iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** IV **Month of publication:** April 2014

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Security issues and challenges in wireless sensor networks

A review analysis

Rajdeep Bhanot[1], Naveen Bilandi[2]

[1]M Tech (CSE) Student, DAV University Jalandhar [2]Assistant Professor in dept. of CSE, DAV University Jalandhar

Abstract: ***As these days, wireless sensor networks are growing at persistent rate. This technology is showing promising positive changes in futuristic communication and data transfer. One of the major applications of wireless sensor network is in Military. So there is strong need of strong security mechanisms. Because sensor networks may interact with sensitive data or operate in unsafe environment. These security concerns should keep in mind while designing the system. The inclusion of wireless communication technology also incurs various types of security threats. In this context, we will identify the security aspects like requirements, classifications, types of attacks and the security mechanisms for wireless sensor security etc. In this paper we will discuss the different security issues, threats and security mechanisms.***

Keywords: **WSN (wireless sensor network), Attacks, Security, Mechanisms.**

1. INTRODUCTION

The sensor network is a group of self-organized sensor nodes. These creates network in spontaneous manner. "The basic idea of sensor network is to disperse tiny sensing devices; which are capable of communicating with other wireless devices over a specific geographic area or change in parameters". WSN is an advanced technology of network and is very different from traditional wireless networks. The main characteristic of WSN is sensing nodes. Wireless sensor networks are quickly gaining popularity due to the fact that they are potentially low cost solutions to a variety of real-world challenges. Communication between wireless sensor networks is done using wireless transceivers Sensor networks introduces severe resource constraints due to their lack of *data storage* and *power* .In traditional computer security techniques of wireless sensor network, *Data storage* and *Power issue* are the major obstacles. The unreliable communication channel and unattended operation make the security defenses harder. According to the need many researchers have begun to address the challenges of maximizing the processing capabilities and energy constraints of Wireless sensor network. WSN security topic attracted many researchers to work on various issues of it. However, while the routing strategies and WSN modeling are getting much preference but security issues are yet to receive extensive focus. Because WSN is a new technique with new challenges or security issues so there are requirements of new security mechanism to remove different types of threats. Here we will discuss the following unique properties like challenges and requirements of security in wireless sensor networks and existing security mechanism of WSN and finally conclusion and future work in wireless sensor network security area.

2. RELATED WORK

Al-Sakib khan pathan, Hyung-woo Lee and Choong Seon Hong explained that most of the attacks against the security are caused by false information. They explained about main threats to the WSN and then proposed the different security mechanisms Like JAM, TIK, REWARD and TinySec etc[1].

Kuthadi venu, Rajendra and Raja Lakashami's paper is mainly concentrated on key distribution mechanisms, detection of node

replications and secure routing mechanisms in WSN. They discussed that existing security mechanisms are providing security to some extent only[2]. In order to achieve full security in WSN, Implementation of security mechanisms would be on each component of sensor network and communication protocols.

Dr. Manoj Kumar Jain have discussed about the sensitive issues of WSN security and described four main aspects of WSN security: Obstacle, requirements attacks and defenses measures[4]. Dr. jain presented effective routing protocol security mechanisms.

Pooja , Manisha and Dr, Yudhvir Singh discussed important security issues that occur in WSN and Sybil attack in wireless sensor network security. These also proposed some important security mechanisms only used for Sybil attacks[6].

John Paul Walters, Zhengqiang Liang, Weisong Shi and Vipin Chaudhary presented a complete survey on WSN security including all the security issues[5] , all the attacks and their prevention algorithms in detail.

Kriti Jain , Upasana Bahugune followed top-down approach to explain the new applications, types of sensor networks, Challenges, Operating system used, standards IEEE 802.15.4, ZigBee, Wireless-hart etc[3].

2. SECURITY REQUIREMENTS

WSN shares many characteristics with traditional networks, including their security requirements: however they also introduce several requirements that are exclusive to them.

3.1 Data confidentiality: Data confidentiality is the biggest problem in network security. Every network with any security approach would probably address this issue before any other. A sensor node must not filter sensor readings to its neighbors; like in military applications where the stored data in a node can be highly confidential. This problem is faced in many applications, so it is very important to build a secure communication channel in WSN. For this purpose, public information and keys can be encrypted to protect data against traffic analysis attacks

3.2 Data integrity: With encryption scheme, we can secure data from adversary. But adversary still could modify the data that can affect the overall operation of the network. Like, a malicious user may add or remove certain fragments to a packet. when this packet will be communicated to its original destination. The data lose or corruption can occur without the presence of malicious user. So data integrity assures that the received data have not been modified in transit.

3.3 Data freshness*:* Even though data confidentiality and integrity has been achieved, we must assure that each message is fresh. Data freshness suggests that the data are recent, and assures that no old message has been resent. This requirement is especially important when shared keys strategies are being used. Typically, shared keys need to be renewed over time. However, it takes time to propagate the new keys through the entire network. Under this scheme, it would be easy for an adversary to perpetrate a packet replay attack. Furthermore, it would be easy to corrupt the operation of the network if the nodes are not well informed of the time at which the key will change. To solve this problem, a time dependent counter may be added to the packet for assuring data freshness.

3.4 Authentication: Besides modifying packets, an adversary can also potentially alter the flow of the packets through the addition of fake packets to the network. Consequently, the adversary can make receiving node believe that the data comes from an authentic source. Additionally, authentication is needed for several administrative tasks (i.e., dynamic network reprogramming, controlling node duty cycle). Thus, we can determine that message authentication is important for many sensor network applications.

3.5 Availability: Adjusting current traditional encryption algorithms to sensor network implies an additional cost. Some approaches suggest modifying code to favor code reutilization as much as possible. Other approaches tend to use additional communication to achieve the same goal. Other more radical approaches impose restrictions to the data or propose less robust schemes (like centralized schemes) to simplify algorithms. But all of these approaches decrease the level of availability of the nodes and consequently, the availability of the entire network for the following reason.

- The introduction of additional processing results in additional power consumption. If we exhaust the available energy of a node, its data would no longer be available.

- Introducing additional communication operations also consumes more energy. Furthermore, adding more communication considerably increases the probability of generating a collision.

- If we introduce a centralized scheme, it would only have a single point, which can be a constant threat to the availability of the entire network.

The implementation of security mechanisms not only interferes with network operation, it also can considerably affect availability of the entire network.

3.6 Auto configuration : WSN are an extreme case of ad hoc networks, which require that each node be *independent* and *flexible* for configuring itself according to several situations. There is no fixed infrastructure to administer a sensor network. This also brings a great challenge for security in this type of networks. In the area of public key cryptography on wireless sensor networks, this same dynamicity requires efficient mechanisms for key distribution. WSN must auto-configure for key management and for establishing trust relationships among nodes, in a similar way as they auto-configure to perform multi-hop routing. If a sensor network lacks of auto-configuration, the damage done by an adversary or even by the hostile environment could be fatal.

4. SECURITY ATTACKS ON WIRELESS SENSOR NETWORKS

The nature of the WSN makes them vulnerable to several types of attacks. Such attacks can be perpetrated in a variety of ways, most notably are the denial or service attacks (DoS), but there are also traffic analysis attacks, eavesdropping, physical attacks, and others. DoS attacks in wireless sensor networks go from simple communication channel saturation techniques to more sophisticated designed to tamper with the message authentication code (MAC) layer protocol (Perrig, Stankovic, & Wagner, 2004).

Due to the great differences in available energy and computational power, protecting against a well designed denial-of-service attack is practically impossible. A more powerful node could easily block any other normal node, and consequently, prevent the sensor network from performing its function.

We can observe that attacks on sensor networks are not exclusively restricted to denial-of-service attacks; among these other types of attacks we can include compromised nodes, attacks to routing protocols, and physical attacks.

4.1 Attack-scenario

To propose and develop efficient prevention and recuperation mechanisms for attacks on wire- less sensor networks it is important to know and understand the nature of the potential adversaries; these can be classified in two groups (Karlof &Wagner, 2003): mote class adversaries and laptop class adversaries. In the first case, the adversary has access to sensor nodes. In contrast, the laptop class adversary has access to more powerful de- vices such as personal computers, PDAs, and so forth. Thus, in this case, the devices have many advantages over legit nodes: larger energy source, more powerful processors, and they could also have high-power transmitters or a highly sensitive antenna to eavesdrop on traffic.

A laptop class adversary can produce more damage as opposed to an adversary that only has access to a few sensor nodes. For instance, a sensor node can only block radio links in a small neighborhood while an adversary with a laptop computer could block the entire sensor network with the help of a more powerful transmitter. Furthermore, a laptop class adversary could potentially eavesdrop on the traffic of the entire network, while a mote class adversary could only eavesdrop on the traffic in a very limited area.

Another commonly used adversary classification considers external and internal adversaries. Previously, we discussed external attacks, where the adversaries do not have any access to the sensor network. Conversely, internal attacks are those perpetrated by an authorized participant in the network that has turned malicious. Internal attacks can be mounted from compromised nodes that are executing malicious codes or from laptop computers that have access to cryptographic materials, data, and codes from authorized nodes.

4.2 Attacks to Routing Protocols:

Most routing protocols for WSN are very simple; due to this simplicity, they are generally more vulnerable to attacks than their counterparts in ad hoc networks. Most attacks on network layer protocols fall into one of the following categories:-

• *DoS(Denial of service attack):-* A standard attack on wireless sensor network is simply A standard attack on wireless sensor networks is simply to jam a node or set of nodes. Jamming, in this case, is simply the transmission of a radio signal that interferes with the radio frequencies being used by the sensor network . The jamming of a network can come in two forms: constant jamming, and intermittent jamming. Constant jamming involves the complete jamming of the entire network. No messages are able to be sent or received. If the jamming is only intermittent, then nodes are able to exchange messages periodically, but not consistently.

• *Spoofed, altered, or replayed routing information:-* This attack is directed toward the routing information that is exchanged between nodes. By spoofing, altering, or replaying routing information, the adversaries could potentially create routing loops, attract or repel network traffic, lengthen or shorten routes, generate fake error messages, partition the network, increase node to node latency, and so forth.

• *Selective forwarding*:- Multi-hop networks often operate assuming faithfully that messages will be received by their destination. On a selective forwarding attack, malicious nodes could prevent forwarding certain messages or even discard them; consequently, these messages would not propagate through the network. A simple form of this attack is very easy to be detected because the neighbor nodes could easily infer that the route is no longer valid and use an alternate one. A more subtle form of this attack is when and adversary selectively forwards packets. Therefore, if an adversary is interested in suppressing or modifying packets that come from certain source, the adversary could selectively forward the rest of the traffic, thus, the adversary would not raise any suspicion of the attack.

• *Sinkhole attacks:* - In a sinkhole attack, the goal of the adversary is to attract all the traffic to a certain area or the network through a compromised node, creating a sinkhole (metaphorically speaking). Due to the fact that the nodes that are located across the route have the ability to alter application data, the sinkhole attacks could facilitate other types of attacks (like selective forwarding for in- stance).

• *Sybil attacks*:- In a Sybil attack (Douceur,2002), a node presents multiple identities to the rest of the nodes. Sybil attacks are a threat to geographical routing protocols, since they require the exchange of coordinates for efficient packet routing. Ideally, we would expect that a node only sends a set of coordinates, but under a Sybil attack, an adversary could pretend to be in many places at once[6].

• *Wormhole attacks*:- In a wormhole attack (Hu, Perrig, & Johnson, 2002) an adversary builds a virtual tunnel through a low latency link that takes the messages from one part of the network and forwards them to another. The simplest case of this attack is when one node is located between two other nodes that are forwarding. However, wormhole attacks commonly involve two distant nodes that are colluded to underestimate the distance between them and forward packets through an external communication channel that is only available to the adversary.

• *HELLO flood attacks*:- Some protocols require nodes to send HELLO packets to advertise themselves to their neighbors. If a node receives such packet, it would assume that it is inside the RF range of the node that sent that packet. However, this assumption could be false because a laptop class adversary could easily send these packets with enough power to convince all the network nodes that the adversary is their neighbor.

• *Acknowledgement spoofing*:- Some routing algorithms require the use of acknowledgement signals (ACK). In this case, an adversary could spoof this signal in response to the packets that the adversary listens to. This results in convincing the transmitting node that a weak link is strong. Thus, an adversary could perform a selective forwarding attack after spoofing ACK signals to the node that the adversary intends to attack.

TABLE I : Sensor network Layer and Attack:

LAYER	ATTACK
Physical Layer	DoS-Jamming , Sybil
Data-Link Layer	DoS- Collision, Exhaustion , Unfairness, Sybil- Data aggregation
Network Layer	Dos , Sybil and Wormhole Attack

Transport Layer	DoS- Flooding , De-synchronization

5. SECURITY MACHENISMS

Now days, the researchers are attracted by security concepts of wireless sensor networks. Many researchers have proposed some security mechanisms in wireless sensor networks. In this section we will deal with different security mechanisms.

5.1 TABLE II: Security Schemes for Attacks in WSN:

Security scheme	Attacks deterred	Network Architecture	Major features
JAM	DoS attack(Jamming)	Traditional wireless sensor network	Avoidance of jammed region by using coalesced neighbor nodes
Wormhole based	DoS attack(Jamming)	Hybrid(mainly wireless partly wired) sensor network	It uses wormholes to avoid jammed region in sensor network.
Random key pre-distribution	Sybil attack	Traditional wireless sensor network	Uses radio resource, random key pre-distribution, registration procedure, position verification and code attestation for detecting Sybil entity.
Bidirectional verification, multi-path multi-base station routing	Hello flood attacks	Traditional wireless sensor network	It adopts probabilistic secret sharing, use bi-directional verification and multi-path multi-base station routing
Communication security based	Information or data spoofing	Traditional wireless sensor network	Adopts efficient resource management, Protects the network even if part of network is compromised
TIK	Wormhole attack , information or data spoofing	Traditional wireless sensor network	Based on symmetric cryptography .require accurate time synchronization between all communicating parties.

There are some more security mechanisms used those are used in security schemes of wireless sensor network security.

5.2 secFleck: (Public key cryptography in wireless sensor network): This approach is used to provide the massage security services as confidentiality, Integrity and authentication in WSN with fast computation and lower energy utilization. For design and implementation of public key system, WSN needs new hardware and software. This approach is called as secFleck. This approach uses RSA algorithm to implement asymmetric public key system. This approach uses new operating system called Fleck OS or FOS. FOS is a C-based co-operative multi-threaded

operating system with public key cryptography primitives like encryption, decryption, signature verification etc. This approach is also good for massage security level.

5.3 LiSP:(Lightweight Security Protocol): It's lightweight security protocol for Wireless sensor networks[10]. It aims to provide authentication without retransmission of keys and also provides scalability in computing. It use symmetric key system approach. It uses temporary keys and master keys. It uses temporary keys and master keys. Temporary keys (TK) are used to encrypt and decrypt data packets. The master key (MK) is used to send temporary keys to single node. After network had been deployed, this protocol automatically selects one group of cluster heads as key server. The key server is used to distribute the temporal key, authenticate new nodes and detect nodes that have been compromised. When a key server transmits a packet for the first time it contains the length of the TK buffer, the key refresh rate, and the initial TK. The need for a Message Authentication Code is eliminated because the nodes are able to implicitly authenticate the TK by checking to see if the new TK matches the sequence of the other TK's in the TK buffer.

5.4 TinySec: A link layer security architecture for wireless sensor networks" is a light weight and link layer security protocol[9]. It provides security services as message Integrity, message authentication and access control at routing level and Reply protection in Adversary. It supports two different security options. They are Authenticated Encryption and Authentication only. In the Authenticated Encryption, the payload is encrypted first and then packet is encrypted using MAC. In Authentication only, the packet is directly encrypted with MAC without encrypting payload. This approach is used Cipher Blocked Chaining to encryption. TinySec is independent of cipher, key scheme, application. The TinySec packets are more in size then WSN packets, due to this; it needs more computing and processing power.

CONCLUSION

WSN Security has attracted many researchers, due to its unique characteristics, low cost deployment. This review paper is concentrated on key distribution mechanisms and secure routing mechanisms in wireless sensor network. The existing security mechanisms are providing security to some extent only. In order to achieve full security in WSN, implementation of security mechanism would be done on each component of sensor networks. Most of the attacks against security in wireless sensor networks are caused by insertion of false information by compromised nodes within the network. For defending the inclusion of false information by compromised nodes, there is requirement of detecting the false reports. However, developing such a detection mechanism and making it efficient represents a great research challenge.

REFFERENCES

[1] Al-Sakib khan Pathan[1] , Hyung-Woo Lee[2] , Choong Seon Hong[3] "security in wireless sensor networks: issues and challenges" [1]Kyung Hee University, Korea , [2]Hanshin University, Korea , [3]Kyung Hee University, Korea

[2] Kuthadi venu Madhav[1] , Rejendra.c[2] and Raja Lakshami Selvaraj[3] "Styudy of security challenges in WSN" [1]University of Johannesburg South Africa, [2]Audisankaara College Of Engineering and Technology,Gudur Nellore , Andhra Pradesh, India , [3]Botho College Gaborone, Botswana

[3] kriti Jain[1] , Upasana Bahuguna[2] "Survey On Wireless Sensor Network" [1]Tulas Institute Dehradun, India

[4] Dr. Manoj Kumar Jain, "Wireless Sensor network: Security issues and Challenges" , ijcit, vol. 2, issue 1, pp. 62-67, 2011

[5] John Paul Walters[1], Zhengqiang Liang[2] , Weisong Shi[3] and Vipin Chaudhary[4] "Wireless sensor network security : A survey" [1]Wayne State University

[6] Pooja[1] , Manisha[2] and Dr. Yudhvir Singh[3] "Security issues and Sybil Attack in Wireless sensor Networks" , International Journal of P2P network trends and technology , vol. 3 , issue 1 , pp. 7-13 , 2013

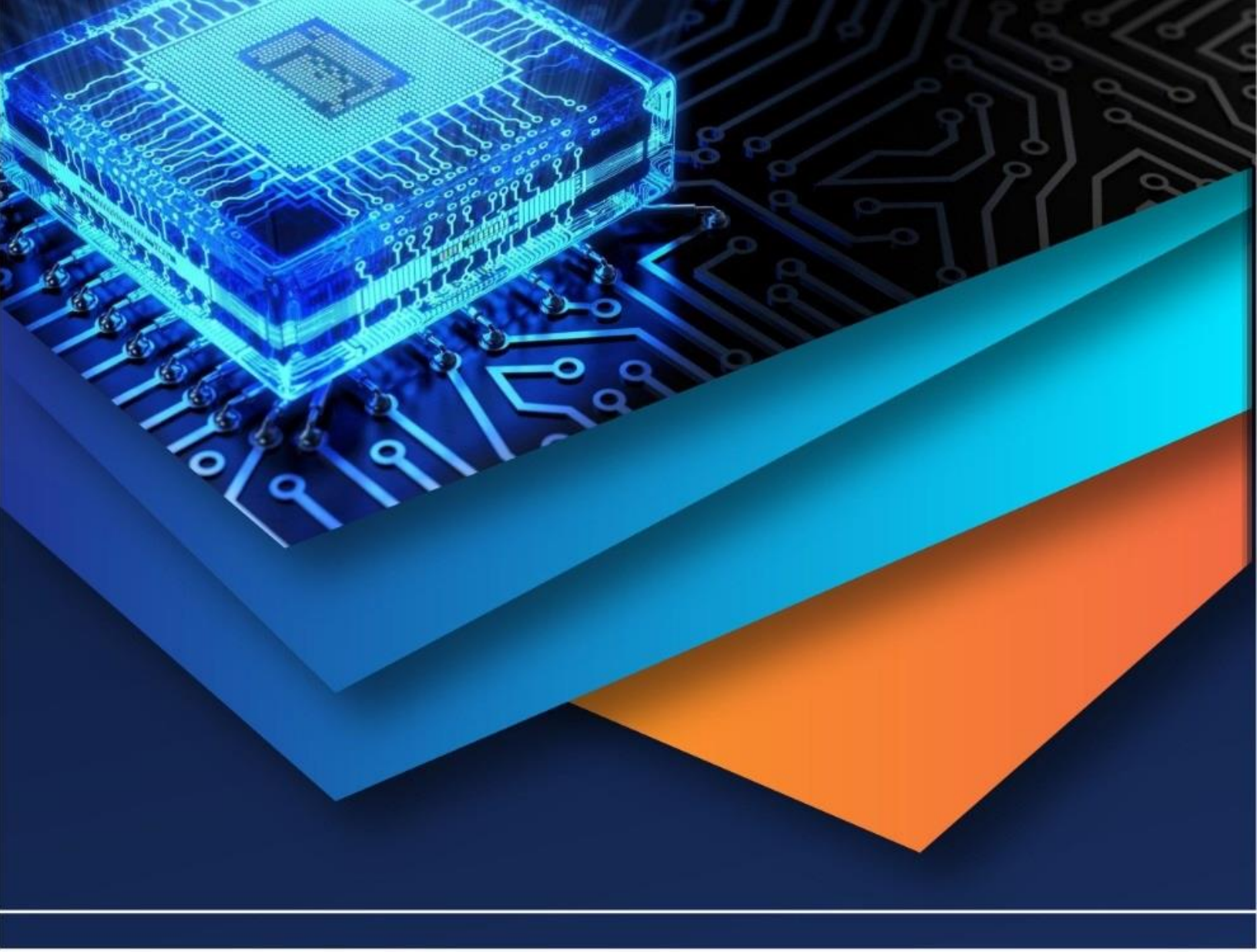
[7] Karlof[1] C, Wagner[2] D "Secure routing in wireless sensor networks : Attacks and Countermeasures" Ad hoc network Journal(Elsevier) 1(2-3) (2003) 293-315.

[8] Jaydip Sen[1] "A survey on wireless sensor network security" International journal of communication network and information security, Vol. 1 no. 2, Aug 2009.

[9] C. Karlof, N. Sastry, and D. Wagner."TinySec: A Link Layer Security Architecture for Wireless Sensor Networks", SenSys '04. Pages 162-175. November 3-5.

[10] T. Park and K. Shin. "LiSP: A Lightweight Security Protocol for Wireless Sensor Networks". ACM Transactions on Embedded Computing Systems, Vol 3, No. 3, Pages 634-660, August 2004.

[11] A. Perrig, J. Stankovic, and D. Wagner."Security in Wireless Sensor Networks", Communications, ACM, 47(6):53–57, 2004.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY