect them from man-in-the-middle attack. The Super Cluster heads send the digitally signed document to the cluster heads and using the pre-distributed public key of the base station, the cluster heads could verify the signature.
After mutual authentication, the super cluster head chooses a large prime number r_t and a modulus p. The key seed $Seed_j$ is calculated as follows:

$$Seed_j = k_j\ p + r_t\ j = 1,2,3, \dots \dots \dots \dots, M$$

The value of k_j is known only to the super cluster head. The seed value is send to the cluster heads by the super cluster heads.The super cluster heads stores the seed values.

4.4 Key Generation Phase

Two integers a and b are congruent if they give the same remainder when divided by a positive integer p. This is written as follows:

$$a \equiv b\ (mod\ p)$$

The key$K_{CH_j SCH_t}$ is the key between the cluster head and super cluster head. $K_{G_t}$is the group key.The group key is shared by all cluster heads under the same super cluster head. Each cluster head in the network has a large integer as its key seed. So each cluster head under the same super cluster head can get the same remainder when divided by the same modulus.

$$K_{CH_j SCH_t} = f\left(Seed_j\right)\ j = 1,2,3, \dots \dots \dots \dots, M$$

$$K_{G_t} = f\left(Seed_j\ mod\ p\right)\ j = 1,2,3,\dots, M$$

Where f is a function that converts the numerical value of seed into the word and again converts to numerical equivalent to get a large key value. This is the shared encryption and decryption key. Due to the congruence property of modular arithmetic, all the cluster heads under the same cluster head can compute the shared group key K_{G_t}.

4.5 Key Establishment between Nodes

Sensor nodes are used to collect and process useful data. This data is transmitted to the cluster head via multiple hops. So it needs to be encrypted by the different keys that are being shared between different types of sensor nodes.

Key Establishment between Cluster Heads belonging to same Super Cluster Head:- The super cluster head generates a session key and sends it to both of the Cluster Heads encrypted by the key shared between them. To establish a session key between two cluster heads, the cluster head CH_1 sends a key setup request to its super cluster head. This message contains IDs of these two sensor nodes. After the super cluster head SCH_1 receives this request, it randomly generates a session key by a pseudo random function and encrypts it by the shared keys with these nodes. The encrypted session keys are sent to these two nodes respectively. Each node receives this encrypted session key, decrypts it, and begins to communicate with each other securely.

Key Establishment between Cluster Heads under different Super Cluster Heads:- Let N_1 be a node belonging to a cluster head CH_1. CH_1 belongs to the Super Cluster Head SCH_1. N_1wants to communicate with N_{10} that belongs to CH_5under the super cluster head SCH_2. N_1 sends a key request message with the id of $N_{10}$to its cluster head CH_1. The cluster head generates a session key encrypts it with the key it shares with the SCH_1 ,$K_{CH_1 SCH_1}$ and sends it to SCH_1. The SCH_1 sends the key to the SCH_2encrypted by the key K_{S1S2}. SCH_2 encrypts it with the key $K_{CH_5 SCH_2}$.

The shared key $K_{S1S2}$is created on demand using elliptic curve Diffie-Hellmen [9] algorithm as follows:

The Super Cluster Head SCH_1will calculate the shared key K_{S1S2} by the point multiplication of private key of $SCH_1$and public key of SCH_2.

Similarly SCH_2 will calculate the shared key K_{S1S2} by the point multiplication of private key of SCH_2 and the public key of SCH_1.

Removal of a Compromised Cluster Head and Selection of New One:- Assume that the Super Cluster Head can detect the compromise of a Cluster Head. A member sensor node with maximum remaining energy is identified and made the new Cluster Head. The base station removes the connection with the compromised node, a new key seed is send to the cluster head and a different key is established.

5. Experimental Setup and Results

The system was implemented in NS2 and various aspects have been evaluated. *NS*2 is a discrete event simulator for networking research. It is a piece of software or hardware that predicts the behavior of a network without an actual network being present. It can set up packet traffic similar to internet and measure various parameters. Here a network is created and a new application layer protocol is designed that could carry the additional key details in it. Group deployment is employed.

Key Storage Space: Key storage space is the total memory usage of keys stored in the network. In the proposed scheme each cluster head needs to store only a key seed. The Super cluster head has a digital document, a pair of public/private keys, a key seed table.

Time Consumption for Key Establishment:-In the basic schemes of key establishment consists of two phases:- the shared key discovery phase and path key establishment phase. The shared-key discovery phase takes place after each node has finished finding shared keys with its neighbors. Each node broadcasts a list of identifiers of the keys on its key ring to all its neighbors. Two neighboring nodes will setup a secure link if they share at least one key. However, if two neighboring nodes have no keys in common, they will begin a path key establishment phase with the help of their neighbors. A path key establishment may span one or more hops. If the nodes cannot be reached via a shared key (i.e., one link or one hop),it will take at most two or three hops to contact it. We can find that the time consumption of key establishment under the basis scheme is affected by the

following three factors: the number of a node neighbors, the key ring size, and the key pool size.

In the proposed scheme, there is no need to find the shared keys. Here the time consumption of key establishment is the time for each node to finish authentication and get a key seed from the super cluster head. So even if the number of nodes increases the time consumption for key establishment is unique.

Resilience against Sensor Node Capture:- Wireless sensor nodes are more likely to be captured than other wireless nodes due to the constraint capability of sensor nodes. Thus, the resilience of a wireless sensor network is very important. When a sensor node is compromised, we assume that the adversary can get all materials of the node. In a key-pool based key management scheme, the capture of a sensor node will disclose some keys of the network. Other sensor nodes that have a subset of keys shared with this node will be affected. When the keys stored in the captured node are revoked, it will decrease the connectivity of the network. In the proposed method the shared session keys are established on demand. Each pair of nodes shares a unique symmetric key, and this session key is blind to other member sensor nodes. Thus, the capture of member nodes has no impact on the secure links between other uncompromised nodes. The comparison of number of links being compromised by compromising different number of nodes in the case of proposed method and the basic Eschenauer and Gligor[3] method is plotted.

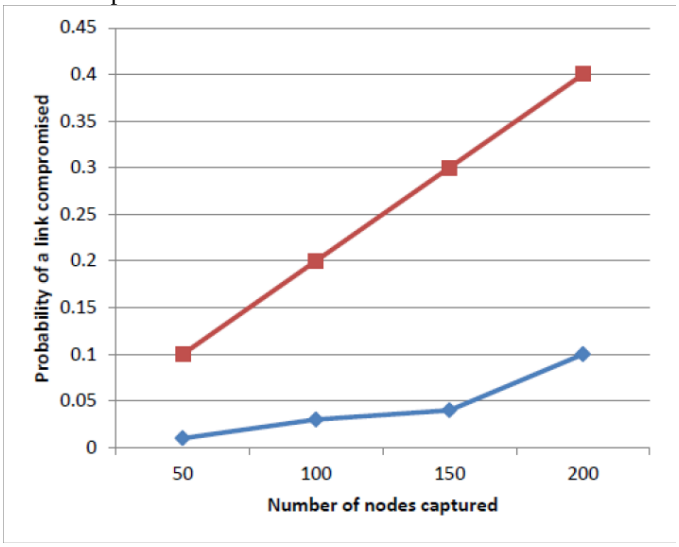

Figure 1: Resilience Against Node Capture

Energy Consumption for Key Establishment: Although security is a critical issue in wireless sensor networks, it is also necessary to consider the energy consumption of sensor nodes because they are constraint in power supply.

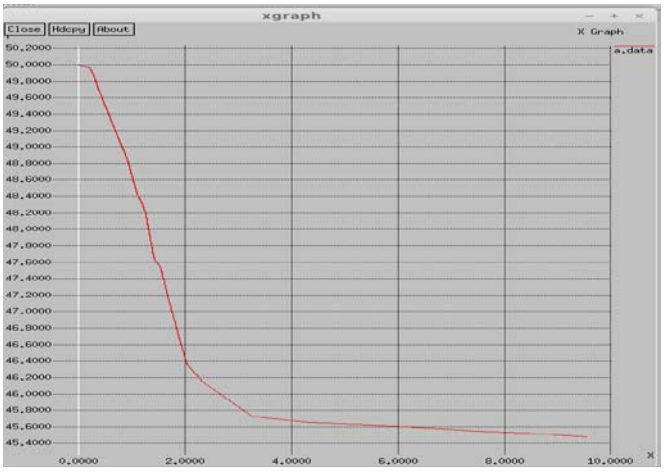

Figure 1: Graph Between Time and Energy Consumption

If some sensor nodes run out of energy, the performance of the whole network will be degraded. In our MAKM scheme, we have tried to provide an energy-efficient solution. The graph of Energy against Time is shown in the Figure:2. The Graph shows that the energy is consumed only in the earlier stages of key establishment. After that the energy consumption is uniform.

.

6. Conclusion

Key Management in WSNs becomes a serious issue due to the resource constraints of sensor nodes in the wireless sensor networks. Functionalities like authenticity, confidentiality, flexibility and integrity need to be maintained by the system. Key management is the precondition of all security issues, for example, data encrypting/decrypting, mutual authentication and message integrate and so on. Cryptographic Key establishment is a prior requisite for secure communication. Here an intra-cluster key management technique for hierarchical wireless sensor networks is proposed.

In the proposed scheme, each super cluster head stores only a pair of private and public key in its memory, which means it is a storage-optimal scheme for the resource-limited sensors. Also some steps are performed offline or pre-distributed with some sort of key details, it reduces the power consumed. Each the cluster head receives a key seed only rather than a key, thus resilient against node capture attack. Mutual authentication is carried by using digital documents. And since elliptic curve cryptography is used, it is more energy efficient than other public key systems.

The proposed method is resilient against attacks since the capture of a super cluster head does not key, only a key seed.

References

[1] I.F Akyildiz, W.Su, Y.SankarasubramaniamAnd E.Cayirci:- “A Survey On Sensor Networks” :IEEE Communication Magazine Vol.40.
[2] Wenliang Du, Jing Deng, Yunghsiang S Han, Shigang Chen And Pramod K Varshney :- “A Key Management Scheme For Wireless Sensor Networks Using Deployment Knowledge”.

[3] Eschenauer .L, GligorV.D :- "Key Management Scheme For Distributed Sensor Network" :Ninth ACM Conf On Computer And Communications Security.
[4] Bloom R 1985:- "An Optimal Class Of Symmetric Key Generation"
[5] ChienH.Y, Chen R.C, ShenA :- "Efficient Key Pre-Distribution For Sensor Networks With Strong Connectivity And Low Storage Space" 22nd International Conference On Advanced Information Networking And Applications 2008.
[6] LihChyauWuu, Chi HsiagHing, Chia Ming Chang :- "Quorum Based Key Management Scheme In Wireless Sensor Networks " : ICUTMC'12 Malaysia.
[7] Bohg, .M,Trappe.W :- "An Authentication Framework For Hierarchical Ad Hoc Sensor Networks" : Second ACM Workshop On Wireless Security 2003.
[8] Jolly G, Kuscu M, Kokate P, YounisM :- " A Low Energy Key Management Protocol For Wireless Sensor Networks" : Eight IEEESympOn Computers And Communications, 2003.
[9] Dahai Du, "An Efficient Key Management Scheme for Wireless Sensor Networks", International Journal of Distributed Sensor Networks, Volume 2012, Article ID 406254.