New Approach for Improving Security Measures of Private Key Algorithm in Wireless Sensor Network Environment

Priyanka Dudhatra¹ Asst. Prof. Rashmi Agrawal² Bhoomi Pipaliya³ Hardik Kothadiya⁴
¹, ³, ⁴ PG Student, ² Associate Professor
Electronics and Communication Department
¹, ² Atmiya Institute of Technology & Science, Rajkot, Gujarat, GTU
³, ⁴ R. K. College, Tramba, Rajkot, Gujarat, RKU

Abstract--- A wireless sensor network (WSN) is mainly made of distributed manually working sensors to monitor both physical and environmental conditions like temperature, sound, pressure, etc. and it collect the data from the all thee node and pass their data by the network to a main location. Nowadays many modern sensor networks are bi-directional, and it also control of sensor activity. Wireless sensor networks is mainly developed by the motivation of military applications like battlefield surveillance; today wireless sensor networks are mainly used in industrial and consumer applications like monitoring process of industry and health monitoring control industries and so on. So Many algorithms are already exits with many security limitations in wireless sensor network but with many limitation .For instance key maintenance is a great problem faced in less security level is a major problem of private key encryption methods ,even though key maintenance is hard ,So by improving the security of this algorithm we can solve this problem.

I. INTRODUCTION

Wireless Sensor Networks (WSN) are entering as an important measures in the IT ecosystem and a rich domain for research activity which includes hardware and system design, networking, data management, distributed algorithms, programming models, security and social factors [1], [2], [3]. The basic idea of wireless sensor network is to develop small sensing devices; which are able to do sensing some changes of communicating and incidents/parameters with many other devices, over a short or long specific geographic area for many specific purposes like surveillance, target tracking, environmental monitoring etc. Today’s sensors are capable for monitoring pressure, humidity ,temperature, soil makeup, noise levels, vehicular movement, lighting conditions, the presence or absence of certain kinds of objects or substances, mechanical stress levels on attached objects, and other properties [4]. In case of wireless sensor network, the communication is mainly among the sensors is done using transceivers. This kind of attractive features of the wireless sensor networks attracted many researchers to work on various issues related to these types of networks. However, while the wireless sensor network and routing strategies and modeling are getting much preference, the research in security issues are yet to discover more interest in focus. In this paper, we proposed the new algorithm for next generation wireless sensor networks and discuss the crucial parameters that require extensive investigations.

Wireless sensor networks are mainly the combinations of tiny sensors which communicate with each other with the use of wireless communication. Wireless sensor network are a distributed network which consist of resource and wireless devices called sensor nodes. Each sensor node is capable of monitoring some physical phenomenon (e.g., pressure, light, humidity, temperature) inside the area of deployment. The collected information from the entire node is sent to a base station. The communication range of wireless sensor nodes is limited to some specific meters and so all the sensor node cannot communicate with each other.

Some basic features of sensor networks are:
- They are Self-organization
- They Short-range broadcast communication and multi-hop routing
- They Do Dense deployment and cooperative sensors
- They Frequently changing topology, due to fading and node failures
- Limitations in computational resources, such as energy and memory [2].

II. WIRELESS SENSOR NETWORK (WSN)

Fig. 1: Architecture of sensor node

Wireless sensor networks (WSN) [2], [3], [9] allows to do monitoring and provide the security man-made and natural environments to great level of clarity and granulites. This macroscopically monitoring is possible by
and achieved by placing 100’s to 1000’s of tiny wireless sensor nodes or motes, in the target area for sensing fields and forces. For this, each and every sensor node contains sensors, limited data processing capabilities, information data and energy storage, and transceiver which is most probably wireless which allows to enabling them to form a network and work together. In order for deployment many sensors in mass the sensor nodes must be expendable and should also have the mobility, easy to deploy and use, inexpensive and maintain. These features of WSN make it very flexible and open for wide range of applications. Wireless sensor networks were started in the military with sensor nodes. The first reported deployments of small, pager sized nodes were [5] for air pollution monitoring and for environmental monitoring [6]. Military applications are also developed in wireless sensor network which includes target tracking, detecting radiation [7], and biological. Architecture of sensor node is as given below

III. STUDY OF SYMMETRIC KEY ALGORITHMS

There are many number of asymmetric algorithms but from all of them i have referred few of the basic algorithm like DES/3DES,AES,IDEA,RC5,RC6 and we will briefly discuss AES Algorithm as the proposed algorithm is the advance version of AES algorithm.

A. AES (Advance Encryption Standard)

This algorithm consists of four steps which are shown below.

1) Encryption Process
   - Substitute bytes
   - Shift rows
   - Mix Columns
   - Add Round Key

2) Decryption Process
   - Inverse Shift rows
   - Inverse Substitute bytes
   - Inverse Add Round Key
   - Inverse Mix Columns

B. Substitute bytes:-

In this step bytes are substituted from the S-box and then the new matrix would be created so that this step can be achieved which is shown in the below fig.

As shown in Fig 2. x,y would be loaded in the same way which is shown in fig and this how the substitute bytes will form a new matrix and output of it is given to next step which is shift rows

1) Shift Rows

This type is just the simple permutation which is done as described below.

- The first row of state is not altered.
- The second row is shifted 1 bytes to the left in a circular manner.
- The third row is shifted 2 bytes to the left in a circular manner.
- The fourth row is shifted 3 bytes to the left in a circular manner.

Fig. 3: Shift Rows

2) Mix Columns

It involves the mixing of column by multiplying the message matrix to constant matrix as shown in the below fig.

Fig. 4: Mix Column

As shown in fig the encryption is done in this way and decryption of the same is done in the same way so that is hard to break and here the computation cost decreases so that it the step where maximum energy is consumed.

3) Add Round Key

In this step there is XOR multiplication is done with key matrix so key is being XOR with the message matrix as shown in below figure.
Here k matrix is the text which needs to be encryption and w is the matrix of key which private of 32 bit which is being XOR at with k matrix and in this way the add key will occur and in the decryption process again the XOR will occur so that the original text can be obtained.
For 32-bit encryption this process is repeated ten times for 64-bit encryption it is repeated twelve times.

IV. PROPOSED ALGORITHM :- P-AES
This algorithm consists of four steps which are shown below.

A. Encryption Process
- Substitute bytes
- Shift rows
- Diagonal Inverse
- Add Round Key

B. Decryption Process
- Inverse Add Round Key
- Diagonal Inverse
- Inverse Shift rows
- Inverse Substitute bytes

In the proposed algorithm the three step will be working same as the original AES algorithm which is explained below the new step is Diagonal Inverse it will inverse the diagonal of the matrix which in there in fig. 3. Which will increase the security and complexity will be reduced.
Mix Column step is removed from the algorithm and new step Inverse Diagonal is introduced as mix column involves multiplication which increases the complexity of the algorithm and energy consumption is more in existing algorithm .So this new algorithm would help to improve the security and will decrease the complexity in WSN environment.

V. SUMMARY AND CONCLUSION
It has aimed in this paper to give a brief overview of recent and updated progress in wireless sensor network. At first, the working of sensor is described with sensor architecture and then all the security issue is described in detail with an example. Then we discussed the symmetric key algorithms from which AES algorithm is discuss in detail with each and every phase. Finally we proposed our own algorithm which will be implemented in future with increase in security and decrease in complexity of existing AES and will provide very rich algorithm to wireless sensor network.

ACKNOWLEDGEMENT
The authors would like to thank the Atmiya College and in Rajkot for the full support of this project. Special thanks to our guide Asst. Prof. Rashmi Agrawal for their guidance and supervision during out this research project at Atmiya College.

REFERENCES