Designing To Provide Reliability in Wireless Sensor Networks Using Cryptographic Techniques

R.Prabhakar Naidu[1], M.Padmavathamma [2]
[1]Associate Professor, Mother Theresa Institute of Computer Applications, Palamaner,
[2]Professor, Sri Venkateswara University, Tirupati,

ABSTRACT: ***Now a days, wireless device networks are very fashionable and become wide utilized in several applications. The wireless device networks are nothing but a combination of small devices known as sensor nodes. In wireless sensor networks, the sensor nodes are connected to sense and communicate the data to the base station. Wireless sensor networks are characterized by different things like number of energy resources, power consumption, computation capability, storage space and throughput .while passing the data from source to destination there is a possibility to loss the data because of attackers. During this process if we lose some data means, we did not get the exact data at the destination so automatically it raises the security issues. In order to overcome security attacks we use cryptography technique. symmetric cryptography technique takes more processing time when number of nodes increases for this reason we use asymmetric cryptography techniques(public key algorithms).In this paper we use two public key algorithms called salt encryption and salt encryption and divide data into blocks. Here we found out that salt encryption and divide data into blocks has more advantages when compared to salt encryption like high throughput, less computation time and it results to low power consumption and less storage space.***

Keywords: -Wireless Sensor Network, Security, Cryptography, salt encryption, salt encryption and divide data into blocks.

I.INTRODUCTION

In wireless sensor networks (WSNs), sensor nodes are connected with each other through wireless links. Sensor node is a basic component in WSNs .Each sensor node having some qualities like Sensor node is a smart, tiny, self organizing, low cost, and multi-functional device, equipped with battery, radio communication, microcontroller and sensor. It has very limited processing capability battery power, memory and also limited data sensing. A WSN may consist [1] of heterogeneous or homogenous nodes. Homogenous nodes are easily maintainable because of lesser complexity. Each node consists of a actuating unit, processing unit (CPU, micro controller or DSP kit), memory (for storing data), an RF transceiver (Omni-directional antenna) and power. Route maintenance and data communication are the two processes that consume energy in WSNs. Frequent network maintenance and node replacement isn't possible in WSNs due to the nature of the environment where they are deployed. Hence WSN must be fault tolerant. Multipath routing is an option to continue the networking in the presence of faults. But this requires more control overhead. A sensor [2] node is also called as mote. In a wireless sensor network, each node has capable to perform the processing, and gathering of the sensor information for communication with all other connected nodes in the network. Sensors are the hardware devices. They produce a proper response by some physical condition like pressure or temperature. Sensors are monitored by using a physical data parameter. Wireless sensor [3] networks contain so many characteristics like low cost, energy efficient, Computational power, Communication Capabilities, Security and Privacy, Self-organization and Small physical size.

Low cost: A wireless sensor network contains hundreds or thousands of sensor nodes to perform gathering the information and communicating with other nodes which are connected in the network. While using this much sensor nodes automatically the cost of network will be high so to reduce this cost we kept the cost of sensor node as low as possible.

Energy efficient: energy in WSN is used for different purpose like gathering the information, communicating with other nodes and storage. To perform, all these actions the sensor node can consume more power. If they run out of the power they often become invalid as we do not have any option to recharge. So, we take a bit care about the protocols and algorithm which are choosing in the design phase.

Security and Privacy: In WSNs, each sensor node should have some security mechanisms in order to prevent data access from unauthorized persons.

Self-organization: Each sensor node can have the capabilities like gathering the information and communicating with other nodes which are connected in the network. Each sensor node has to adjust them and form the network automatically.

Small physical size: sensor nodes are generally small in size with the restricted range. Due to its size its energy is limited which makes the communication capability low.

The main purpose [5] of WSN is to serve as an interface to real world, providing physical information such as temperature, light, radiation etc to a computer system.

Wireless sensor [4],[8],[7] network contains certain requirements such as confidentiality, integrity, availability, authenticity and quality of service.

Confidentiality: It prevents the information right to use from unauthorized user in a system.

Authentication: A secret authentication code is shared between the nodes that are communicating in a very network to realize secure data communication in a network; it provides security to data from source to destination.

Integrity: It prevents the information modification from unauthorized user in a system.

Availability: In WSNs contain certain services. in that some are fixed services and a few are on demanding services like node property is typically fixed service and a few time on demand service to supply such services at any time we use accessibility parameter.

Quality of Service: In a WSNs protection also deals with timely and accurate information packet delivery to avoid information loss.

Security is the major problem in wireless sensor networks. In order to achieve data security [4], [9] in WSNs mostly cryptographic techniques are used. Cryptography techniques are used to meet some basic requirements like confidentiality, integrity, availability, authenticity and quality of service.

Cryptography techniques are divided into 2 varieties symmetric cryptography and asymmetric cryptography. Symmetric secret writing is additionally named as secret-key cryptography. It uses one secret key for each secret writing and decryption. symmetric key techniques [6] are engaging due to their energy efficiency. Their basic arrange is that the secret keys are pre-distributed among sensors before their preparation. Their goal is to use quantity of memory to realize the best level of connectivity and additionally the best level of resilience. However, due to the limitation on memory, these techniques are not able to attain each a perfect property and a perfect resilience for large-scale sensor networks. Asymmetric secret writing is additionally referred to as public-key cryptography. It uses 2 keys public key and personal key .public key is used for encryption and personal key is used for decryption. The personal secret is never exposed. the utilization of Public-Key Cryptography (PKC) would eliminate the on top of drawback. because of its asymmetry property, sensors don't need to carry the pre-distributed keys. Any 2 sensors will establish a secure channel between themselves, and also the capture of some sensors won't have an effect on the protection of others. By taking above advantages, asymmetric cryptography techniques are more useful. Because of these advantages in existing paper also they used asymmetric cryptography technique called salt encryption. In existing technique, they used one algorithm called salt encryption. In salt encryption, we are encrypting the data to provide security. In that we encrypt the entire data at a time by using hash function. Here for encryption we are using one public key and for decryption we are using one private key. If any case the private key is exposed then we lose entire data. By using this algorithm throughput also less when compared to proposed technique. Throughput is less means automatically performance will be degraded. To avoid all these limitations we move to proposed technique called salt encryption and divide data into blocks.

II.RELATED WORK

"Analysis of Security Threats in Wireless sensing element Network" [10] This paper provides the protection schemes and additionally the threat attacks in wireless sensing element network. Security schemes like: Cryptography, Steganography and Physical layer Secure Access. Threat attacks like: Collisions, Tampering, Jamming, Unfairness, and Flooding etc. They additionally propose an answer for the attacks in wireless sensing element network. One attainable resolution is that the utilization of cryptography techniques.

"A Survey on Wireless sensing element Networks Security" [11] provides the layered style of wireless device network. These are fully totally different layer square measure different functions. the target of Network layer is to seek out best path for economical routing mechanism .In this layer are used leach protocol to avoid wasting the energy consumption (power of sensor) therefore on improve the period of sensors. LEACH provides cluster based transmission. The target of application layer is chargeable for data collection, management and method of the data through the appliance code for getting reliable results. During this layer are used SPINS (security protocol in device network) protocol are provides knowledge authentication.

"An Energy economical Reconfigurable Public Key Cryptography Processor ",[12] The ever increasing demand for security in transportable, energy unnatural environments that lack a coherent security design has resulted in the need to give energy efficient hardware that's rule agile. we demonstrate the practicability of utilizing domain-specific reconfigurable process for asymmetric cryptographical applications so as to satisfy these constraints. design is planned that's capable of implementing a full suite of finite field arithmetic over the integer's modulo-N, binary mathematician Fields, and non-super singular elliptic curves over GF (2n), with operands go in size from eight to 1024 bits. during this paper we use DSRCP, in this we estimate simulated performance of the DSRCP and energy potency of the DSRCP vs. standard solutions (FPGA & S/W).

"Wireless sensing element Networks: Security issues, Challenges and Solutions", [13] Security in Wireless sensing element Network is very important to the acceptance and use of sensing element networks. above all, Wireless sensing element Network product in business will not get acceptance unless there is a full proof security to the network. This paper summarizes the attacks and their classifications in wireless sensing element networks and additionally an endeavor has been created to explore the protection mechanism wide accustomed handle those attacks. The challenges of Wireless sensing element Networks are in short mentioned.

"Analyzing and modeling cryptography overhead for sensing element network nodes",[14] Recent analysis in sensing element networks has raised security issues for little embedded devices. Security concerns unit driven by the activity of an outsized variety of sensory devices at intervals the sector. Limitations in method power, battery life, communication bandwidth and memory constrain the connectedness of existing cryptography standards for tiny embedded devices. A pair between wide arithmetic for security (32 bit word operations) and embedded knowledge bus widths (often solely eight or sixteen bits) combined with lack of bound operations (e.g., multiply) at intervals the ISA present totally different challenges. This paper offers a pair of contributions. First, a survey investigation the procedure wants for kind of common cryptography algorithms and embedded architectures is given. the target of this work is to cover a good class of typically used cryptography algorithms and to figure out the impact of embedded architectures on their performance. This may facilitate designers predict a system's performance for cryptography tasks. Second, ways to derive the machine overhead of embedded architectures typically for cryptography algorithms are developed. This permits one to project machine limitations and ensure the threshold of possible cryptography schemes below a bunch of the constraints for an embedded design.

III.PROPOSED WORK

To avoid all the limitations in existing technique we move to proposed technique called salt encryption and divide data into blocks. In this proposed technique we are dividing the data into blocks and then encrypt the data with different blocks. In that for every block we are having one private key to decrypt the data i.e., each block contain different private keys. If any case one private key exposed then we loss only a small amount of data then automatically we say that security is more when compared to existing technique. In proposed technique the throughput is also high when compared to existing technique. By observing all these points we can say that performance is also high.

IV.ALGORITHMS

SALT ENCRYPTION

Salt (cryptography) in cryptography, a salt is random data that is used as an additional input to a one-way function that hashes data, a password or passphrase.

Step 1: Enter input message.

Step 2: Encrypt entire message at a time by using hash functions along with public key.

Step 3: Generate one private key.

Step 4: If we want to decrypt that encrypted message then we can decrypt that data by using hash function along with private key.

Step 4: Initialize starting time and ending time.

Step 5: Calculate throughput by using following formula.

$$\text{Throughput}=\frac{no.of\ bits\ recieved*8}{simulation\ time*1000}*100$$

Step 6: Display graph.

SALT ENCRYPTION AND DIVIDE DATA INTO BLOCKS

In this technique, we are applying salt encryption along with the data which is divided into blocks. Here, we are dividing the data or message into blocks based upon the message length. Once it is done then encryption of the each block takes place. After encryption the data is securely transferred to the destination via base station. At the destination side we can decrypt the message which is encrypted in the blocks by using hash function along with different private keys. At last the original can be seen to us by appending each block data which is decrypted. By this we are going to provide high security to the data as one cannot decrypt all blocks data.

Step 1: Enter input message.

Step 2: Divide entire data into blocks.

Step 3: Encrypt all the blocks by using hash functions along with public key.

Step 4: Generate one private key for each block.

Step 5: If we want to decrypt that encrypted message then we can decrypt all the blocks by using hash function along with different private keys.

Step 6: Append all the data from different blocks.

Step 7: Initialize starting time and ending time.

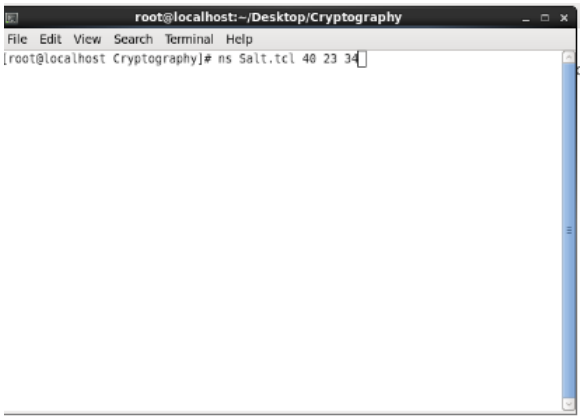
Step 8: Calculate throughput by using following formula.

$$\text{Throughput}=\frac{no.of\ bits\ recieved*8}{simulation\ time*1000}*100$$

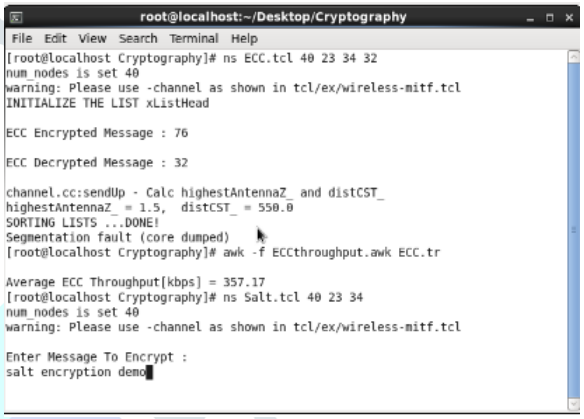
Step 9: Compare proposed throughput with existing throughput.

Step 10: Display graph.

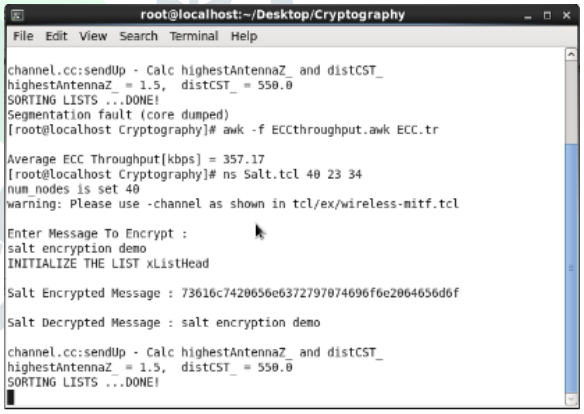
V.RESULTS NAD DISCUSSIONS



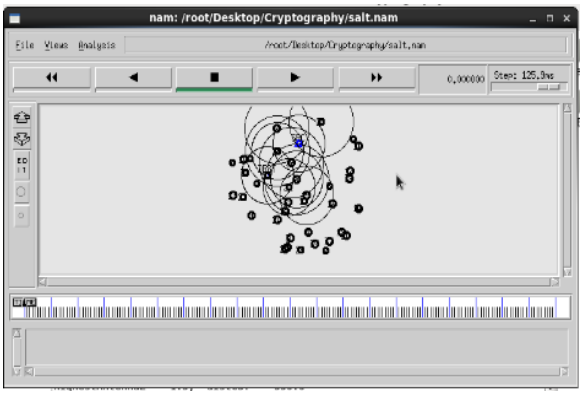
In above screen executing Salt encryption simulation. 40 is the total no of nodes and 23 is source and 34 is destination.

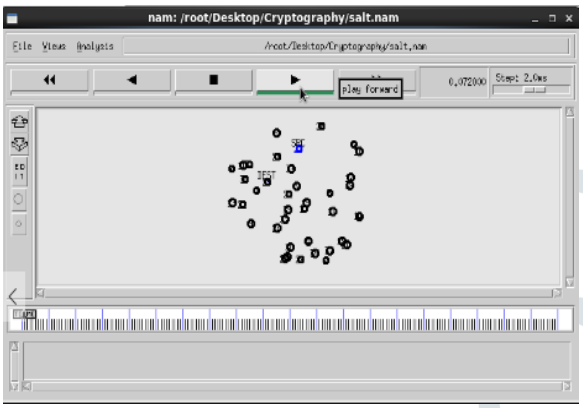


In above screen enter message to encrypt.



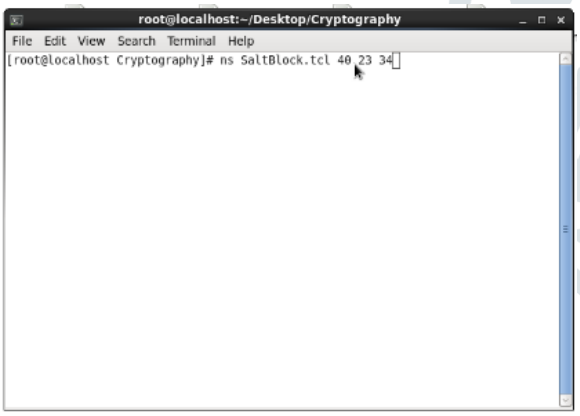
In above screen we can encrypt the message by using hash function and we can see the decrypted message also. Here encrypted data can be decrypted by using hash function along with one private key with salt technique.



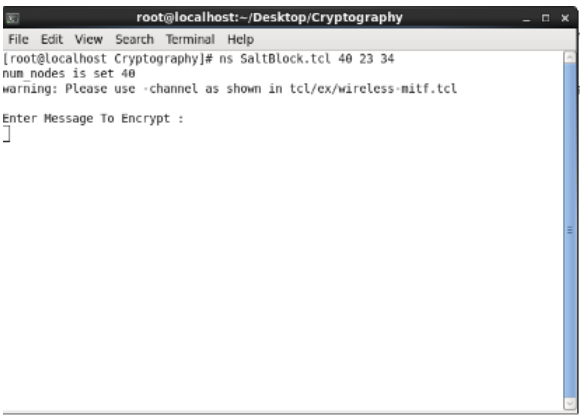


In above simulation screen we can see data transmission between source and destination.

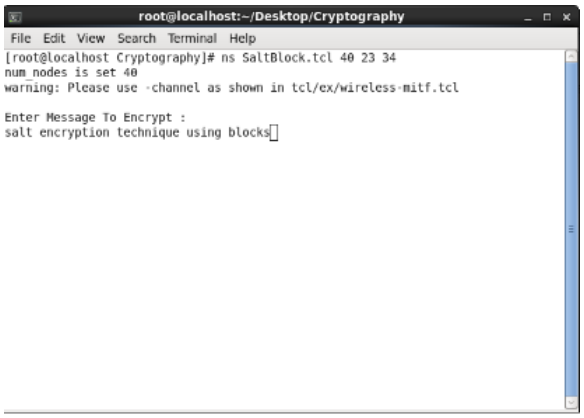
Now run Salt encryption by dividing message into blocks

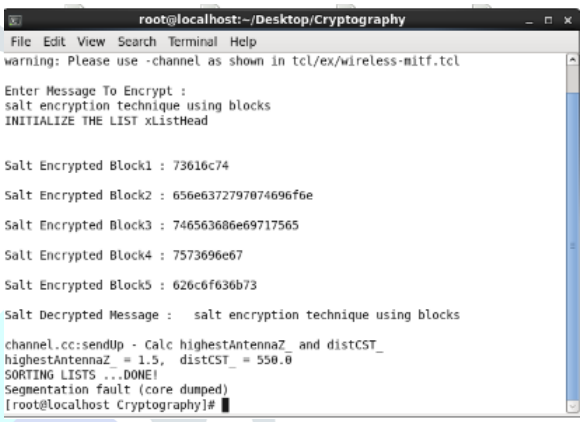


In above screen executing salt with block technique.40 is the total number of nodes, 23 is source and 34 is destination

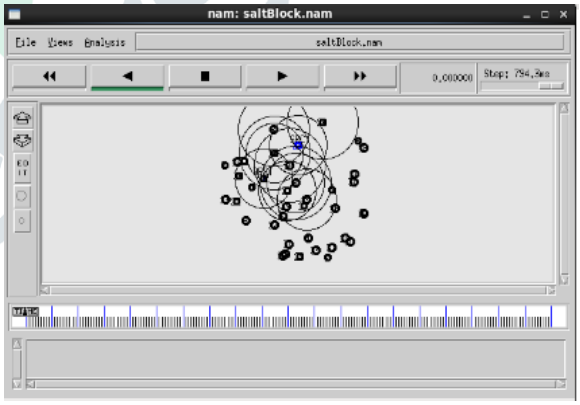


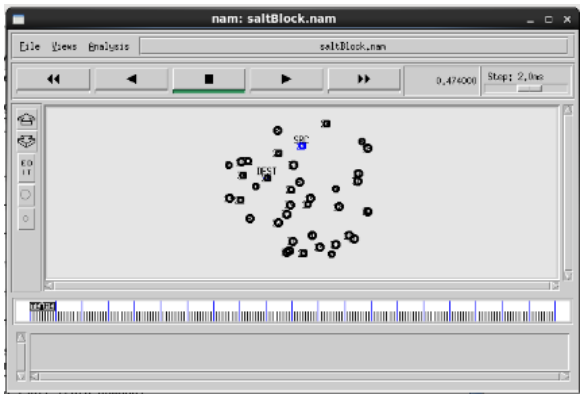
In above screen enter message to divide to blocks and then encrypt it





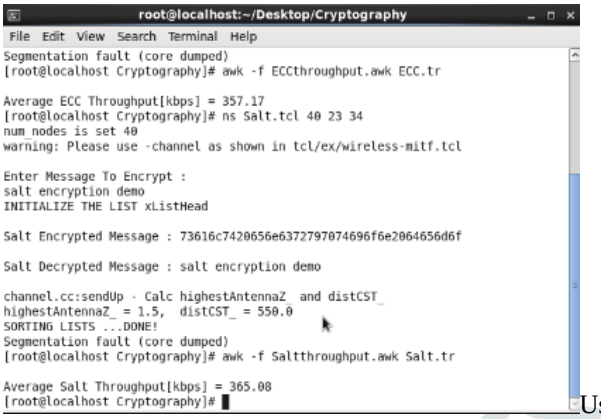
In above screen we can encrypt the data blocks by using hash function and we can see the decrypted message also. Here encrypted data can be decrypted by using hash function along with different private key .at last we append entire data.





In above simulation screen we can see data transmission between source and destination.

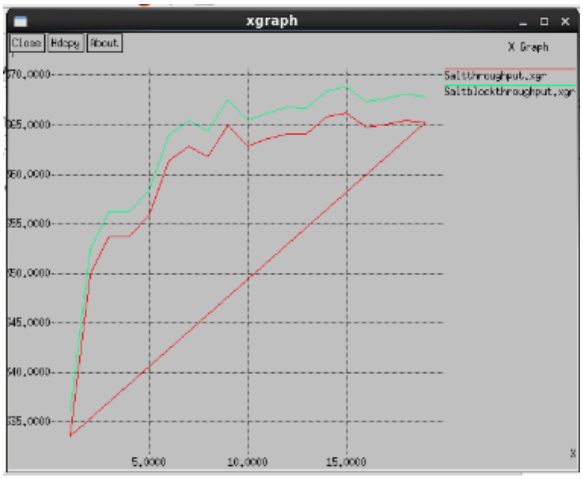
Throughput graph for salt encryption and salt encryption and data into blocks.



Use above screen command to calculate salt throughput

Use above screen command to calculate salt block throughput

Throughput graphs



In above graph x-axis represents time and y-axis represents throughput at that time. In above graph red line is for salt encryption and green line is for salt encryption and divide data into blocks.

CONCLUSION

The wireless sensor networks still grow and become wide utilized in several applications. So, we need a lot of security. However, the wireless sensor network suffers from several constraints like limited energy, process capability, and storage capability, etc. There are several ways to produce security; one amongst the attainable ways is cryptography. Choosing the correct cryptography technique place a significant to produce security in WSNs. Public Key primarily based} cryptographic schemes are used take away the drawbacks of symmetric based approaches. In this we paper we are comparing salt encryption and divide data into blocks with salt encryption. In that we found salt encryption and divide data into blocks gives more advantages when compared to salt encryption due to high throughput, low storage space, low power consumption and shorter key length compared to salt encryption.

REFERENCES

[1]. K.Akkaya and M.Younis,A survey on routing protocols for wireless sensor networks,Ad Hoc Networks,3(2005),325-349.

[2] Muhammad R Ahmed , Xu Huang ,Dharmandra Sharma,and Hongyan Cui.,"wireless-sensor networkcharacteristics-and-architectures", International Journal of Information and Communication Engineering Vol:6, No:12, 2012.

[3]. Dr.Khaled M.elleithy, Dema aldhobaiban.," Characteristics of Wireless Sensor Nodes and Prevention of Wormhole Attacks",may 2014.

[4]."Secure Data Transmission using Cryptography Techniques in Wireless Sensor Networks:A Survey", Vol 9 (47) December 2016.

[5] Yashaswini R, Nayana HG, Bindu AThomas,"Wireless Sensor Network Security using Cryptography", International Journal of Advanced Research in Computer Science & Technology Vol. 4 (Apr. - Jun. 2016).

[6]. Ning P, Wang R and Du W (2005), ―An efficient scheme for authenticating public keys in sensor networks‖,Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, Chicago, IL,USA, pp. 58-67.

[7]. Sonia , Kusum Dalal," Security Enhancement in WSN Networks usingCryptography Techniques",2016.

[8]."Security in Wireless Sensor Networks using CryptographicTechniques", American Journal of Engineering Research Volume-03(2014).

[9]. "A Survey on Security in Wireless Sensor Networks Using Cryptography", International Journal of Advanced Research in Computer Science Volume 7, No. 2, March-April 2016.

[10].SahabulAlam .et al ., "Analysis Of Security Threats In Wireless Sensor Network", International Journal of Wireless &Mobile Networks (IJWMN) Vol. 6, No. 2, April 2014.

[11]. AbhishekPandey. et al., "A Survey on Wireless Sensor Networks Security", International Journal of computer Application (0975-8887) Volume 3-No.2,June 2010.

[12]. Goodman J and Chandrakasan P (2001), ―An Energy Efficient Reconfigurable Public Key Cryptography Processor ‖, IEEE journal of solid state circuits, pp. 1808-1820, November 2001.

[13]. [6]Vikash Kumar1.et al., " Wireless Sensor Networks: Security Issues, Challenges and Solutions", International Journal of Information & Computation Technology,ISSN 0974-2239 Volume 4, Number 8 (2014).

[14]. Ganesan P, Venugopalan R, Peddabachagari P, Dean A, Mueller F and Sichitiu M (2003), ―Analyzing and modelling encryption overhead for sensor network nodes ", In Proceeding of the Ist ACM international workshop on Wireless sensor networks and application, San Diego, California, USA, September 2003

.

AUTHOR PROFILE

R.Prabhakar Naidu is a research scholar (Ph.D.) in Computer security and Privacy from Dravidian University, Kuppam . He has finished his MCA from University of madras in 2003, He is currently HOD & Associate Professor in Mother Theresa Institute of Computer Applications-Palamaner with total experience of 14 years in Computer Science. His areas of interest are Computer Security, Operating Systems and Software Engineering.

Prof M.Padmavathamma, Holds Doctorate in Mathematics from Sri Venkateswara University. M.Phil. and M.Sc. in Mathematics from Sri Venkateswara University. Due with respect from her publications currently she works as a Professor and BOS- Chair person in Department of Computer Science in Sri Venkateswara University ,Tirupatii with a total of 25 + years of experience. Her areas of Interest are Operations Research, Business Mathematics and statistics, Differential