ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 7, October 2015

Achieving Secure Communication in Wireless Sensor Networks using MES (Ver – I) Standard

A.Praveena

Assistant Professor, Dept. of I.T., Dr. N.G.P Institute of Technology, Coimbatore, Tamil Nadu, India

ABSTRACT: Once considered a playground for hackers and malicious attacks, wireless networks are fast becoming more secure than their wired counterparts. Developments in micro electro mechanical systems (MEMS) and wireless networks are opening a new domain in networking history. Recent technological advances in wireless networking, IC fabrication and sensor technology have lead to the emergence of millimetre scale devices that collectively form a Wireless Sensor Network (WSN) and are radically changing the way in which we sense, process and transport signals of interest. They are increasingly become viable solutions to many challenging problems and will successively be deployed in many areas in the future such as in environmental monitoring, business, and military applications. The huge challenge in WSN is due to inherent resource and computing constraints.

However, deploying new technology, without security in mind has often proved to be unreasonably dangerous. There have been significant contributions to overcome many weaknesses in sensor networks like coverage problems, lack in power and making best use of limited network bandwidth, however; work in sensor network security is still in its infancy stage. The problem of securing these networks emerges more and more as a hot topic. Symmetric key cryptography is commonly seen as infeasible and public key cryptography has its own key distribution problem. In contrast to this prejudice, this paper presents a new symmetric encryption standard algorithm which is the amalgamation of two different encryption algorithms proposed by Nath et. Al namely TTJSA and DJSA algorithms in randomized method. The algorithm is named as Modern Encryption Standard version – I algorithm. The idea of modern encryption standard is to make a symmetric key cryptographic method which should be unbreakable. The MES version –I algorithm is effective against frequency analysis and spectral analysis. Further improvements can be bit level encryption can be performed on the text files after dividing the plaintext into two text files.

KEYWORDS: Wireless Sensor Networks, Cryptography, Energy Efficient, Modern Encryption Standard

I. INTRODUCTION

In recent digital communication era, sharing of information is increasing significantly. The information being transmitted is vulnerable to various attacks. Therefore, the information security is one of the most challenging aspects of communication in any modern network. This also applies to Wireless Sensor Networks (WSNs), especially those used in applications that monitor sensitive information (e.g., health care applications). These networks are quickly gaining popularity due to the fact that they are potentially low cost solutions to a variety of real world challenges and are expected to play an essential role in the upcoming age of pervasive computing. However, the highly constrained nature of sensors imposes a difficult challenge: their reduced availability of memory, processing power and energy hinders the deployment of many modern cryptographic algorithms considered secure. For this reason, the choice of the most memory-, processing- and energy-efficient security solutions is of vital importance in WSNs. To date, several authors have developed extensive analyses comparing different encryption algorithms WSNs can be seen as a special type of ad-hoc network composed by a large number of tiny, cheap and highly resource constrained sensor nodes, known as motes. The sensors are distributed in the area of interest, and can then gather and process data from the environment (e.g., mechanical, thermal, biological, chemical, and optical readings). They have applications in a variety of fields such as environment monitoring which involves monitoring air, soil and water, condition based maintenance, habitat monitoring seismic detection, military surveillance, inventory tracking, smart spaces and gathering sensing

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 7, October 2015

information in inhospitable locations, medical and home security to machine diagnosis, chemical/biological detection etc. Motes are typically battery-powered, which has motivated considerable research efforts on the development of energy aware protocols, such as data link layer protocols. On the other hand, security is often very sadly considered at the very last step in the design of WSNs. Actually, most WSN deployments do not even consider security among their requirements because the execution and energy overheads it adds to the system is seen as an undesirable "extra cost" in such constrained environments. However, in WSN-based applications that monitor sensitive information, it is essential to prevent eavesdropping, which is typically obtained by means of encryption algorithms (e.g., symmetric ciphers). Even when the information acquired is not confidential, it is still necessary to ensure data integrity and authenticity by means of message authentication mechanisms, since the acceptance of invalid data (generated either by natural causes or with malicious purposes) could lead to mistaken actions and severe consequences. Finally, given that such algorithms depend on the existence of secret keys for their functioning, applications need also to handle these keys' distribution.

From national defence, medical applications, to the environment, the data delivered from the sensor networks are unstructured, using their own format and protocols. Sensor networks are delivering near-real-time information to scientists worldwide. Extracting this information to gain knowledge and understanding is one of greatest challenges.
These networks are an important ingredient of "anywhere and anytime" ubiquitous wireless next generation communication infrastructure. WSN is a combination of nodes that are used to sense data from its environment and to send the aggregated data to its control node often called sink. In this diversified yet integrated future network environments, sensor network has a role of reliable monitoring and control of variety of applications based on environmental sensing.

WSN facilitate monitoring and controlling of physical environments from remote locations with better accuracy. In spite, they pose a number of unique technical challenges due to the following factors: Adhoc deployment, unattended operation, untethered, and dynamic changes. In this paper for achieving security the author have used a new encryption algorithm called Modern Encryption Algorithm version – I (MES ver – I) which is an amalgamation of two different algorithms proposed by Nath et.al namely TTJSA and DJSA in randomized fashion for achieving better security.

A. *Contributions of the paper:*
This paper is intended to be an introduction to wireless sensor networks—with an emphasis on structural and environmental monitoring applications. A thorough but general survey of the area and referring to several papers in the computer science and engineering literature detailed information were given. In this paper for achieving security the author have used a new encryption algorithm called Modern Encryption Algorithm version – I (MES ver – I). The method is achieved by splitting the file, which is to be encrypted, and encrypting the split sections of the file in various ways using TTJSA and DJSA cipher methods. The primary idea behind the implementation of the algorithm is to build a strong encryption method, which should be unbreakable by any kind of brute force methods or differential attack.

The rest of the paper is described as follows. Section 2 discusses the background information for the architecture of WSN and components of a sensor node. The motivation for the proposed scheme presented is discussed in Section 3. Section 4 discusses the related work. Section 5 discusses the limitations with the previous work. Section 6 discusses the proposed scheme. Conclusions and future work conclude the paper.

II. SENSOR NETWORK ARCHITECTURE

A typical architecture of WSN is shown in the figure 1. The sensor nodes are usually scattered in a sensor field. Each of these scattered sensor nodes has the capabilities to collect data and perform partial or no processing on the data. Each sensor node has the required infrastructure to communicate with the other nodes. Data are routed back tot the sink/base station by a multihop infrastructure less architecture through the sink. A distinguished special type of node is called as gateway node. Gateway nodes are connected to components outside of the sensor network through long range communication (such as cables or satellite links), and all communication with users of the sensor network goes through the gateway node.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 7, October 2015

The sink node communicates with the task manager via core network which can be Internet or Satellite. Since Sensors are low cost, low power, and small in size, the transmission power of a sensor is limited. The data transmitted by a node in the field may pass through multiple hops before reaching the sink. Many route discovery protocols (mostly inherited from Ad hoc networks) have been suggested for maintaining routes from field sensors to the sink(s). Due to low memory, scarcity of available bandwidth and low power of the sensors, many researchers considered these separate route discovery mechanisms undesirable. Once sensors are deployed they remain unattended, hence all operations e.g. topology management, data management etc. should be automatic and should not require external assistance. In order to increase the network life time, the communication protocols need to be optimized for energy consumption. It means a node must be presented lowest possible data traffic to process.

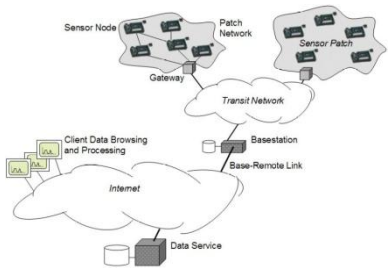

Fig.1.Sensor Network Architecture

The figure 2 shows the components of a sensor node. A sensor node is made up of four basic components: a sensing unit, a processing unit, a transceiver unit and a power unit. They may also have additional application-dependent components such as a location finding system, power generator and mobilizer. Sensing units are usually composed of two subunits: sensors and analog to digital converter. The analog signals produced by the sensors based on the observed phenomenon are converted to digital signals by the ADC, and then fed to the processing unit. The processing unit is generally associated with a small range a small storage unit, manages the procedures that make the sensor node collaborate with the other nodes to carry out the assigned sensing tasks. A transceiver unit connects the node to the network. One of the most important components of the sensor network is the power unit. Power unit may be supported by power scavenging units such as solar cells. There are also other subunits that are application dependent.

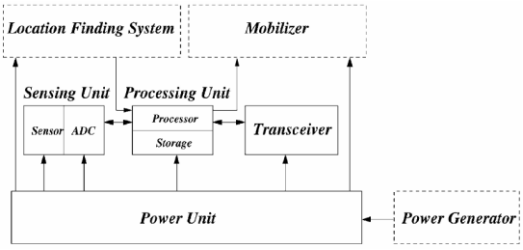

Fig.2.Components of a Sensor Node

The emergence of sensor networks as one of the dominant technology trends in the coming decades has posed numerous unique challenges to researchers. These networks are likely to be composed of hundreds, and potentially thousands of tiny sensor nodes, functioning autonomously, and in many cases, without access to renewable energy resources. Cost constraints and the need for ubiquitous, invisible deployments will result in small sized, resource-constrained sensor nodes. Such sensor nodes have resource constraints as: communication, power consumption, computation, uncertainty in sensor readings etc. While the set of challenges in sensor networks are diverse, we focus on security challenges in this paper.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 7, October 2015

III. SECURITY ISSUES IN WIRELESS SENSOR NETWORKS

Because the sensor nodes are battery powered, increasing the autonomous lifetime of a WSN is a challenging optimization problem. Communication of data within a WSN is one of the most energy-expensive tasks a node undertakes – using data compression to reduce the number of bits sent reduces energy expended for communication. Data compression which highly reduces the communication overhead by aggregating and compressing data packets can be performed at intermediate sensor nodes. However, compression requires computation, which also expends energy. Apart from achieving energy efficiency many WSN applications that span military and civilian use assume that the sensor nodes will be deployed hostile environments and thus be prone to a wide variety of malicious attacks. As a result, security becomes a key concern. Sensor networks are particularly vulnerable to several key types of attacks, such as denial of service attacks, traffic analysis, privacy violation, physical attacks, node take overs, attacks on routing protocols, etc.

The data transported and exchanged between sensor nodes is critical. Such data has to be protected against threats in a way so classic security properties like integrity, authenticity or confidentiality can be guaranteed[12].To accomplish such security goals in modern networks like the Internet or companies local area network cryptographic primitives like encryption / decryption as well as signature schemes are usually needed. Keys for encryption purposes must be agreed upon by communicating nodes. Due to resource constraints, achieving such key agreement in wireless sensor networks is non-trivial. Many key agreement schemes used in general networks, such as Diffie-Hellman and public-key based schemes, are not suitable for wireless sensor networks. Pre-distribution of secret keys for all pairs of nodes is not viable due to the large amount of memory used when the network size is large.

The lack of a fixed infrastructure and the ad hoc nature of WSN deployments suggest that the ability to encrypt and decrypt confidential data among arbitrary sensor nodes while enabling undisputed authentication of all parties will be a fundamental prerequisite for achieving security. To do this, nodes must be able to establish a secret key and know who their counterparts are. Thus, it becomes highly desirable to have a secure and efficient distribution mechanism that allows simple key generation for large-scale sensor networks while facilitating all the necessary authentications.

Although a variety of key-generation methods have been developed, they cannot be directly applied to sensor network environments due to the problems such as very limited resources (memory, power), unreliable communication (unreliable transfer, conflicts, latency), Unattended Operation (Exposure to Physical Attacks, Managed Remotely, No Central Management Point) etc. Due to these constraints it is difficult to directly employ the existing security approaches to the area of wireless sensor networks.

IV. RELATED WORK

Because of the problems mentioned in previous section security is commonly considered as a delicate problem. One security aspect that receives a great deal of attention in WSN is the area of key management. The two possibilities for achieving security are to use symmetric cryptography and public key cryptography. Two of the major techniques used to implement public-key cryptosystems are RSA and elliptic curve cryptography (ECC).

But most security work on WSN focuses on the search for and development of alternatives to classical public-key algorithms and public key infrastructures. Recent work has challenged notion that Diffie-Hellman and public key based schemes are infeasible in WSNs. Recently; however, several groups have successfully implemented public-key cryptography (to varying degrees) in WSN. ECC has thus emerged as a suitable public key cryptographic foundation that provides high security for relatively small key sizes. In [1] Gura et al. report that both RSA and elliptic curve cryptography are possible using 8-bit CPUs with ECC demonstrating a performance advantage over RSA. Another advantage is that ECC's 160-bit keys result in shorter messages during transmission compared the 1024 bit RSA keys. In particular Gura et al. demonstrate that point multiplication operations in ECC are an order of magnitude faster than private-key operations within RSA, and are comparable on the RSA public-key operation [1].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 7, October 2015

In [3], Watro et al. show that portions of the RSA cryptosystem can be successfully applied to actual wireless sensors, specifically the UC Berkeley MICA2 motes [2]. In particular, they implemented the public operations on the sensors themselves while offloading the private operations to devices better suited for the larger computational tasks. Shamir proposed the idea of identity-based cryptography in 1984, and described an identity-based signature scheme in the same article. However, practical Identity-based encryption (IBE) schemes were not found until recently with the work of Boneh and Franklin [5,6] and Cocks [8] in 2001. Cocks's scheme is based on the Quadratic Residuosity Problem, and although encryption and decryption are reasonably fast (about the speed of RSA), there is significant message expansion, i.e., the bit-length of the ciphertext is many times the bit-length of the plaintext. The Boneh-Franklin scheme bases its security on the Bilinear Diffie-Hellman Problem, and is quite fast and efficient when using Weil or Tate pairings on super singular elliptic curves or abelian varieties. ID-based encryption has some disadvantages as key escrow problem. The problem of obtaining authentic public keys has been replaced by the problem of obtaining authentic public parameters of PKGs. Review of security issues and various attacks in WSN is discussed [15].

V. LIMITATIONS WITH PREVIOUS WORK

Symmetric cryptography, which is computationally inexpensive, can be used to achieve some of these security goals. One major drawback with this approach is the key exchange problem i.e. the two communication nodes must somehow know the shared key before they can communicate securely.

So the problem that arises is how to ensure that the shared key is indeed shared between the two hosts who wish to communicate and no other rogue hosts who may wish to eavesdrop. How to distribute a shared key securely to communicating hosts is a non-trivial problem since pre-distributing the keys is not always feasible. Unfortunately, capturing even a single node, in the network would easily reveal the network's secret key. So it is inflexible with respect to key management, as it requires pre-distribution of keys. On the other hand, public key cryptography allows for flexible key management, but requires a significant amount of computation.

The main difficulty today in developing secure systems based on public key cryptography is not the problem of choosing appropriately secure algorithms or implementing those algorithms. Rather, it is the deployment and management of infrastructures to support the authenticity of cryptographic keys: there is a need to provide an assurance to the user about the relationship between a public key and the identity of the holder of the corresponding private key. In a traditional PKI, this assurance is delivered in the form of certificate, essentially a signature by a Certification Authority (CA) on a public key [1].The issues associated with certificate management, including revocation, storage and distribution and the computational cost of certificate verification.

In 1984, Shamir proposed a concept of Identity-based cryptography where users' identifier information such as email or IP addresses instead of digital certificates can be used as public key for encryption or signature verification. It reduces the system complexity and cost for establishing, managing the public key authentication framework known as Public Key Infrastructure (PKI). In IBE schemes private key generator (PKG) is responsible for generating private keys for all users, and it is a performance bottleneck for organizations with large number of users.

VI. PROPOSED WORK

The cryptographic method suggested in this paper is a type of symmetric key encryptions standard algorithm developed by Nath et al. namely TTJSA and DJSA in randomized method. The algorithm is named as Modern Encryption Standard version-I (MES ver-I). Below, we discuss the notion of MES ver-I.

A. *Encryption Algorithm:*

MES ver-I is essentially the combination of existing encryption methods developed by Nath et al. Two independent methods are involved (i) DJSA which is the extended version of MSA and (ii) TTJSA which is again a combination of three independent methods such as NJJSAA, MSA and generalized modified Vernam Cipher method.
Step 1: Split the plaintext file testdata.tt into two files t1.txt and t2.txt.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 7, October 2015

Step 2: Encrypt t1.txt using TTJSA method and generate t11.txt. Encrypt t2.txt using TTJSA method and generate t21.txt. Encrypt t21.txt using TTJSA method and generate t2e.txt
Step 3: Combine t2e.txt and t11.txt, generate t12e.txt and encrypt the file using DJSA method and generate t12e1.txt
Step 4: Split t12e1.txt into two files as t12e11.txt and t12e12.txt.
Step 5: Encrypt t12e11.txt using TTJSA, generate t12n1.txt and Encrypt t12e12.txt using TTJSA, generate t122n2.txt.
Step 6: Combine t12n1.txt & t122n2.txt, generate t12ne.txt file. Encrypt t12ne.txt file by DJSA, generate t12nee.txt file
Step 7: Encrypt t12nee.txt file using TTJSA method and generate t12nef.txt file. This will be final encrypted file.

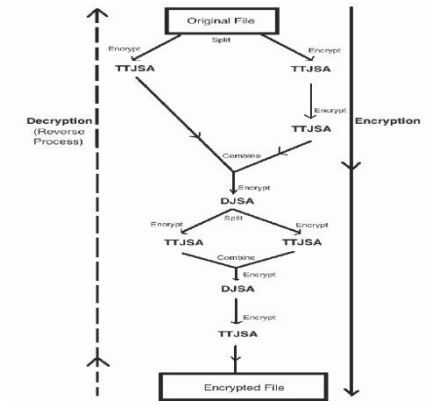

Fig.3.Block Diagram of Proposes MES ver-I algorithm

B. *Decryption Algorithm:*
Step 1: Decrypt t12nef.txt file using TTJSA, generate t12.txt file. Decrypt t12.txt DJSA method and generate t12d.txt.
Step 2: Split t12d.txt into two files as t122.txt and t121.txt. Decrypt t122.txt using TTJSA method and generate t12d.txt file. Decrypt t121.txt file using TTJSA method and generate t11d.txt file.
Step 3: Combine t11d.txt and t12d.txt, generate t1_2.txt file. Decrypt t1_2.txt using DJSA, generate t1_2d.txt file.
Step 4: Split t1_2d.txt file into two files as t2d.txt and t1d.txt files. Decrypt t2d.txt using TTJSA method and generate t2d1.txt file. Decrypt t2d1.txt using TTJSA method and generate t2df.txt file.
Step 5: Decrypt t1d.txt using TTJSA method and generate t1df.txt file. Combine t1df.txt and t2df.txt and generate t12f.txt file. This is the final decrypted file and it will be same as testdata.txt file. All the steps of encryption and decryption algorithms are listed as block diagram.

VII. SECURITY ANALYSIS OF MES VERSION – I

One of the classical cryptanalysis method used is by detecting the frequency of characters in the encrypted text message. To test the effectiveness of MES ver-I method, spectral analysis of the frequency of characters are closely observed. From the spectral analysis and also from the frequency analysis, it is evident that there is no pattern of repetition in the encrypted file. Hence this method is very effective and strong.

VIII. CONCLUSION AND FUTURE WORK

As the applications of WSN tend to increase more rapidly, the problem of achieving energy efficient communication and securing them against attacks becomes much more important. Without proper security, it is impossible to completely trust the results reported from sensor networks deployed outside of controlled environments. In this paper we have seen how one can use the Modern Encryption Standard version –I algorithm to achieve secure communication in WSN. The method is very much flexible in comparison to any standard methods. We can split the original file more than two also and we can apply TTJSA and DJSA in alternate ways and the whole process can be applied multiple times. The method can be further strengthened if we apply in bit level. Split the plaintext file into two files and apply bit level encryption separately in two different blocks. Then combine the two encrypted files and apply the bit level encryption on the combined file

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 7, October 2015

REFERENCES

1. N. Gura, A. Patel, A. Wander, H. Eberle, and S. Shantz, 2004 Comparing elliptic curve cryptography and RSA on 8-bit cpus. *In 2004 workshop on Cryptographic Hardware and Embedded Systems*, Aug.
2. R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus, 2004 Tinypk: Securing sensor networks with public key technology. *Proceedings of the 2nd ACM workshop on Security of Ad hoc and Sensor Networks (SASN '04)*, pp. 59–64. ACM Press.
3. P. Gaudry. NTLJac2, Tools for genus 2 Jacobians in NTL. .
4. A. Perrig, J. Stankovic, D. Wagner, 04 Security in wireless sensor networks. Commun. *ACM* 47(6): 53–57
5. Menezes, A., Okamoto, T., and Vanstone, S. "Reducing elliptic curve logarithms to logarithms in a finite field". *Proceedings of the twenty-third annual ACM symposium on Theory of computing.* ACM Press, 1991: p 80 – 89.
6. S. AlRiyami and K.G. Paterson. Certificateless public key cryptography, 2003 *In Advances in Cryptology – ASIACRYPT 2003*, vol. 2894 of LNCS, pp. 452–473, available at http://eprint.iacr.org/.
7. D. Boneh and M. Franklin, Identity-Based encryption from Weil pairing. *SIAM Journal of Computing*, 32(3): 586–615, 2003.
8. C. Cocks, An Identity Based Encryption Scheme Based on Quadratic Residues, 2001,*Proceedings of the 8th IMA International Conference on Cryptography and Coding, LNCS 2260*, pg 360-363, Springer-Verlag.
9. D. Boneh and X. Boyen, 2004, Secure Identity Based Encryption without Random Oracles, *extended abstract in Proceedings of CRYPTO '04, LNCS 3152, Springer-Verlag*, available in IACR eprint archives.
10. D. Boneh and M. Franklin. Identity based encryption from the Weil pairing, in *Advances in Cryptology – Crypto 2001, Lecture Notes in Computer Science* ***2139*** *(2001)*, Springer, 213–229.
11. G. Hanaoka, T. Nishioka, Y. Zheng, and H. Imai. An efficient [hierarchical identity based key-sharing method resistant against collusion-attacks, *in Advances in Cryptology – Asiacrypt 1999, Lecture Notes in CS* ***1716*** *(99)*, Springer, 348–362.
12. J. Horwitz and B. Lynn. Toward Hierarchical Identity-Based Encryption, *in Advances in Cryptology – Eurocrypt 2002, Lecture Notes in Computer Science* ***2332*** *(2002), Springer*, 466–481.
13. D. Boneh and X. Boyen. Secure identity based encryption without random oracles. Crypto '04.
14. Aashima Singla and Ratika Sachdeva, Review of Security Issues and attacks in WS N, in International Journal of Advanced Research in Computer Science and Software Engineering, Vol 3, Iss 4, Apr 13, ISSN 2277-128X.
15. Symmetric key cryptosystem using combined cryptographic algorithms-Generalized modified Vernam Cipher method,MSA and NJJSAA: TJSA algorithm-Proceedings of Information and Communication Technologies(WICT), 2011, 11th -14th, Dec2011, pg 1175 – 1180.
16. Al-Sakib Khan Pathan, Hyung-Woo Lee,, Choong Seon Hong, Security in Wireless Sensor Networks: Issues and Challenges, ICTACT, 2006, ISBN – 89 – 5519 – 129 – 4.
17.

BIOGRAPHY

A.Praveena is an Assistant Professor in the Information Technology Department, Dr.N.G.P Institute of Technology, Coimbatore, TamilNadu, INDIA. She received Master of Engineering in 2005 from Anna University, Chennai,INDIA. She is currently doing her Part time Research in Anna University, Chennai. Her research interests are Computer Networks (wireless Networks), Security etc.