ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 4, October 2013

Energy Optimized Secure Routing Protocol for Wireless Sensor Networks

Santhosh Simon, K Paulose Jacob
Department of Computer Engineering, Cochin University, Kerala, India

Abstract*— The evolution of wireless sensor network technology has enabled us to develop advanced systems for real time monitoring. In the present scenario wireless sensor networks are increasingly being used for precision agriculture. The advantages of using wireless sensor networks in agriculture are distributed data collection and monitoring, monitor and control of climate, irrigation and nutrient supply. Hence decreasing the cost of production and increasing the efficiency of production. This paper describes the security issues related to wireless sensor networks and suggests some techniques for achieving system security. This paper also discusses a protocol that can be adopted for increasing the security of the transmitted data.

Index Terms—**Wireless Network Security, Energy Efficient Mobile Network, Crop monitoring, Precision agriculture, Wireless Sensor Networks.**

I. INTRODUCTION

Kuttanad, the rice bowl of Kerala, is unique among the rice ecologies of the world; the biggest wetlands of the country, located 0.5 – 2.5 metres below mean sea level (msl). Rice is grown by construction of bunds and dewatering the so formed polders mainly during the puncha (rabi) season from Oct. – Nov. to Jan. – Feb. The soils of Kuttanad are low to medium in fertility. Soil is enriched by annual silt deposition during the mansoon floods. The soils are alluvial with silty clay texture and are acid sulphate in nature with excessive iron content. The major problems faced by Kuttanad rice are flood and lack of drainage, intrusion of saline water and soil acidity. The major occupation in Kuttanad is farming. Rice is the important agricultural product, giving Kuttanad the moniker of "The Rice Bowl of Kerala". Three crops are grown every year now instead of the traditional two per year. Large farming areas near Vembanad Lake were actually reclaimed from the lake. Rice is the one of the most widely grown crops in the world and is one of the major food crops grown extensively in India. The most important rice producing states of India are West Bengal, Andra Pradesh, Bihar, Tamil Nadu, Assam and Kerala. In Kerala, Palaghat, Trichur and Kuttanad are the main rice producing regions. The vast area of paddy fields in Kuttanad extends from 90 17' N to 90 40' N and 76019' E to 76033' E. These are divided into "padasekharams" literally meaning groups or blocks of paddy fields and are separated by canals, bunds and water-logged masses. The puncha lands of Kuttanad are classified under three categories based on elevation, geographical formation and soil characteristics, into Karappadoms, Kayal lands and Kari lands. The Karappadoms are generally situated along with the waterways and constitute the lower reached of the eastern and southern periphery of Kuttanad, usually 1-2 m below mean sea level. Vembanad Lake for agricultural purpose and the elevation ranges from 1.5 to 2.5 m below the mean sea level. The soil of the paddy fields of Kuttanad is salty and is extremely acidic. The acidity is due to the production of sulphuric acid by microbiological oxidation of sulphur compound present in the soil. High amount of iron, manganese, aluminum and sulphides are present in the soil. This acidity of the soil is a major constraint which retards the production of rice in the Kuttanad area. Regular rinsing of the soil by water can reduce the acidity and increase the production. Due to the socio-economic states prevailing in the state of Kerala the labor community is getting narrower. The paddy field owners are not able to recruit sufficient labors for these processes. The initial activities like plowing, seeding etc and the final activities like harvesting are done as a group and hence can be easily coordinated. The periodic monitoring of needs, controlling the pests and water level monitoring is a tedious process. Majority of the paddy field farmers are employed in some other activities or are considering this cultivation as a secondary business. Hence their involvement on a daily basis should be greatly reduced. Since the pumping of water to and from the field is the major activity from plowing to harvesting, automating the process can greatly reduce the load on farmers. Automated systems may monitor the water level and regulate the levels by sophisticated systems and can send messages to the farmers.

A. Wireless Sensor Network For Monitoring Water Level

Paddy field is a large area and is nearly flat in nature. Normally the water level in a field will be uniform throughout the field. Water wells can be made as per the need and the water level in each well can be monitored. Water level sensors can be used for sensing the levels. Even though electronic sensors are available due to the environmental conditions electro-mechanical devices are more applicable. The mechanical part in the devices will float on water and the electrical part will produce the signals based on the portion of the floating device. These values or signals generated by the sensor needs to be transmitted to the farmers. Due to the issues like transmission media, power consumption, security etc, conventional communication techniques cannot be used. Low cost communication devices which needs low power and less maintenance, which can operate on a wireless architecture is the solution. The new generation wireless sensor networks can be considered for the situation.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 4, October 2013

Fig 1. Wireless Sensor Node in the Paddy Field

Wireless sensor Network (WSN) is a major technology used for real time monitoring of environmental assets. WSN has the advantages of large scale deployment, low maintenance, scalability, adaptability, less power needs etc. with the disadvantages of low memory, low power, low bandwidth etc. They can be employed in hostile environments and the features like use of low power and low maintenance makes them the most suited technology for real-time environmental monitoring. They can be highly useful in monitoring the water level in the paddy fields. ZigBee is the most commonly used netwok standard today and it is a low-cost, low-power consumption, low data-rate, two-way wireless networking standard that is aimed at remote control and sensor applications which is suitable for operation in harsh radio environments and in isolated locations. It builds on the IEEE standard 802.15.4-2003 which defines the physical layer and medium access control sub layer. Above this, ZigBee defines the application and security layer specifications enabling interoperability between products from different manufacturers. There are several different network topologies that a wireless sensor network can form: star, tree, bus, ring, and mesh. All these topologies have their own individual benefits but the mesh network topology is best suited in our case.

II. SYSTEM DESIGN

As described earlier we have three types of nodes in the network field. The base level is the sensor (SN) nodes which collect data from the physical sensors, packetize this data and send them through its cluster head (CH). The whole network is divided into many clusters and each cluster contains a number of sensor nodes and a head node (CH) which controls the sensor nodes (SN). The cluster heads of various clusters communicate each other for transmitting the data. The cluster heads transmits the collected data from the sensor nodes to the sink node. The sink node is the network controller node and is situated near to the cluster heads. The sink node is connected to the field control centre (FCC) (user computer) through a GPRS connection. The FCC is at a remote location and long distance communication in necessary between the sink node and FCC.

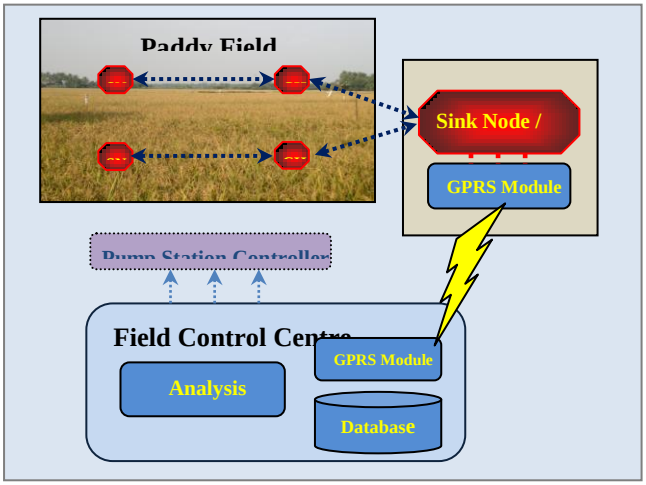

Fig 2. Wireless Sensor Network Architecture

A. SENSORS FOR MONITORING WATER LEVEL IN FIELDS

In our system the sensor network is deployed as a three tier system. The bottom level is the end sensor nodes(SN) which are normally in a sleepy condition. The water level sensors are connected in these nodes. They collect the values of water level from the electrical sensors and transmit them. The second tier is the routers or the cluster heads(CH). The end sensor nodes are grouped according to their geographical positions and for a group of end sensors a cluster head is allocated. The end sensor node sends their data to their respective cluster heads periodically. The cluster heads are connected to the sink node(SN) or the co-coordinator node which form the third tier. The overall monitoring and controlling is done by the FCC (Field Control Center). FCC is a software program residing in the user computer. The sink node transmit the data to the FCC and FCC issues the necessary commands for network monitoring and other operations like pumping in and out of water. Periodic monitoring of the water level in the paddy field is essential because the water supplied to the plants are different at different times for optimum or maximum crop production. The base level is the ordinary sensor nodes, which are large in number. They are divided into number of clusters and controlled by cluster heads(CH). The functions performed by the sensor nodes are precise and are normally done periodically. They collect the data from the physical sensors attached to them. These sensors nodes are mounted on the fixed sensor columns. These sensor columns contain the sensors for measuring the water level. These water levels are analog values. The sensor nodes count these values into digital data and packetize them. The data packets are transmitted to the cluster heads. These sensor nodes are simple devices, that is with low processing power and less battery power. Since the amount of energy is constrained the overall usage of these nodes should be limited and energy efficient schemes should be employed.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 4, October 2013

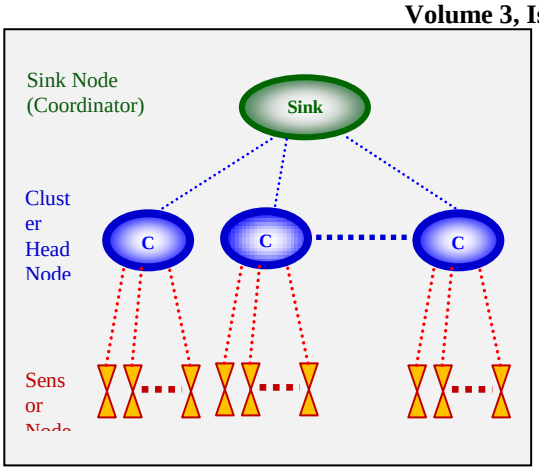

Fig 3. Node levels in WSN Architecture

III. NEED FOR SECURITY

Due to the unique characteristics of WSNs, they are vulnerable to security attacks compared to infrastructure based wireless networks. The main objective of security services in WSNs is to protect the data and resources from attacks. The major security requirements in WSNs are as follows:

- *Availability* - which ensures that the desired network services are available even in the presence of denial-of-service attacks.
- *Authorization* - which ensures that only authorized sensors can be involved in providing information to network services.
- *Authentication* - which ensures that the communication from one node to another node is genuine, that is, a malicious node cannot masquerade as a trusted network node.
- *Confidentiality* - which ensures that a given message cannot be understood by anyone other than the desired recipients.
- *Integrity* - which ensures that a message sent from one node to another is not modified by malicious intermediate nodes.
- *Nonrepudiation* - which denotes that a node cannot deny sending a message it has previously sent.
- *Freshness* - which implies that the data is recent and ensures that no adversary can replay old messages.

A. Security through Cryptology

The security services in WSNs are usually centered on cryptography. However, due to the constraints in WSNs, many already existing secure algorithms cannot be directly used in WSNs. Cryptology is one of the most common and reliable means to ensure security. It is the study of principles, techniques and algorithms by which information is transformed into an intermediate form which no unauthorized person can read, but can be recovered in its original form by an intended recipient. In the context of cryptography the information to be sent is known as plain text. This plain text is converted to cipher text by exemption. An authentic receiver can decrypt the cipher text back into plain text by the process of decryption. The encryption and decryption is done using keys. The four main goals of cryptography are confidentiality, integrity, authentication and non-repudiation. The two main types of cryptographic techniques are: symmetric key algorithm and asymmetric key algorithm. Symmetric key algorithm uses the same key for exemption and decryption while the asymmetric key algorithms uses two different key for exemption and decryption. Wireless sensor networking has certain specific challenges while implementing cryptography and key management, due to the lack of infrastructure. The first is the network infrastructure, such as dedicated routers and stable links. The second missing infrastructure is services such as name resolution, directory and TTPs. The third missing infrastructure in WSN is the administrative support of certifying authorities. Selecting the most appropriate cryptographic method is fundamental in WSN design because the strength of the security system is ensured through it. The selected cryptographic algorithm should be of low code size, low data size, less processing time and low power consumption. This is because of the low processing power, less memory size and low power capacity of the WSN nodes. Most of the public key algorithms are computationally intensive with large code size, data size and consumes much higher power. Hence they are undesirable to be employed for ensuring security in WSNs. Symmetric key cryptography is superior to public key cryptography in terms of speed, low data size and low energy cost. Due to the constraints in the WSNs, symmetric key cryptography is best suited for WSNs.

B. Key Management

The main objective of the key management scheme is to supply required keys between the sensor nodes that are to communicate each other. Since key is the crucial element of any cryptographic techniques, this key management is vital in WSNs security mechanisms. The WSNs has only very limited resources hence the key management schemes to be adopted are different from schemes in other networks. A separate key for each communicating nodes is impractical since n-1 keys are to be stored in each node in a network of n nodes. Hence large amount of memory is needed. In sensor network energy node may not be able to communicate with every other node so many of the keys are of no use. Also addition of new nodes and deletion is a tedious task. Based on the network structure the key management can be centralized or distributed. In a centralized scheme there is only one key distribution centre which generates and distributes the keys. The main disadvantage of this method is that the entire system is

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 4, October 2013

dependent on one key distribution centre (KDC). The failure of the network becomes vulnerable as keys are not generated or distributed. Also scalability is another drawback. In the distributed key management system there will be two or more key distribution centers for generating and distributing the keys. Therefore a single point of failure will not affect the entire system security. Thereby minimizing the risk of failures and improving the scalability. Even though the distributed key management system is found to be attractive, the overheads of maintaining multiple key distribution centers are a headache unless it is essential. Also the KDCs should be trustworthy. Considering the processing overheads of key generation and distribution the base station having KDC's should have more processing power and power backup. In our WSN system the sink node can be used as the KDC as it has more processing and memory power, and also the maintenance of the sink node is easy. Hence centralized key distribution mechanism is preferred for our WSN system.

C. Symmetric – Centralized – Session based key scheme

Our WSN system is designed to use a symmetric key cryptography algorithm and the keys are distributed from a central key distribution centre on a session basis. The sink node is the base node and it acts as the central key distribution centre. Below this we have the clusters with sensor nodes and cluster heads. The keys generated by the sink node or the KDC will be given to these cluster heads. These cluster heads transmits there keys to their sensor nodes. Initially at the time of system start up each sensor node will be loaded with a key which will be the initial key. The sensor node senses the values from the physical sensor devices and converts these values into digital data packet. This digital data is then encrypted using a symmetric cryptographic algorithm and the encrypted packet is send to the cluster head. This encryption is done using the key loaded to the system at the time of start up. After completing the time for one session the sink node or the KDC will generate a new session key using a pseudorandom function (f) and encrypt using the previous key and send it to the cluster heads. This new key is transmitted to the sensor nodes from the cluster heads. The sensor nodes on receiving the key packet, it decrypts the packet with the existing key and receives the new key for the new session. It uses the new key for the subsequent encryption and decryption and the process continues. Hence a new key is used by the system dynamically for every session. The data packets send by the sensor nodes are encrypted by a symmetric cryptographic algorithm known as Blowfish and hence making the communication more secured.

D. The Blowfish Algorithm

A standard encryption algorithm must be implementable on a variety of different platforms. The algorithm should be efficiently implementable on a VLSI custom made hardware, should be simple to code, easy key management and should be easily modifiable. Blow fish is a variable length key, 64 bit block cipher. The algorithm consists of two parts: a key of at most 448 bits into several sub key arrays totaling 4168 bytes. Data encryption occurs via a 16 round Feistel network. Each round consists of a key-dependant permutation, and a key and data dependent substitution. All operations are XORs and additions on 32 bit words. The only additional operations are four indexed array data lookups per round. The mini version of Blowfish is blowfish-16 which has a 16 bit block size and sub key arrays of 8-bit entries, each s-box has 4 entries [35]. Different cryptographic algorithms were evaluated for performance. DES is a powerful encryption algorithm. Its 56-bit key size is vulnerable to a brute-force attack [34]. Other algorithms like Khufu [25,26], REDOC II [14,13,19], and IDEA [27, 17, 18] are protected by patents. AES algorithm [9] is a very fast algorithm but requires at least 800 byte memory space for lookup tables. RC6 [12] is a small algorithm, but it is slower than blowfish. The mini version of blowfish is easily implementable on any 8 bit processor with a minimum of 24 bytes RAM and 1 KB RAM [9].

IV. SECURE ROUTING PROTOCOLS

There are many routing protocols specifically designed for users. They can be broadly classified into three categories: flat based routing, hierarchical routing and location based routing [16]. In flat based routing nearly all nodes are assigned equal roles or functions. In hierarchical based routing nodes play different roles according to hierarchy. In location based routing physical portions of the nodes are used to route data in the network. Even though there are many routing protocols as stated most of them lacks security services. Hence WSNs with conventional routing protocols are vulnerable to many types of attacks. Security is of prime importance in WSNs because nodes assume a large amount of trust among themselves during data aggregation and event detection. The data send from a large set of cluster nodes in a cluster to the head may be aggregated and only one final aggregated message may be send to the sink. So it is essential to ensure data security for communication links and data exchange. Most networks layer attacks against sensor networks fall into the below given categories:

- Spoofed or altered data
- Selective forwarding
- Sybil attack
- Sink hole
- Worm hole
- Hello flood attack

Routing protocols can be attacked by spoofing or altering the routing information exchanged between nodes. This can lead to errors in routing table or even partitioning the network. The Sybil attack [5] occurs when a single node presents itself as multiple entries to the network. This can affect the fault tolerance of the network and confuse the geographic routing algorithms. Encryption and authentication of a global key by a

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 4, October 2013

central key distribution centre can prevent these attacks initiated by an outsider. A selective forwarding attack is a method by which a node forwards only some messages it intends to. The message from a node to sink is passed through many intermediate nodes and if any node is not forwarding the message it affects the performance of the entire system. Sinkhole attack is by which a malfunctioning node presents itself to be a very favorable to the routing algorithm so that most data is routed through it. This node then performs selective forwarding or acts as a sink. The wormhole attack lures traffic through a very long path by giving false information to the nodes about their distances. Worm hole and sinkhole attacks are difficult to overcome because the routing information supplied the node is difficult to verify. In our WSN system the routing protocols is of geographic in nature and are not affected by these attacks. Hello flood attacks can be caused by a node broadcasting, a hello packet with very high power. A large number of nodes even at very far distances in the network choose this node as its parent. Then onwards all messages needs to be multi hopped to this node (parent) which increases the delay. This attack can be avoided by the node by checking the bi-directionality of the link. There by checking if the new parent is one hop away or not. Many protocols can be developed to improve the security of senior nodes. LEAP- Localized encryption and authentication protocol [7] is a key management protocol. For WSNs based on symmetric key algorithms. In a WSN if every pair of node is using a common key, then it is ideal for security. LEAP uses different keying mechanism for different packets depending on their security requirements. Directed diffusion is a flat based routing algorithm for WSNs [20]. In directed diffusion, sensors measure events and create gradients of information in their respective neighboring nodes. The base station request data by broadcasting interest which describes a task to be conducted by the network. This interest is diffused through the network hop by hop and broad casted to each node by its neighbors. Each sensor node sets up a gradient towards the sensor node from which it received the interest. This process is continued until gradients are send from the sources to the sink node. Directed diffusion is vulnerable to many kinds of attacks if authentication is not included in the protocol [31]. Geographic and Energy Aware Routing [GEAR][24] is a location based routing protocol. It requires location information to be exchanged between neighbors. This location information can be misrepresented by an intruder. There by the intruder can act as a path in the known flow. Then he can implement selective forwarding and Sybil attacks in the data flow. Security protocols for sensor networks (SPINs) [32] is suite of security protocols that are specially designed for highly resource constrained sensor networks. SPINs consists of two main blocks. Sensor Network Encryption Protocol (SNEP) and a micro revision of timed, efficient, streaming, loss-tolerance authentication protocol µTESLA. SNEP provides data authentication, protection from replay attacks and semantic security, all with low communication overheads of eight bytes per message provides data confidentiality, two party data authentication, and data freshness for peer-to-peer communication. µTESLA provides authenticated broadcast; i.e. nodes which receives a packet can be assured of its sender's identity it requires a loose time synchronization between BS and nodes, with an upper bound on maximum synchronization error. The MAC keys are derived from a chain of keys obtained by applying a one way function (F). All nodes have an initial key Ko, which is some key in the key chain. The relationship between keys proceed as K0 = F(K1), K1 = F(K2) and in general Ki = F(Ki+1) µ SPINS assumes that each node is pre-distributed with a master key K which is shared with the Base station at creation time. All other keys, including key Kener for encryption, key Kmac for MAC generation and a key K rand for random number generation, are derived from the master key using a strong one way function. SPINS uses RC5 for confidentiality. Logical Key Hierarchy for WSNs (LKHW) is an extension of directed diffusion. It provides robustness is routing and security and supports both backward and forward security for sensor joins and leave operations [28]. However it does not provide data authentication.

A. Energy Efficient Hierarchical Secure Routing Protocol (EEHSRP)

A new energy efficient hierarchy based data routing protocol (EEHSRP) which is secured enough was developed for the WSNs to be employed in the paddy field. The network routing is hierarchical is structured in which data is routed from sensor nodes to the sink through the cluster heads (CH). The sink is the base node and is assumed to have sufficient power for computation and large memory size. It can securely communicate with all sensor nodes through the cluster heads. The sensor nodes are deployed in the field randomly over an area to be monitored. They form the clusters and powerful node in the cluster is selected as the cluster head. The cluster head position is not rotated as the cluster head node is resource rich compared to other nodes in the cluster. As we discussed earlier there are three layers in the network : the lower level sensor nodes, the middle layer cluster heads (CHs) and the upper layer sink node. The functions performed by nodes in these layers are as follows.

Sensor Node (SN)

Fetch the data from the physical sensor column

Packetize this analog data after converting it into digital data

Encrypt the data packet using Blowfish algorithm

Send the data packet to the cluster head (CH)

Receives the control packets from the cluster heads

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 4, October 2013

(CH) nodes

Decrypt the control packet and update the session key.

Cluster Heads (CHs)

Receive data packets from its single hop sensor nodes(SN)

Aggregate the data packet after checking repeated data

Append logical time stamp

Packetize the data after appending its own CH ID

Route the packet to the sink

Receive session keys from the sink

Send control packet to all its cluster nodes (SNs)

Sink Node

Receive the data packets from the cluster head (CH)

Decrypt the packet

Check the authenticity and integrity of the packet

Check the time stamp of the packet with its own time stamp

Generate new session keys when current session expires

Encrypt the new session key with current session key and send to the cluster heads (CHs)

B EEHSR Protocol

Notations used:

$\mathbf{P_i}$ - *Data Packet*
$\mathbf{S_i}$ - *Sensor Node*
E( ) - *Encryption Function*
D( ) - *Decryption Function*
SK - *Session Key*
CH - *Cluster Head*
F( ) - *Pseudorandom Function*
$\mathbf{T_{CH}}$ - *Logical Timestamp of Cluster Head*
$\mathbf{T_{SN}}$ - *Logical Timestamp of Sink Node*
$\mathbf{SK_{new}}$ - *New Session Key*
$\mathbf{SK_{cur}}$ - *Current Session Key*
$\|$ - *Concatenation Operation*

Begin

1. **Sensor node sending packet (P_i) to Cluster Head ($S_i \rightarrow CH_i$)**

A sensor Node S_i collects the values from the physical sensors and coverts it into data packets P_i. It then encrypts this packet using the current session key SK and transmits this data to its cluster head CH_i.

$$\mathbf{E_{SK}\,(P_i)} \rightarrow \mathbf{G_i}$$

2. **Cluster Head to Cluster Head ($CH_i \rightarrow CH_j$)**

The cluster head concatenates the encrypted packet send by its members and the packets it received from other cluster heads. The logical timestamp $\mathbf{T_{CH}}$ (incremented by one) and its own ID is appended to this packet and transmits it to the next cluster head on the way to the sink node.

$$\mathbf{\{E_{SK}\,(P_i)\}} \,\|\, \mathbf{\{E_{SK}\,(P_j)\}} \,\|\, \ldots\ldots \|\, \mathbf{\{E_{SK}\,(P_n)\}} \,\|\, \mathbf{T_{CH}} \,\|\, \mathbf{CH_i\}}$$

$$\mathbf{\{\{[E_{SK}\,(P_x)\}} \,\|\, \mathbf{T_{CH}} \,\|\, \mathbf{CH_j]\}} \,\|\, \ldots\ldots \|\, \mathbf{\{[E_{SK}\,(P_y)\}} \,\|\, \mathbf{T_{CH}} \,\|\, \mathbf{CH_m]\}}$$

where $\mathbf{P_i}$, $\mathbf{P_j}$ *and* $\mathbf{P_n}$ *are packets from packets from sensor nodes* $\mathbf{S_i}$, $\mathbf{S_j}$, $\mathbf{S_n}$ *belonging to the cluster head* $\mathbf{CH_i}$. $\mathbf{[E_{SK}\,(P_x)\}} \,\|\, \mathbf{T_{CH}} \,\|\, \mathbf{CH_j\,]}$ *is the data packet received from cluster head* **CHj** *and* $\mathbf{[E_{SK}\,(P_y)\}} \,\|\, \mathbf{T_{CH}} \,\|\, \mathbf{CH_m]}$ *is the data packet received from cluster head* **CHj**

3. **Cluster Head to Sink Node ($CH_n \rightarrow SN$)**

The sink node receives the incoming packets from the cluster heads

$$\mathbf{\{\{E_{SK}\,(P_i)\}} \,\|\, \mathbf{\{E_{SK}\,(P_j)\}} \,\|\, \ldots\ldots \|\, \mathbf{\{E_{SK}\,(P_n)\}} \,\|\, \mathbf{T_{CH}} \,\|\, \mathbf{CH_i\}}$$

$$\mathbf{\{\{[E_{SK}\,(P_x)\}} \,\|\, \mathbf{T_{CH}} \,\|\, \mathbf{CH_j\,]\}} \,\|\, \ldots\ldots \|\, \mathbf{\{[E_{SK}\,(P_y)\}} \,\|\, \mathbf{T_{CH}} \,\|\, \mathbf{CH_m]\}}$$

Upon receiving the packet from a cluster head performs the following checking processes :

It checks the timestamp appended on each packet from the cluster head with its own timestamp. If $\mathbf{T_{CH}} \geq \mathbf{T_{SN}}$ then the timestamp is valid it accepts the packet, otherwise it sends a retransmission request to the respective cluster head.

It checks the Cluster Head ID appended on the packet with the IDs stored in the data base. If found valid it accepts the packet, or else it rejects.

if ($\mathbf{T_{CH}} < \mathbf{T_{SN}}$) **then** send retransmission request

else if (CHi member of **CH) then** Accept Packet

else Reject packet

endif

If the packet is found valid and is accepted then it decrypts the

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 4, October 2013

packets for obtaining the data from the sensor nodes for further processing.

$$D_{SK} (\{ \{E_{SK} (P_i)\} \| \{E_{SK} (P_j)\} \| ..... \| \{E_{SK} (P_n)\}$$

$$\| T_{CH} \| CH_i \} \{ \{ [E_{SK} (P_x)\} \| T_{CH} \| CH_j] \}$$

$$\| ..... \| \{ [E_{SK} (P_y)\} \| T_{CH} \| CH_m] \})$$

4. New Session key generation and transmission

On expiry of the current session the timestamp is incremented by one

$$T_{SN} = T_{SN} + 1$$

a new session key is generated using the pseudorandom function F( )

$SK_{new} = F (SK_{cur} , x)$ where x is a random number.

The sink node encrypts the new session key using the current session key and sends it to the cluster heads.

$$ESK_{cur} (SK_{new}) \rightarrow CH_s$$

The cluster heads broadcasts the new session key and the sensor nodes update the same.

End

V. SECURITY

A. Secure Communication

The communication is highly secures in our protocol because the data send from the nodes to the sink is encrypted using a sufficiently strong cryptographic Algorithm. The key used for encrypted and decryption is symmetric and is used only for a sensor. When the session is copied new key is generated and used. Changing the session key dynamically after each session there by making the eavesdrop attack on the network by an intruder nearly impossible.

B. Key freshness

As we are using a random function for generating the key at the sink node, it produces new session key at each session. So the key for each session is fresh.

C. Data freshness

We are appending a time stamp with cluster head after aggregating the data packets to be sent to the sink. Therefore the sink node can verify the time stamp in the incoming packet with its own time stamp and ensure the freshness of the data.

D. Integrity and origination

The cluster heads are adding its ID that is the CHID along with the packet send to the sink node. Therefore the sink node can understand the address of the cluster head from which the data packet originated and the cluster heads which subsequently forwarded the packet reaching the sink. Majority of the attacks possible in a WSN system are considered and precautionary measures were taken while developing the EEHSRP protocol. As we are using encryption and authentication measures while sending the data using a globally shared key the chances for altering the routing information is minimized. With this measure we can avoid spoofing, network partitioning and Sybil attacks [5]. Even though we are using a hierarchical method for routing, our cluster size, cluster head, and sensor nodes are stationery. The sensor nodes (SN) are only one hop away from the cluster head. The cluster nodes one fixed nodes, so location coordinate can be used for verifying the false distances provided by node which are attacked. Thus we can avoid worm hole and sink hole attacks. As our sensor nodes are one hop away from the cluster heads there is less change for Hello flood attacks.

VI. ENERGY-EFFICIENCY OF THE EEHSR PROTOCOL

A Static Cluster Heads

Most routing protocols employ cluster head selection and rotation process for equally draining the energy of the nodes. But the process of dynamically electing and changing the cluster heads is a time consuming, computationally strong and communication overhead process. Our cluster heads are resource rich nodes and can function as a cluster head for sufficiently longer period. Therefore the cluster head rotation is not required. This will eliminate the over heads of solution for other sensor nodes and they can perform their intended functions alone. Hence by using static cluster head concept we can reduce the energy consumption of the cluster.

B Single hop communication

In our project the transmission power of the sensor nodes are fine tuned to send a packet of data to the cluster head in a single hop. The sensor nodes are not intended to perform as intermediate nodes for forwarding the data packet. Only the cluster head node will accept the packet from the cluster sensor nodes. Therefore the sensor node only needs to listen to the packets broadcasted from the cluster head. As the data packets from the sensor nodes reach the cluster head in a single hop much energy can be saved.

VII. CONCLUSION

By automating many of the farming procedures and use of advanced machines, farming can be made more profitable, thereby attracting more persons into farming and increasing the production. This paper discussed some issues related to the security of the wireless sensor networks. Due to the unique characteristics of WSNs, they are vulnerable to security attacks compared to infrastructure based wireless networks.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 4, October 2013

The main objective of security services in WSNs is to protect the data and resources from attacks. Some mechanisms that can be adopted in our system were also discussed in his paper. Routing is another key area where security is essential. A secure routing protocol which ensures security and energy optimization is also discussed in this paper. The next step is to apply these techniques in the physical wireless sensor network already deployed in the field.

REFERENCES

[1] D. Song J. Newsome, E. Shi and A. Perrig. "The sybil attack in sensor networks analysis and defenses". In Proceedings of the third international symposium on Information processing in sensor networks.

[2] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: "Attacks and countermeasures". Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, 1(2-3):293{315, September 2003.

[3] H. Chan and A. Perrig. "Security and privacy in sensor networks". IEEE Computer Magazine, pages 103{105, 2003.

[4] Sanjay Burman. "Cryptography and security - future challenges and issues". Invited Talk, in proc. of ADCOM, 2007.

[5] J. Doucer, "The Sybil Attack", proceedings of IPTPS 2002, March 2002.

[6] 39, J. Deng, R. Han and S. Mishra, "INSENS: Intrusion Tolerant Routing in Wireless Sensor Networks", Poster presentation at IEEE ICDCS 2003.

[7] S. Zhu, S. Setia and S. Jojodia, "LEAP: Efficient Security Mechanism for Large-scale distributed Sensor Networks", Proceedings of ACM Conference on Computer and Communications Security 2003, Oct 2003.

[8] Bruce Schneier. "The blow¯sh encryption algorithm retrieved". http://www.schneier.com/blow¯sh.html, October 2008.

[9] A.A. Tamimi. "Performance analysis of data encryption algorithms".www.cs.wustl.edu, October 2008.

[10] J. Stankovic A. Perrig and D. Wagner. Security in wireless sensor networks.

[11] P.Nair H.Cam, S.Ozdemir and D. Muthuavinashiappan. Espda: "Energy efficient and secure pattern based data aggregation for wireless sensor networks". Computer communications IEEE Sensors, 29:446{455, 2006.

[12] N. El-Fishawy. "Quality of encryption measurement of bitmap images with rc6, mrc6, and rijndael block cipher algorithms". International Journal of Network Security, pages 241{251, November 2007.

[13] M.C. Wood, "Method of Cryptographically Transforming Electronic Digital Data from One Form to Another," U.S. Patent 5,003,596, 26 Mar 1991.

[14] T.W. Cusick and M.C. Wood, "The REDOC-II Cryptosystem," Advances in Cryptology--CRYPTO '90 Proceedings, Springer-Verlag, 1991, pp. 545-563.

[15] Jonathan Jen-Rong Chen Prasan Kumar Sahoo and Ping-Tai Sun. "Efficient security mechanisms for the distributed wireless sensor networks". Proceedings of the IEEE Third International Conference on Information Technology and Applications (ICITA'05), pages 0{7695{2316{1, 2005.

[16] J. N. Al-Karaki and A. E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey," IEEE Wireless Commun., vol.11, no. 6, Dec. 2004,

[17] J.L. Massey and X. Lai, "Device for Converting a Digital Block and the Use Thereof," International Patent PCT/CH91/00117, 16 May 1991.

[18] J.L. Massey and X. Lai, "Device for the Conversion of a Digital Block and Use of Same," U.S. Patent 5,214,703, 25 May 1993.

[19] B. Schneier, Applied Cryptography, John Wiley & Sons, New York, 1994.

[20] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks," MobiCom '00: Proc. 6th Annual Int'l. Conf. Mobile Computing and Networking, New York: ACM Press, 2000,

[21] Vijay Garg b M.S. Meitei c S. Raman c A. Kumar c N. Tewari R.K. Ghosh a. Ad hoc networks. pages 168{185, 2006.

[22] Wei Ding and et.al. Energy equivalence routing in wireless sensor networks.

[23] Sajid Hussain and Abdul W. Matin Jodrey. Energy efficient hierarchical cluster-based routing for wireless sensor networks. Technical Report - TR-2005-011, 2005. 073720m@acadiau.ca.

[24] Y. Yu, R. Govindan, and D. Estrin, "Geographical and Energy Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks," UCLA Computer Science Department, Tech. Rep. UCLA/CSD-TR-01-0023, May 2001.

[25] R.C. Merkle, "Fast Software Encryption Functions," Advances in Cryptology--CRYPTO '90 Proceedings, Springer-Verlag, 1991.

[26] R.C. Merkle, "Method and Apparatus for Data Encryption," U.S. Patent 5,003,597, 26 Mar 1991.

[27] X. Lai, J. Massey, and S. Murphy, "Markov Ciphers and Differential Cryptanalysis," Advances in Cryptology--EUROCRYPT '91 Proceedings, Springer-Verlag, 1991, pp. 17-38.

[28] R. D. Pietro et al., "LKHW: A Directed Diffusion-Based Secure Multicast Scheme for Wireless Sensor Networks," ICPPW '03: Proc. 32nd Int'l. Conf. Parallel Processing Wksps., IEEE Computer Society Press, 2003

[29] Samir Alan Price, Kristie Kosaka. A secure key management scheme for sensor networks. Proceedings of the Tenth Americas Conference on Information Systems, New York, 41, August 2004.

[30] Mustafa C Gaurav Jolly. A low-energy key management protocol for wireless sensor networks. Proceedings of the Eighth IEEE International Symposium on Computers and Communication (ISCC'03), pages 1530{1546, 2003.

[31] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. First IEEE Int'l. Wksp. Sensor Network Protocols and Applications May 2003.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 4, October 2013

[32] A. Perrig et al., "SPINS: Security Protocols for Sensor Networks,"Wireless Networks, vol. 8, no. 5, Sept. 2002

[33] J.L Smith, The Design of Lucifer, A Cryptographic Device for Data Communication, RC 3326, White Plains: IBM Research.

[34] M.J. Weiner, "Efficient DES Key Search," Advances in Cryptology--CRYPTO '93 Proceedings, Springer-Verlag, in preparation.

[35] Deamen, R. Govaerts, and J. Vandewalle, "Block Ciphers Based on Modular Arithmetic," Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography, Rome, Italy, 15-16 Feb 1993,

AUTHOR'S PROFILE

Santhosh Simon has been working as a Lecturer of Department of Computer Science at St.Thomas College of Engineering and Technology, Kerala, India and a research student of Cochin University of Science and Technology. He has acquired BTech and MTech degree in Computer Science. He has presented research papers in several National and International conferences. His research interests are in Artificial Intelligence, Sensor Networks and Robotics. Santhosh Simon is a Professional Member of ISTE and IEEE.

K Poulose Jacob Professor of Computer Science at Cochin University of Science and Technology since 1994, is currently Director of the School of Computer Science Studies there. A National Merit Scholar all through, Dr. Jacob has been teaching at the Cochin University since 1980. He has presented research papers in several International Conferences in Europe, USA, and other countries. Dr. K.Poulose Jacob is a Permanent Professional Member of the ACM and a Life Member of the CSI. His research interests are in Information Systems Engineering, Intelligent Architectures and Networks. Till now 5 candidates have obtained PhD degrees under his supervision. He has more than 70 research publications to his credit.