Abstract

Modern society consumes large amounts of fuel, and the petroleum industry is a crucial part of the infrastructure and maintenance of society in almost all countries. The petroleum industry is one of the world’s largest industries. An oil platform, offshore platform, or oil rig is a large structure with facilities to drill wells, to extract and process oil and natural gas, or to temporarily store product until it can be brought to shore for refining and marketing. In many cases, the platform contains facilities to house the workforce as well. To monitor disasters in rigs, wireless sensor networks are used with mobile sinks and key pre-distribution. Organizations operating in the oil and gas sector face enormous challenges in the field of security, so while working with Wireless sensor networks, authentication & secure communication is vital. Mobile Sinks are essential for wireless sensor network application because of the data loss due to failure of a single sink node or base station. For securing mobile sinks, a framework with key pre-distributions is a good choice, and it consists of key pools for mobile sink nodes to access the sensor network and for secure communication among the sensor nodes, mobile sink and base station. Symmetric and asymmetric encryptions are used for higher security. After monitoring the disasters, mobile sink informs base station and take necessary actions to overcome the situation.

1. INTRODUCTION

Wireless sensor Network consists of autonomous sensors which are spatially distributed, that also monitors physical or environmental conditions and pass their data cooperatively.
through a network to a main location. The commonly monitored parameters are temperature, humidity, pressure, wind direction, speed, illumination intensity, vibration intensity, pollutant levels, vital body functions etc. Sensor networks can be deployed for habitat monitoring, environmental monitoring including forest fire detection, air pollution and green house monitoring, industrial and consumer applications. They are extremely useful in military applications that demand high security for nuclear and chemical attack detection, battlefield surveillance and so on. Sensor networks can be deployed for habitat monitoring, environmental monitoring including forest fire detection, air pollution and green house monitoring, industrial and consumer applications. They are extremely useful in military applications that demand high security for nuclear and chemical attack detection, battlefield surveillance and so on.

Using wireless sensor networks data’s are transmitted in broadcast manner so security of data is very important during transmission. Wireless Sensor Networks are easily vulnerable to various security attacks. Security is critical for these networks deployed in hostile environments. Most sensor networks monitor their surroundings actively, and to tamper the network to get the data and deduce information other than the data monitored is very easy. The wireless communication employed by sensor networks facilitates eavesdropping and packet injection by an adversary. The combination of these factors demands for sensor networks at design time to ensure operation safety, secrecy of sensitive data, and privacy for people in sensor environments.

![Figure 1: Wireless sensor network with mobile sink](image)

The location of the personals working in the rig is uncertain. While occurring any disastrous events, it is very difficult for the Control station officers to locate the positions of the workers in the particular sites. It requires more time and effort. Portable device can be used to overcome these problems. These devices can be fixed in their helmet or jacket. The devices have also the facilities for measuring various parameters because they consist of sensors. They are Gas sensor, Temperature sensor, Heart beat sensor, Pressure sensor. These portables device sense various parameters (gas, temperature, pressure) continuously. And if the sensed value exceeds a reference value, it immediately activates the relay driver and produces an alarming sound. So it will be useful for the person to know about hazardous situation. Heart beat sensor, senses the
workers heart beat continuously. If the person loses his/her consciousness then this information is sensed by the sensor and it will be passed to the control room.

When base station is too far from the sensing field, transmitting the data over long distances using Multihop may further weaken the security. It requires more energy at nodes near the base station while forwarding data to base station, and thus reducing the lifetime of the network. Therefore, the better option in the operation of sensor network application is mobile sinks (MSs), including data collection in hazardous environments, localized reprogramming, oceanographic data collection, and military applications etc.

2. RELATED WORKS

Wired and wireless networks can be implemented using variety of security algorithms but they cannot be used in wireless sensor networks because of the limited energy, memory and computation capability. The basis of the secure communications and the fundamental security mechanism in wireless sensor network is Key management protocols. WSN mainly faces the problem of mobile sink replication attack. To overcome this problem, an existing mechanism is three tier security frameworks for authentication and pair wise key establishment, based on polynomial pool based key pre-distribution scheme. This technique is able to give network resilience to mobile sink replication attacks. Two separate polynomial pools are used, a mobile polynomial pool and a static polynomial pool. Polynomials from Mobile polynomial pools are used for authentication between mobile sinks & stationary access nodes. Polynomials from static mobile pools are used for authentication and key establishment between sensor nodes & Stationary Access nodes. Before deployment random subset of polynomial from mobile polynomial pool is selected for mobile sinks and stationary access node s are given a polynomial from mobile polynomial pool. Similarly, random subset of polynomial from static polynomial pool are selected for all the sensor nodes & stationary access nodes. To launch a mobile replication attack, attacker has to get at least a single polynomial from mobile polynomial pool to gain access to the network. To launch a stationary access node replication attack, attacker has to get at least a single polynomial from static polynomial pool to gain access to the network. The limitation of this scheme is it may introduce considerable communication overhead.

3 Problem Definitions And Algorithm

In wireless Sensor network Security & Privacy support is major concern The sensor nodes are normally deployed in harsh, & unattended remote areas, so wireless sensor networks are susceptible to various security attacks due to lack of tamper resistance, sensor node failures, limited processing capabilities and non-availability of human assistance. Secure ways for communicating data are not available for wireless communication. The user can enter to the network and collect data based on his interest by compromising sensor nodes, so the sensors must send the sensed data to the intermediary only by encrypting with symmetric encryption. The Symmetric encryption is preferred because the sensors have no or little intervention with users. Various authentication and key predistribution based
on symmetric schemes exists for sensor networks. To address the security issues, a general framework that permits the use of any pair wise key pre distribution scheme to make pair between sensor nodes and Mobile Sinks based on the RSA symmetric encryption algorithm is used. The proposed technique will substantially improve network resilience to mobile sink replication attacks compared to the single polynomial pool-based key pre distribution approach. Shortest path is selected during the process of making pair between the nodes for data transmission. Here this work consists of a smart phone as sensor, the minimum requirement for using a smart phone as sensor is it must have sensors to sense temperature, heat, pressure etc. For the connectivity between the sensor and the wireless network, IEEE 802.11ac is used because it is the common standard for wireless connectivity of the smart phones.

3.1 Algorithm
Preliminary communication between the sensor and mobile sinks for authentication requires heavy computation may degrade the performance of the system. The keys are pre-distributed between the sensors and mobile sinks [6]. To sign the message ‘M’ from sensor to mobile sink first compute the hash function h=hash (M), here h is implemented via cryptographic hash function MD5 . The key generation algorithm runs RSA to obtain the values of N, d and e. The key generation algorithm returns pk and sk, where pk=(N,e) and sk=(N,d),Signature generation is as follows
Sign N, d (M)

a) Y--> H (M)
return y^d mod N Verification process is as follows
Verify N, e (M, x) Y--> x^e mod
Y^1 -->H (M)
If (y = y^1 then return 1 else return 0), here (M, x) is the message signature pair.
The RSA algorithm is used for communication between the sensor and the mobile sink because it is one of the first practical public-key cryptosystems and is widely used for secure data transmission. Sensors have only minimum storage capacity and least human interventions so for authentication between the sensors and mobile sinks private key encryptions are more suitable. The main reason for choosing this algorithm is that the data required to be encrypted and decrypted will be of small size, so that it doesn’t degrade the performance speed and its overall performance is better than other asymmetric algorithms.
RSA requires least amount of storage space for encrypted files [7].
b) Authentication efficiency for communication between mobile sink and base station is critical. To provide secure communication asymmetric key encryptions are used. This work mainly consist of two encryption mechanism such as AES encryption mechanism and one time password creation using hash function for communication between the base station.
and mobile sink[8]. Figure shows the encryption mechanisms used during communication.

![Figure 2: Encryption mechanisms for communication](image)

### 4. IMPLEMENTATION AND PERFORMANCE EVALUATION

This work consists of three modules.

#### 4.1. Sensors

The sensor detects temperature, pressure, and light value continuously and sends data in an encrypted form while it crosses the threshold value to the mobile sinks. While detecting any events, the sensors immediately activates an alarm to alert workers and send notifications to coast guard systems. Base station must validate and authenticate each sensor before deployment. Sensor generates keys for communication and sends the sensed data along with the key to the mobile sink. Transmission is in broadcast manner. As smart phones are used as sensors, each worker may have smart phones and they can use their phone as sensors, which may also have connectivity with mobile sinks. An android application is created for setting the threshold value and locating the sensors. All the sensors are positioned in the rig. There are many smart phones accessible which will work as sensors even they are in flight mode. Satellite phones are other alternatives which can also be used as sensors. To track the location of sensors, GPS services are included with sensor module.

#### 4.2 Mobile Sinks

Coast guard Systems consists of dedicated systems with wireless connectivity which rotates around the rig in a boat on a committed path, acts as mobile sink which provides the communication link between sensor and control room. The coast guard systems must be authorized and approved by the control room authorities. Coast guard receives the encrypted data from the sensor and decrypts the message using the symmetric algorithm. It
can check the notifications from the sensors and inform the emergency notifications to the control room, by encrypting the data using asymmetric algorithm. For secure data transfer between the sensor and control room using wireless network communication, the mobile sink (coast guard) must use the symmetric and asymmetric algorithms. Mobile sink also have the GPS service to locate the sensor.

4.3 Base Stations
Control room system which monitors each and every operations as well as the status of off-shore and on-shore plant acts as the base station. It records all the details about the sensors and coast guard systems. It receives notification on any disaster detection and decrypts the encrypted message from the coast guard using asymmetric algorithm. They are responsible for taking necessary actions on notification from coast guards such as informing the rescue team and acknowledging the coast guard and the persons on the rig etc.

The proposed work consists of the following steps
   i.) Sensor compute private key and sends its data with its own ID to the Mobile sink.
   ii.) Mobile sink decrypt the message and send the message to base station using asymmetric algorithm.
   iii.) Base station decrypts the message, take necessary action for disaster recovery and also acknowledge the mobile sink.

Compared to other schemes, the proposed system is efficient and the system has the following advantages:
- it provides better performance and authenticity
- no leakage of data and secure data transmission
- Free from wireless attacks
- An intermediate is present between the two sensor nodes for providing data security
- There is no complexity in computation and memory usage
- Few number of computational steps that are automatic, so no need of manual computation

5. EXPERIMENTAL RESULT
This work results a secure communication between the sensor node, coast guard system and the control room. As the RSA encryption mechanism is used, it is more secure for communication between the coast guard system and the control room which require high protection. Symmetric encryption is used between the sensor node and the coast guard, so attacking becomes difficult with compromised nodes. The time occupied for data transmission and connection establishment is less compared to the existing system. This work detects disasters and makes alarm to notify the employees about the disasters and communicate with coast guard system. Coastguard system report control room about the emergency situation and control room taken necessary actions for rescue operation. As compared to existing system it has better performance.
5. CONCLUSION
Delivering the right information at the right time is very crucial in disaster management. In wireless sensor networks security and privacy support with minimum cost is a major concern. The smart phones and web technologies in disaster management should be seen as a new era in micro blogging during disasters to aid in identification of victims and survivor. It does not compromise the leakage of data.

6. REFERENCES