ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 4, Issue 2 (Apr. - Jun. 2016)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2016)

Wireless Sensor Network Security using Cryptography

[I]Yashaswini R, [II]Nayana HG, [III]Bindu AThomas
[I,II,III]Vidya Vikas Institute of Engineering and Technology, Mysuru, Karnataka, India

Abstract
The wireless sensor networks are a combination of tiny devices called sensor nodes.Thesecure communication among various sensor nodes is a fundamental challenge for providing security services in WSNs. Wireless sensor networks are characterized by several energy resources and the security mechanism are used to detect, prevent and recover from securityattack.WSNs are more popular for designing and implementing which connects physical world to the external world. Therefore security is a main concern for WSNs. In order to overcome security attacks by use of cryptography technique. This paper tends to outline the major aspects of wireless sensor networks security

Keywords
Wireless Sensor Networks, Sensor, Attacks, Security, Cryptographyin WSNs

Introduction

Wireless sensor networks have emerges as modern day technology in information technology ecosystem and research involving hardware system design, data management, security and social factors.Sensor networks refer to a heterogeneous system combining tiny sensors and actuators with general purpose computing elements. Sensornode isasmart, tiny, self organizing, lowcast, and multi-functional device, equipped with batery, radio communication, microcontroler and sensor. It has very limited processing capability battery power, memory and also a restricted field of sensing.

The main purpose of WSN is to serveas an interface to real world, providing physical information such as temperature, light, radiation etc to a computer system. In this paper to address the critical security issues in WSNs we discuss about cryptography.

WSN Security Goals

The main security goals for WSNs are

Data confidentiality

It is the ability to hide message from a passive attacker and is the most important issue in network security. Sensor nodes may communicate with data so it is important to build a secure channel in a WSN.

Data integrity and authentication

It refers to the ability to confirm the message that has not been altered while it was on the network. The attacker can change the whole data packet. Therefore the receiver needs to ensure that the data obtained from the corect source.

Data availability

Availability is of importance for maintaining an operational network. It is the ability of a node to utilize the resources and the network is available for the message to move on.

Data freshness

It ensures that the data content is recent and it does not contain old content of data.This requirement is especialy important when there are shared-key strategies employed in the design and need to be changed over time.

Self-organization

WSN which requires every sensor node to be self-organizing and self-healing according to differentsituations.

Time synchronization

Many WSN applications demand some form of time synchronization for execution. A more colaborative sensor network may require group synchronization for tracking applications.

Secure synchronization

Sensors may get displaced while deploying than or after a time interval or evena fter some critical displacement incident.

Operations On Wireless Sensor Network

The WSNs offers an excelent opportunity to monitor environment and have a lot of applications and also they have large network multiple present functions, such as sensing and processing to fulfil different application objectives. Sensor nodes are staticmost of the time,where as mobile node scan be deployed according to application requirements. Sensor nodeskeepmonitoringthenetworkarea afterbeingdeployedtogether withthenet work.After aneventofi nterestoccurs,oneofthesurounding nodescandetectit,generatear eport,andtransmit thereportto a Base stationthroughmulti-chip wirelesslink.

Collaboration can be caried out if multiple surroundings nodes detect the sameevent.Inthis caseoneofthem generatesafinalreport after colaborating with other nodes. The Base Stationcan process the report and then forward it through either highqualitywirelessorwiredlinktotheexternal world for further processing. The WSN authority can send commands or queries to abasestation, which spreadsthosecommandsintothenetwork. Hence, a Base Station acts as a gateway between the WSN and the externalworld. An example for this shownin below figure.

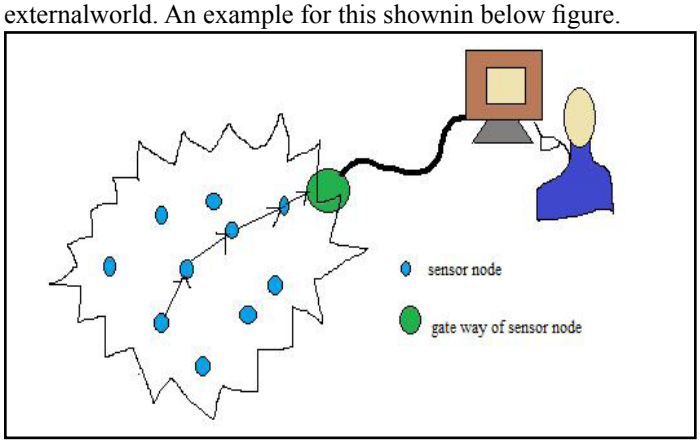


Fig.1 : Wirelesssensornetwork

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Challenges of sensor networks

The nature of large, WSNs presents significant challenges in designing security schemes

A wireless sensor network is a special network which has many constraints.

Wirelessmedium

The wireless medium is less secure because its broadcast nature makes eavesdropping simple. The wireless medium allows an attacker to easily interrupt valid packets and easily inject malicious ones.

Ad-Hocdeployment

The ad-hoc nature of sensor networks means no structure can be staticaly defined. The network topology is always subject to changes due tonodefailure,addition,ormobility.Nodesmaybe deployedbyairdrop,sonothingisknownofthe topologypriorto deployment.Securityschemes mustbe able to operate within this dynamic Environment.

Hostile environment

The next chalenging factor is the hostile environment in which the sensor node functions. The highly hostile environments representa serious chalenge for security researchers.

Resource scarcity

Theextremeresourcelimitationsofsensor deviceposeconsiderable chalengetoresource-hungrysecuritymechanism.

Immense scale

The proposed scale of sensor networks poses a significant chalenge for security mechanisms.Securitymechanismsmustscalableto very large networks while maintaining high computations and communication efficiency.

Unreliable communications

It is anothe rattack to sensor security. The security of the network reliesheavily on a defined protocol,which in turn depends on communication.

Security Attacks

Wireless sensor networks are quite different from other wireless and wirednetworks. Securityis importantin wirelesscommunication assensor nodes deployed in realenvironment so easily vulnerable to different types of attacks and threats.

TheattacksinWSNsare

1. Goalorientedattacks
2. Performer-orientedattacks
3. Layer-orientedattacks

1. Goaloriented attacks: It consists of active and passive attacks

Active attacks: In active attacks, the attacker is no longer passive but takes active measures to achieve control over the network. Some examples of active attacksare Dos, blackhole, worm hole, sinkhole, modificationetc.

Passive attacks: These attacks are mainly due to the data confidentiality. An attacker in passive attack monitors encrypted traffic and looks for sensitive information that can be used in other types of attacks. Passiveattacksincludetrafficanalysis, monitoring communications, capturing authentication information.

Performer-orientedattacks: The another category in attackson WSNs are

Out side attacks: outside attacks may cause passive eavesdropping on data transmissions, as well as can extend to injecting bogus data into the network to consumer network resourcesandraisedenialof service attacks.

Inside attacks: Inside attacks can damage the network stealthy since they can avoid our authenticationandauthorizationbecausetheyare legitimatenodesofthenativenetworkandhave accesstothenetw orkinformation,anditisnoteasy to expect their attack paterns. This attack suppressestheimportantinformationreachingthe basestationwhichsignificantlydegradesnetwork performance,su chaspacketdeliveryratedueto theirrepeatedpacketdrops.

Layer-orientedattacks: WSNs are organized in layered form. This layered architecture makes these networks vulnerable to various kinds of attacks.

The most popular types of security attacks

Denial of service attack

It is produced by the unintentional failure of nodesormaliciousaction. Denialof Serviceattackis meantnotonlyforthe adversary's atemptto subvert,disrupt,ordestroyanetwork,butalsofor any event that diminishes a network capability to provide a service. The mechanism to prevent Denial of Service attacks includes payment for network re\sources,pushbanks,strongauthentication and identificationoftraffic.

Dos attack is an attempt to make a machine or network resourcesunavailabletoitsintendedusers, such as to temporarily orindefinitely interrupt servicesofahostconnectedtotheinternet. Criminal perpetrators of Dos attacks often target sites or serviceshostedonhigh-profilewebservers suchasbanks,creditcar dpaymentgatewaysbut motivateofrevenge,blackmailcanbebehin dother attacks.

Sybil attack

A single node duplicates itself and presented in the multiple locations. The Sybil attack target fault tolerant schemes such as distributed storage, multipathrouting and topology maintenance.

The Sybil attack is computer security is an attack where in a reputation systemis subverted by forging identitiesin peer-to-peer networks. It is named after the subject of the book Sybil, acase studyofwomendiagnosedwithdissociativeidentity disorder.Anentityonapeer-to-peernetworkisa piece of software which as access to local resources.A faultynode oran adversarymay presentmultipleidentitiestoapeer-to-peernetwork inordertoappearandfunctionasamultipledistinct nodes.

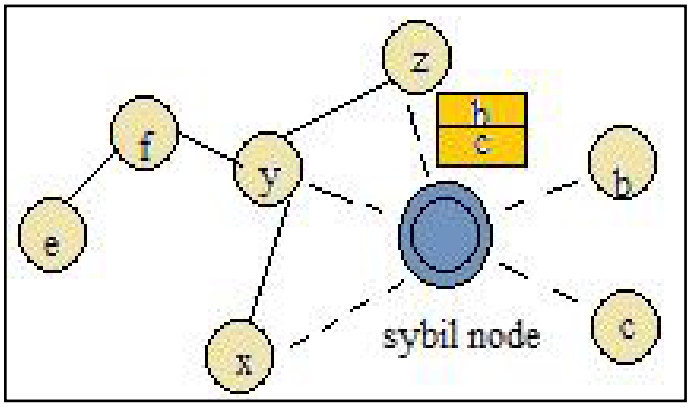


Fig. 2 : Sybilattack

Traffic analysis attack

Trafficanalysisistheprocessofintercepting and examining messages in orderto deduce informationfrom paternsincommunication. It can be performed even when the messages are encryptedandcannotbedecrypted.Ingeneral,the greaterthenum berofmessagesobserved,oreven encryptedandstored,themore canbeinferedfrom thetraffic.Trafficanalysiscanbeperformedin contextofmilitaryinteligence, counter-inteligence, orpatern oflife analysis,and in concern in computer security. Even when the messages transfered as encrypted,itstilleaves a high possibilityanalysisofthecommunicationpaterns. Sensoractivities can potentialy revealenough information to enable an adversary to cause maliciousharmtothesensornetwork.

Traffic analysis is based on the track and analysisoftheflow oftrafficsoastoknow the networkscheme,leadingtodirectnodesa ndhave accesstothem.

Node replication attack

This attack is quite simple; an attacker seeksto add a node to an existing networkbycopyingthe node ID ofan existing sensornode. This is independent attack unique to wireless sensor networks.

The attack makesit possible for an adversary to prepare her own low costsendernodesandinduce thenetworktoacceptthem aslegitimateones.To do so,the adversary,onlyneeds to physicaly capture one node,revealits secretcredentials, replicatethenodeinlar gequantity,anddeploythese malicious nodes back into the network so ast o subvert the network with little effect.

Attacks against privacy

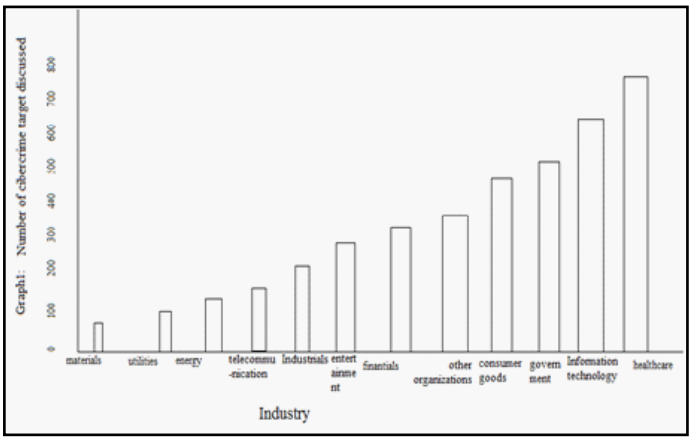
The main privacy problem is not that sensor networks enable the collection of information. Here, much information from sensor networks could probably be collected through discrete site surveillance. The privacy attack is neighbors attack.

Physical attack

Sensor networks typically operate in hostile outdoor environments. In such environments, the small form factor sensors, coupled with the unattended and distributed nature of their deployment make them highly susceptible to physical attacks.

A physical attack is one that involves dealing damage to target in any number of ways that do not involve “magic”. Examples of physical attacks are auto attacking a mob with your weapon, using skills such as jump, blue magic such as head butt, etc.

Cryptography in WSNs



Cryptography is the science if using the mathematics to encrypt and decrypt data. Cryptography, art and science of preparing coded or protected communications intended to be intelligible only to the person processing a key. Cryptography refers both to the process or skill of communicating in or deciphering secretes writings and to the use of coder to convert computerized data so that only a specific recipient will be able to read it using key. The figure below shows the traditional cryptography system.

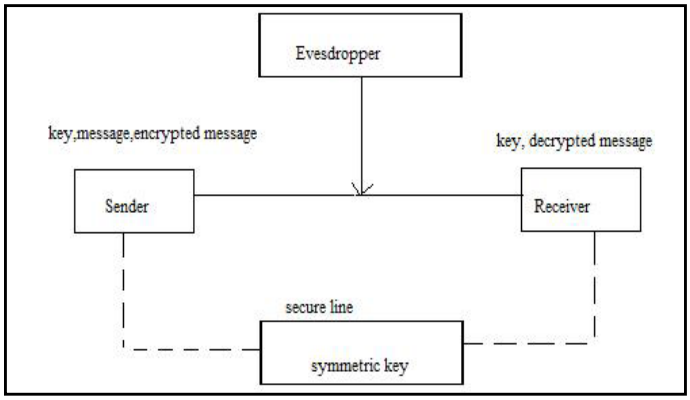


Fig. 3: Traditional cryptography system

Cryptographers call an original communication the clear text or plain text. Once the original communication has been scrambled or enciphered, the result is known as the cipher text or cryptogram. Cryptography is important for more than just privacy, however cryptography protects the world’s banking systems as well.

WSN are used in many critical applications like military, habitat monitoring. Minimum level of security like integrity and authentication is required for certain applications, due to their sensitive nature of WSN. The below figure shows the model of cryptography.

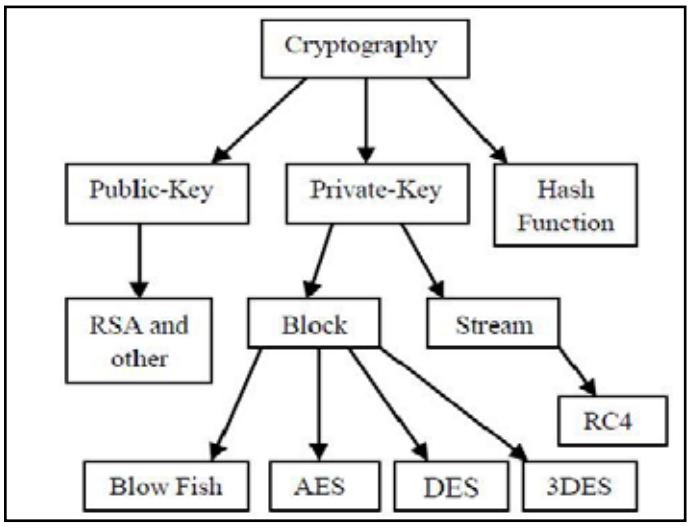


Fig. 3: Model for cryptography

Cryptanalysis

It is the art of analysis cipher text to extract the plaintext or the key. In other words, cryptanalysis is the opposite of cryptography. It is the breaking of cipher, understanding the process of code breaks is very important when designing the encryption system.

The three cryptographic schemes are

Secret key cryptography or symmetric key cryptography

Symmetric key cryptography uses a single key for both encryption and decryption. It can be designed to have high rate of data

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

throughput. Keys of symmetric cipher are too short. These ciphers are composed to produce strong ciphers. The disadvantages of secret key cryptography are in two party communication systems, the key must be shared by the sender and receiver.

Public key cryptography or asymmetric cryptography

It uses one key for encryption and another key for decryption. Only the private key must be secret. In a large network, the number of keys necessarily may be smaller than in the symmetric key scenario. In public key cryptography depending on the mode of usage it remains unchanged for considerable period of time. The disadvantage is key sizes are typically much larger than those required for symmetric key encryption.

Hash function: Uses a mathematical transformation to irreversibly encrypt information.

Public key cryptography is not suitable for WSN because of its resource demanding nature. Symmetric key cryptography is more efficient and suitable for WSN. But it has the inherent problem of sharing the secret keys and hostile nature of WSN makes it is vulnerable to various attacks.

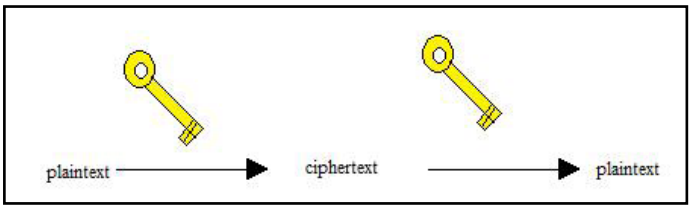


Fig. 4 : Secretkey

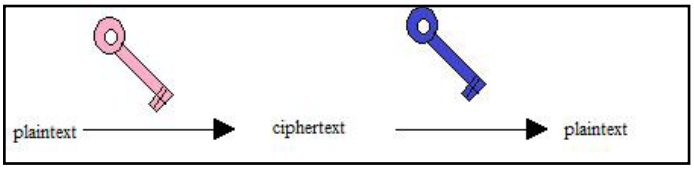


Fig. 5 : Publickey

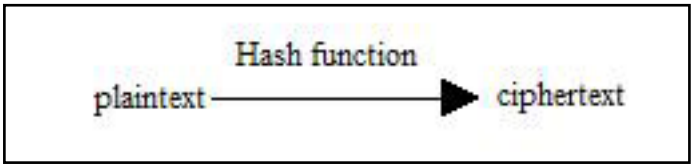


Fig. 6 : Hashfunction

RSA: Rivest-Shamer-Adleman is the most commonly used public key encryption algorithm. RSA can be used to send an encrypted message without a separate exchange of secrete key. It can also be used to sign a message. In RSA, this asymmetry is based on the practical difficulty. Of factoring the product of two large prime numbers, the factoring problem. The security of RSA algorithm relies on the difficulty of factoring of very large numbers. RSA is an asymmetric algorithm and plays a key role in public key cryptography. It is widely used in electronic commerce protocols.

AES: AES is block cipher. It has variable key length of 128, 192, or 256 bits. It encrypts data block of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible; it can be implemented in the various platforms.

Blowfish: it is important schemes type of the symmetric key encryption that has a 64 bit block size and variable key length from 32 bits to 448 bits in general. Because of larger key size it is complex to break code in the blowfish algorithm.

Triple DES: 3DES is an enhancement of DES, it is 64 bit block size with 192 bits key size. In this standard the encryption method is similar to one in the original DES but applied 3 times to increase the encryption level and the average safe time. It is a known fact that 3DES is slower than other block cipher method.

RS4: it is recognized as the most commonly utilized stream cipher in the world of cryptography. RS4 has use in both encryption and decryption while the data stream undergoes XOR together with a series of generated keys. The output is then XORed together with this stream of data in order to generate a newly encrypted data.

DES: Data encryption standard is a symmetric block cipher developed by IBM. The algorithm uses a 56-bit key to encipher/decipher a 64-bit block of data. the key is always presented as a 64-bit block, every 8th bit of which is ignored.

Block cipher: A block cipher is a deterministic algorithm operating on fixed-length groups of bits, called blocks, with an unvarying transformation that is specified by a symmetric key. Block cipher are important elementary components in the design of many cryptographic protocols, and are widely used to implement encryption of bulk data. The modern design of block ciphers is based on the concept of an iterated product cipher. Even a secure block cipher is suitable only for the encryption of a single block under a fixed key.

Selection of Right cryptographic schemes

The selection of right cryptographic schemes relies on following constraints

Time: How much time will be needed for encrypting and decrypting the data and how much time it needs to fulfill the prerequisites before starting an encryption.

Memory: How much memory will be need especially in case of small devices like PDAs, smart cards.

Security: Here, the selected schemes should meet the confidentiality, integrity.

Table1:comparisonofcryptographyandattacks

Cryptography applications	Attacks
Digitalsignature	Denialofservice,lackof integrity
Smartcards	Activeandpassive
E-comers	Denialofservice, unauthorizedaccess
WirelessLocalarea network	Adobeattack
Securecloudstorage	Securityattack,denialof service
FPGA	Cold-bootattack
Ultralowpowerdevice	Biclique,zerocorelation

Conclusion

Providing security in a wireless sensor network is a challenging task. So the need for security becomes vital. However, the WSNs suffer from many constraints such as limited energy, processing capability, and storage capacity, as well as unreliable communication. There are many ways to provide security, and the main one is cryptography method for sensor nodes is fundamental to provide appropriate security services. This paper provides the survey of various types of cryptography and it provide good data

security.

References

[1]. Rajesh R Mane "A review of cryptography algorithms, attacks and encryption tools" international journal of innovative research in computer and communication engineering, vol.3,issue 9, September 2015.

[2]. Monika roopak " review of threats in wireless sensor networks" international journal of computer science and information technology, vol 5,2014,25-31

[3] Anitha S.Sastry, Shazia Sulthana and Dr.S Vagdevi, "Security Threats in Wireless Sensor Networks in Each Layer", International Journal of Advanced Networking and Applications, Vol. 04 Issue 04, pp. 1657-1661, 2013.

[4]. Abhishek Jain, Kamal Kant and M. R. Tripathy ,"Security Solutions for Wireless Sensor Networks", Second International Conference on Advanced Computing & Communication Technologies, 2012.

[5]. Kumar, P.; Cho, S.; Lee, D.S.; Lee, Y.D.; Lee, H.J. TriSec: A secure data framework for wireless sensor networks using authenticated encryption. Int. J. Marit. Inf. Commun. Sci. (2010), 129-135.

[6]. Sharma, K. and Ghose, M. (2010) Wireless Sensor Networks: An Overview on Its Security Threats. IJCA, Special Issue on "Mobile Ad-hoc Networks" MANETs, 42-45.

[7] Kalpana Sharma, S.K. Ghosh, and M.K. Ghose 'Establishing an Integrated Secure WirelessSensor Network System: A New Approach', International Journal of Next Generation Networks (IJNGN), Sept.2010

[8]. Cho, J.-H., Swami, A. and Chen, R. (2011) A Survey on Trust Management for Mobile Ad Hoc Networks. IEEE CommunicationsSurveys & Tutorials, 13, 562-583. http://dx.doi.org/10.1109/SURV.2011.092110.00088

[9] H. Mohamed and B. Majid, "Forest Fire Modeling and Early Detection using Wireless Sensor Network" in Ad Hoc & Sensor Wireless Networks, Vol 7, Philadelphia: Old City Publishing, 2009.

[10] Jinat Rehana, "Security of Wireless Sensor Network", 2009.

[11] David Boyle and Thomas Newe," Securing Wireless Sensor Networks: security Architectures" (2008), Journal of Networks, VOL. 3, NO. 1,pp 65-77.

[12] Haodong Wang, Bo Sheng, Chiu C. Tan, Qun Li, "Comparing Symmetric-key and Public-key based Security Schemes in Sensor Networks:

[13] A Case Study of User Access Control", College of William and Mary Williamsburg, VA 23187-8795, USA.

[14] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Sean Hong, "Security in Wireless Sensor Networks: Issues and Challenges", Proc. ICACT 2006, Volume 1, 20-22, pp. 1043-1048, Feb. 2006

[15] David J. Malan, Matt Welsh, Michael D. Smith, "A Public-Key Infrastructure for Key Distribution in TinyOS Based on Elliptic Curve Cryptography", Division of Engineering and Applied Sciences, Harvard University, Dec 2007.

[16] Haowen Chan,and Adrian Perrig,"Security and Privacy in Sensor Networks",Carnegie Mellon University pp.99-101.

[15] W. Xu et al., "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," MobiHoc '05: Proc. 6th ACM Int. Symp. Mobile Ad Hoc Net. and Comp., pp. 46–57, 2005.

[17] D. Culler, D. Estring, M. Srivastava, "Overview of Sensor Networks," Computer, 37, 8, pp. 41–49 August 2004.

[18] E.Shi and A.Perrig, "Designing Secure Sensor Networks", Wireless Commun. Mag., Vol. 11, No. 6, pp.38-43, Dec 2004.

[18] Undercoffer, J., Avancha, S., Joshi, A., and Pinkston, J., "Security for Sensor Networks", CADIP Research Symposium, 2002, available at,

[19] Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol. 47, No. 6, pp. 30-33, Jun. 2004.

[20] W. Stallings. "Cryptography and Network Security", Prentice Hall, 1995.