iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** IV **Month of publication:** April 2019

DOI: https://doi.org/10.22214/ijraset.2019.4119

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

Overhead Assessment in WSN

Syeda Gauhar Fatima[1], Syeda Kausar Fatima[2] , Mohd Merajuddin[3]
[1]*Professor ECE dept, Deccan College of Engineering and Technology, Darussalam, Hyderebad.*
[2]*Research Scholar ECE dept. , JNTUH, Kukatpally, Hyderabad*
[3]*Assistant Professor EIE dept, Deccan College of Engineering and Technology, Darussalam, Hyderabad*

Abstract: There has been a extensive growth in the area of wireless sensor networks mainly because of the marvelous possibility of using it in a wide spectrum of applications such as home automation, wildlife monitoring, defense applications, medical applications and so on. However, due to the intrinsic limitations of sensor networks, commonly used security mechanisms are hard to implement in these networks. For this very reason, security becomes a critical issue and these networks face a wide variety of attacks right from the physical layer to application layer. This paper present a survey that investigates the overhead due to the implementation of some common security mechanisms viz. SPINS, TinySec and MiniSec and also the computational overhead in the implementation of three popular symmetric encryption algorithms namely RC5 AES and Skipjack.
Keywords: Wireless Sensor Networks, Security Mechanisms, Symmetric Encryption, AES, RC5, Skipjack.

I.INTRODUCTION

Wireless Sensor Networks are comprised of large number of tiny sensor nodes, commonly known as motes. These devices have the ability to sense their environment, process the collected data and transmit them over air to nearby devices. These capabilities make them suitable for monitoring the real world environment in which they are deployed. The sensor nodes are basically cheap devices and hence could be deployed in very large numbers that could cover vast regions. However, the nodes in wireless sensor networks severely lack essential resources such as memory, processing power, energy and hence security mechanisms employed in traditional networks are not suitable for WSN. As a result of which these networks face a variety of attacks such as physical tampering, node fabrication attacks, eavesdropping, hello flood attacks, eavesdropping and so on. This has motivated researchers to come up with various security mechanisms that are suitable for these resource constrained networks. Number of secure communication protocols [8,9,10], secure routing protocols [1,2,3,4] data aggregation protocols [5,6,7] have been proposed over the years by the research community. However, these security mechanisms impose additional overhead on the already resource constrained network. Hence the security mechanisms and cryptographic primitives used to implement these mechanisms have to be chosen with extreme caution. The remainder of this paper is organized as follows. Section2 discusses the resource constraints faced by WSNS. Section 3 discusses major security goals of WSN. This paper studies three very popular security protocols: SPINS [8], TinySec [9] and MiniSec [10]. Important features of these protocols are described in section 4. The result of these studies in terms of overhead is discussed in section 5. Comparison of computational overhead of three popular symmetric algorithms namely RC5, AES and Skipjack is presented in section 6. Finally section 7 concludes the paper.

II.CHALLENGES IN WSN

Wireless Sensor Networks faces a number of challenges most of which is unique to them. Stringent resources are one of the primary challenges faced by these networks. Sensor nodes that form the WSN are physically very small in size which is the main reason for the resource constraints and hence a major limitation for these networks.
Additionally they also face a host of other challenges discussed in this section.

A. Energy Constraints

Energy is one of the most expensive resource as far as wireless sensor networks are concerned and hence the biggest constraint. Most of these devices are battery powered and are deployed in areas such as deep forests, oceans etc where recharging is not practically possible. Some of these devices are also solar powered but still batteries are the main energy sources and hence should be conserved. Energy is spent both for computation and data transmission. Transmitting a single bit of data requires as much as energy in executing 800-1000 instructions[7] and therefore data transmission consumes the largest chunk of available energy.

B. Memory Constraints

Sensor devices typically consist of very small amount of storage space. For instance, a commonly used mote TelosB has only 10K RAM, 48K program memory and 1024K flash storage[8] . Almost half of this available memory is consumed by the resident operating system. Memory is also required for storing applications, data sensed by the devices and for storing intermediate results of processing. Hence, not much memory is left for implementing security primitives and therefore heavy weight cryptographic algorithms are not suitable for these platforms.

C. Unreliable Communication

Communication in WSN takes place as a result of the nodes transmitting packets to the nodes which are within their communication range, packets hopping from one node to another towards the gateway. This communication follows a connectionless protocol and hence there is always the threat of lost or dropped packets and congested networks. Also the broadcast nature of the communication adds to the unreliability in communication.

D. Limited Post Deployment Knowledge

The sensor nodes are deployed in an adhoc manner usually by aerial scattering and hence not much information is available about the topology or structure of the network. This is especially true in the case of networks that are exceptionally large and deployed in large fields. Lack of any a-priori knowledge about the deployment poses a number of challenges.

E. Remote Management

Sensor nodes are being largely employed in areas where the operations of these devices cannot be attended physically.[11,12] They remain unattended and have to be handled remotely which make the task of providing security quite challenging. Also it makes these networks highly vulnerable to physical attacks.

F. Extensive Scale

In applications such as forest fire monitoring, highway traffic monitoring and management, ocean monitoring, the number of nodes deployed is in the range of thousands or even millions. The sheer size of these networks makes it difficult to manage them efficiently and ensuring security becomes a real challenge.

III.SECURITY GOALS IN WSN

Even though wireless sensor networks face challenges that are most unique to these kinds of resource starved networks, yet the primary security goals or requirement of a WSN is no different from that of a old-style network. The three primary goals are discussed below.

A. Confidentiality

Confidentiality requirement implies that the data that is being sensed and transmitted by these networks should only reach and be understood by the intended recipient and nobody else. No third party should be able to access the information unless they are authorised to do so. This is one of the most critical of the security requirement as these networks are typically employed in applications that deal with highly sensitive data as in medical and traffic monitoring, emergency response management, defence management and battlefield monitoring.

B. Integrity

There are certain applications where the information being transmitted may not be very sensitive in nature and therefore confidentiality is not a major concern rather what is more important is to determine and verify that the information has not been modified or altered while in transit. The data as seen by the recipient should be the same as sent by the source. In traditional networks, mechanisms such as Message Authentication Codes (MAC) and hashes are employed to ensure this security requirement.

C. Availability

It is necessary to ensure that the services of WSN are available uninterrupted even in wake of attempted attacks to bring down the network. Attackers may try performing denial of service attacks or attacks on the base station so as to make the network unavailable to the users. A robust network should be able to handle such attacks and still provide services to users.

D. Authenticity

It is important to verify the authenticity of the source nodes from where the data is believed to have originated. It is possible for an attacker to fabricate false packets and spoof the source address so as make it appear like coming from a legal node in the network. To be able to verify the source of information correctly is one of the crucial requirements in any network, be it a traditional network or a WSN.

E. Data Freshness

In wireless sensor networks, critical decisions are made based on the data collected and communicated by the sensor nodes. Decisions are usually based upon the aggregate of all data collected by the participating nodes and hence it is necessary that the data is not stale. Synchronised counters at both ends or nonce are generally used to ensure data freshness.

IV.SECURITY PROTOCOLS

This section discusses the important features of three popular WSN security protocols namely SPINS, MiniSec and TinySec [8, 9, 10]. All of these security protocols are built over the TinyOS operating system.

A. SPINS

It consists of two secure building blocks, one which handles data confidentiality, two party data authentication, data freshness and a second one that ensures authenticated broadcast called SNEP and µTesla respectively [8]. This security protocol for the resource constrained wireless networks uses the same block cipher for implementing its various cryptographic primitives so that the code could be reused and thereby saving precious storage space. SNEP provides confidentiality by encrypting the data to be transmitted and uses an optimized version of RC5 from OpenSSL to do so [8]. Furthermore to ensure semantic security this protocol uses the concept of a counter at both sides that ensure that the same plain text is encrypted to a different cipher text each time. But instead of transmitting these counters, SNEP requires that the sender and receiver maintain the counter at both sides. It does so to save the energy required for transmitting the counters. However, in situations where the counters at both sides fail to remain synchronized in the event of packet losses, an expensive counter resynchronization protocol is required.

µTESLA on the other hand take care of authenticated broadcast. In traditional networks, authenticated broadcast is implemented by means of uneven mechanism. However, they are impractical to be used in the severely resource constrained wireless networks. µTESLA manages to achieve the same affect by using a symmetric algorithm. In order to achieve irregularity, this protocol requires that the keys needed for decryption be provided by the broadcasting device to the nodes after a certain period of programmed delay [8]. This requires that the base station, which is usually the broadcasting party and the nodes be time synchronized although loosely.

B. Tiny Sec

It is the first fully implemented security architecture for wireless sensor networks [9]. TinySec has two modes of operation, one which encrypts the data and moreover authenticates the packet by computing the MAC over the encrypted data and header called TinySec-AE and the second one called TinySec-Auth which only authenticates the packet by figuring the MAC and no data encryption takes place.

TinySec uses the cipher block chaining (CBC) mode of operation with SkipJack as its underlying block cipher and an 8 byte Initialization Vector (IV) to introduce randomization and hence ensure semantic security. However, unlike SPINS which does not send the counter with the packet, TinySec-AE transmits the 8 Byte IV along with the packet. But it does so in such a way that it incurs an overhead of 5 bytes for this mode and for TinySec-Auth it incurs an overhead of just 1 byte.

C. Mini Sec

Similar to the above two protocols, MiniSec also has two modes of operation. One of which secures point to point communication or unicast mode of communication and the second one designed for multicast mode of operation called MiniSec-U and MiniSec-B respectively [10]. The implementation of MiniSec on Telos platform is publicly available.

MiniSec-U makes use of Offset CodeBook (OCB) which is a block cipher mode of operation and uses Skipjack as the underlying block cipher [10]. OCB mode of operation has the added attraction of performing authenticated encryption in a single pass of plain-text. MiniSec-U also uses an incrementing counter as IV to ensure semantic security but it uses an approach that lies between SPINS and TinySec. SPINS that does not transmit the IV at all and TinySec which transmits the entire IV, MiniSec adopts a novel

approach of sending few bits of IV and also uses an implicit counter resynchronization protocol that ensures that up to 2^x-1 number of packets lost, no expensive resynchronization protocol is required where x being the number of bits of IV being transmitted. MiniSec-B uses Bloom Filters and loose time synchronization to achieve authenticated broadcast [10]. The Bloom filter is a space efficient data structure and is well suited for sensor nodes [13]. It also uses a sliding window approach to protect against replay attacks.

V.COMPARISON OF PACKET OVERHEAD

In this section we compare the increase in size of packets and the resultant energy overhead of the three protocols discussed below. The comparisons are done with respect to a TinyOS packet with no security implementations. The following figures shows the packet formats of some of the protocols discussed.

2	1	1	1	24	2
Dest	AM	Len	Grp	Data	CRC

a) TinyOS Packet Format

2	1	1	1	24	2
Dest	AM	Len	Grp	Data	CRC

b) TinySec-AE Packet Format

2	1	1	24	4
Dest	AM	Len	Data	MAC

A. Tiny Sec-AUTH Packet Format

2	1	1	2	24	4
Dest	AM	Len (3 bit IV)	Src	Data	MAC

d) MiniS ec-U Packet Format

2	1	1	2	24	4
Dest (4 bit ctr)	AM	Len (3 bit ctr)	Src	Data	MAC

B. MiniSec-B Packet Format

Fig. 1. Packet format for the three security protocols and TinyOS which is taken as the reference. The numbers represent the size of the fields in Bytes.

As mentioned in the beginning, every single bit transmitted consumes additional energy and below is a table depicting the overhead in energy consumed due to the additional bytes transmitted for security implementation and the overall percentage overhead in transmission energy for each. The overhead is calculated with respect to the standard TinyOS network stack [10].

Table 1. Comparison of Packet and Transmission Overhead

Protocol	Payload	Packet Overhead	Security Overhead	Total	Energy (mAs)	% Increase
TinyOS	24	7	0	31	0.034	-
SNEP	24	15	8	39	0.0415	22.2
TinySev -AE	24	12	5	36	0.0387	13.9
MiniSe	24	10	3	34	0.368	8.3

According to this table, MiniSec manages to consume the lowest energy in transmitting the packets by keeping the packet overhead to an optimally minimum level.

VI.COMPARISON OF COMPUTATIONAL OVERHEAD OF RC5, AES128, SKIPJACK

Asymmetric encryption algorithms are highly inappropriate to be used in sensor networks because they are typically designed for powerful processors and requires extensive amount of computation and memory for storing keys and intermediate results. The memory of a typical sensor node is not even capable to hold the keys of commonly used uneven algorithms most of which are 1024 bits or higher. Hence the research communities have resorted to symmetric algorithms such as RC5 [16], AES [15,17] and Skipjack [18] for providing security to these networks. SPINS uses an optimized version of RC5 while both TinySec and MiniSec uses Skipjack as its underlying block cipher. Hence in this section, we discuss the computational overhead of these algorithms. Also since Skipjack uses only a 80 bit key and the world is moving towards higher bit keys to ensure security in the long run, this section also analyses AES128 which could be a suitable substitute to Skipjack.

RC5 allows a variable length block size (32, 64, 128 bits) and a variable length key size (up to 2040 bits) and the number of rounds can go up to 255 [14]. AES on the other hand uses a fixed block size of 128 bits and the keys could be either 128, 192 0r 256 bits and accordingly the number of rounds is 10, 12 and 14 respectively. Unlike these two algorithms, Skipjack uses a fixed length block of size 64 bit and an 80 bit key and two rounds named Round A and Round B each of which is executed 16 times in a specific order making a total of 32 cycles. The following table summarizes these parameters as used in the security mechanisms discussed in section 4.

Table 2. Block Cipher Parameters

Algorithm	Block Size(bits)	KeySize(bits)	#Rounds
RC5	64	128	18
SkipJack	64	80	32
AES	128	128	10

The number of CPU cycles per byte for these three block ciphers implemented on ATmega128 processor is shown in the following table.

Table 3. CPU Cycles for Encryption

Algorithm	Block Size(bits)	Cycles/Byte	Cycles/Block
RC5	64	712	5696 [19]
SkipJack	64	186	1488 [20]
AES	128	204	3264 [20]

The energy (E) required by symmetric block ciphers for encryption of N bits of plain text is given by

$$E= (P \times C/f) \times N/u \; . \qquad (1)$$

Where P and f are the power and frequency of the CPU and C is the number of block cycles needed to perform encryption of a block of size u [22]. Table V gives the computational energy cost of encryption operation by the three block ciphers [17].

Table 4. Computational Energy Requirement

Cipher	Energy for Encryption of 128 bit block
RC5	42.5 µJ
SkipJack	31.8 µJ
AES	36.5 µJ

The table shows that the energy efficiency of Skipjack is above the other two ciphers, but from a security point of view AES is considered stronger that Skipjack which has been proved weak against cryptanalysis [21,22].Hence AES seems to be a good choice from a security and energy efficiency point of view.

VII.CONCLUSION

In this paper, we have conducted an extensive research of various types of attack that can be launched against a wireless sensor network. The paper also explores three very popular security protocols and discusses the overhead as a result of their implementation. A study of three different block ciphers and their computational overhead is also conducted. We conclude from the study that of the three security protocols studied MiniSec seems to far better than its counterparts and AES is a good choice as the underlying block cipher.

REFERENCES

[1] Deng, R. Han, and S. Mishra, “INSENS: Intrusion-tolerant routing in wireless sensor networks”, Technical Report CU-CS-939-02, Department of Computer Science, University of Colorado at Boulder, November 2002.

[2] B. Karp and H.T. Kung,“GPSR: Greedy perimeter stateless routing for wireless networks”, In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, pp. 243-254, ACM Press, 2000.

[3] P. Papadimitratos and Z.J. Haas, “Secure routing for mobile ad hoc networks”, In Proceedings of the SCS Communication Networks and Distributed System Modeling and Simulation Conference (CNDS 2002) 2002.

[4] S. Tanachaiwiwat, P. Dave, R. Bhindwale, and A. Helmy, “ Routing on trust and isolating compromised sensors in location-aware sensor networks”, Poster paper , In Proceedings of the 1st International Conference on Embedded Networked Sensor Systems, pages 324-325, ACM Press, 2003.

[5] L. Hu and D. Evans, “Secure aggregation for wireless networks”, In Proceedings of the Symposium on Applications and the Internet Workshops, 2003, pp. 384, IEEE Computer Society, 2003.

[6] N. Shrivastava, C. Buragohain, D. Agrawal, and S. Suri, “Medians and beyond: New aggregation techniques for sensor networks, In Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, pp. 239-249, ACM Press, 2004.

[7] B. Przydatek, D. Song, and A. Perrig, “SIA: secure information aggregation in sensor networks, In Proceedings of the 1st International Conference on Embedded Networked Systems (SenSys’03), New York, ACM Press, 2003, pp. 255-265.

[8] A. Perrig, R. Szewczyk, V. Wen, D.E. Culler, and J.D. Tygar, “SPINS: Security protocols for sensor networks”, Wireless Networks, Vol.8 , No. 5, pp. 521-534, September 2002.

[9] C. Karlof, N. Sastry, and D. Wagner, “TinySec: a link layer security architecture for wireless sensor networks”, In 2nd ACM Conference on Embedded Networked Sensor Systems (SensSys’04), Baltimore, MD, November 2004, pp. 162-175.

[10] Mark Luk, Ghita Mezzour, Adrian Perrig, Virgil Gligor “MiniSec: A Secure Sensor Network CommunicationArchitecture”, IPSN'07, April 25-27, 2007, Cambridge, Massachusetts, USA. ACM 2007.

[11] Pathan, A.S.K.; Hyung-Woo Lee; Choong Seon Hong, “Security in wireless sensor networks: issues and challenges” Advanced Communication Technology (ICACT), year 2006.

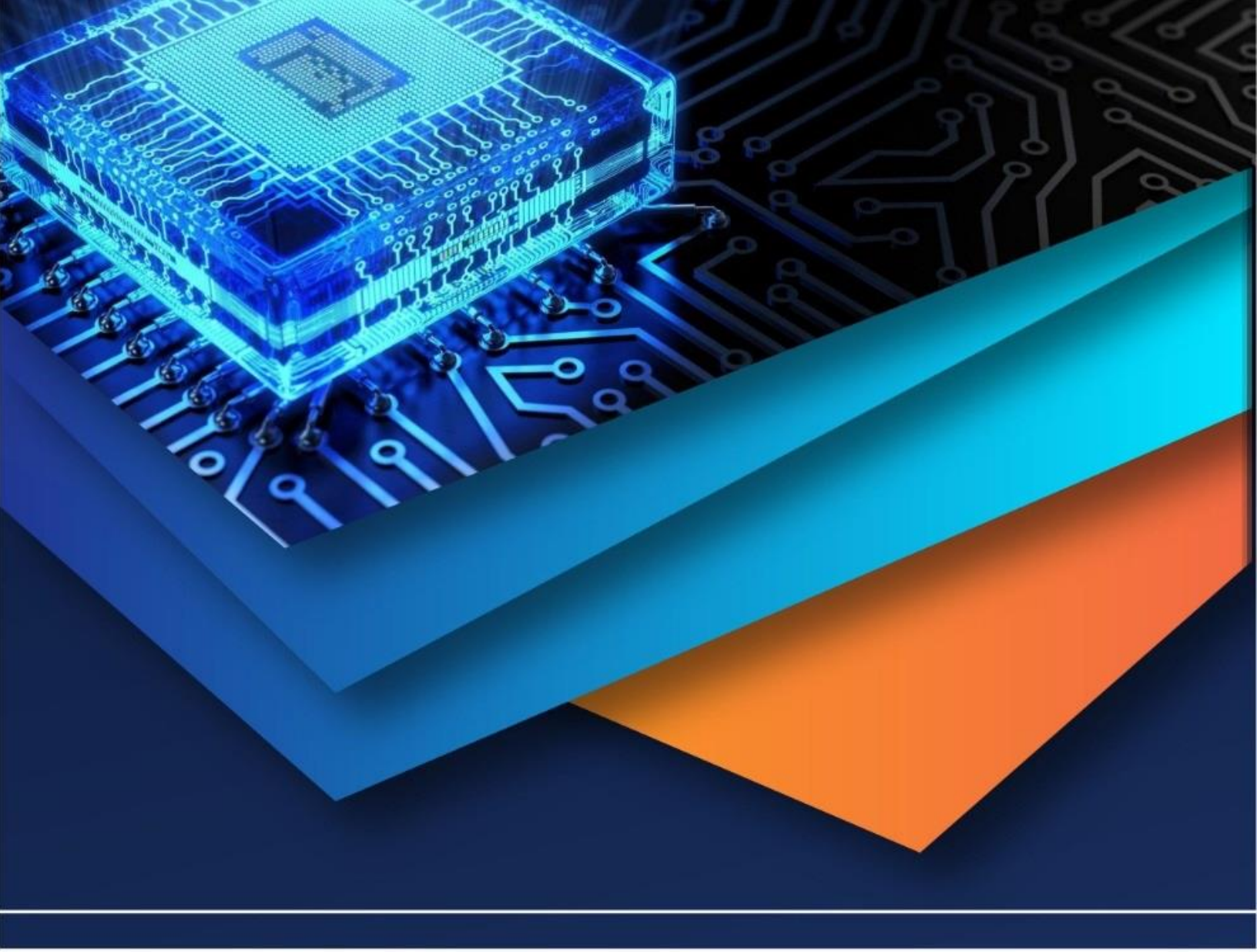
[12] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks”, IEEE Communications Magazine, Vol. 40, No. 8, pp. 102-114, August 2002.

[13] B. Bloom. Space/time trade-offs in hash coding with allowable errors. In Communications of the ACM, July 1970.

[14] R. Rivest, "The RC5 encryption algorithm", in Proceedings of the 1994 Leuven Workshop on Fast Software Encryption, pages 86-96, Springer-Verlag, 1995.

[15] National Institute of Standards and Technology (NIST), “Advanced Encryption Standard (AES),” Federal Information Processing Standard (FIPS) 197, Nov. 2001

[16] "Skipjack and KEA algorithm specifications" National Institute of Standards and Technology, Mai.1998.
[17] Yee Wei Law, Jeroen Doumen and Pieter Hartel "Survey and Benchmark of Block Ciphers for Wireless Sensor Networks" ACM Transactions on Sensor Networks Volume 2 Issue 1, February 2006
[18] Xueying Zhang, Howard M. Heys, and Cheng Li "Energy Efficiency of Symmetric Key Cryptographic Algorithms in Wireless Sensor Networks"
[19] M.Razvi Doomun and KMS Soyjaudah "Analytical Comparison of Cryptographic Techniques for Resource-Constrained Wireless Security" International Journal of Network Security, Vol.9, No.1, PP.82–94, July 2009.
[20] L.Granboulan,"Flaws in Differential Cryptanalysis of Skipjack,"Lecture Notes in Computer Science 2355: Fast Software Encryption,Springer-Verlag, pp. 81-98, 2002.
[21] L. R. Knudsen, M. J. B. Robshaw and D. Wagner, "Truncated Differentials and Skipjack," Lecture Notes in Computer Science 1666: Advances in Cryptology – CRYPTO'99, Springer-Verlag, pp. 790, 1999.
[22] Kai Xing , Shyaam Sundhar, Rajamadam Srinivasan , Manny Rivera , Jiang Li , Xiuzhen Cheng , "Attacks and Countermeasures in Sensor Networks: A Survey" 2005 Springer.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY