iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** V **Month of publication:** May 2015

DOI:

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Information Security in WSN's using AES

Mr. Atul Singh[#1], Dr. Rajashekarappa[*2], Dr. S. R. Biradar[#3]
[#1] *M. Tech in Information Technology, ISE Department SDMCET, VTU, India*
[#2] *AP, ISE Department*, SDMCET, VTU, India
[#3]*Professor, ISE Department, SDMCET, VTU, India*

Abstract— Wireless sensor networks simplify the collection and analysis of data from multiple locations. The self-organization capabilities of wireless sensor networks enable rapid deployment of target tracking and intrusion detection in hostile environments. However, sensor nodes deployed in adversarial environments, it must be fortified against various attacks. This thesis examines the threats against attacks and countermeasures to protect their communications with origin integrity and data integrity. This thesis solves the data security problem in wireless sensor networks deployed for surveillance and target tracking by application of appropriate security mechanisms. Cryptography provide the data security and the* multi-hop transmission will reduce the power consumption.

Keywords— ***Wireless Sensor nodes, Multi-hop routing algorithm, Power-Trace***

I. INTRODUCTION

A wireless sensor network is popular and it provides solution when it is difficult or to run a mains supply to the wireless sensor node. However, the sensor nodes are spread in a hostile area, it is difficult-to-reach location and replacing the node battery can be costly and inconvenient for the sensor node application user [6]. An important aspect for the development of a wireless sensor node is ensuring that there is always enough battery energy available to power up the sensor nodes. In these cases, the use of solar energy in the wireless sensor node is an effective technique. There are various different types of energy sources that can be harvested, but the most popular is the energy generated by solar power. A solar-powered wireless sensor nodes are solution for accumulates energy over an extended period of time [2]. It provides the solution for the high computation of the sensor node processor and then sensor can perform more operation on the nodes. In cryptography processor need more consumption of energy and the high processing speed. These wireless sensor node systems spend a majority of the time in a low-power sleep to consume less power and utilize more resources. Sensor nodes are always powered by battery and harvest the energy all times, making them ideal for industrial controls, building security, intelligent and fire.

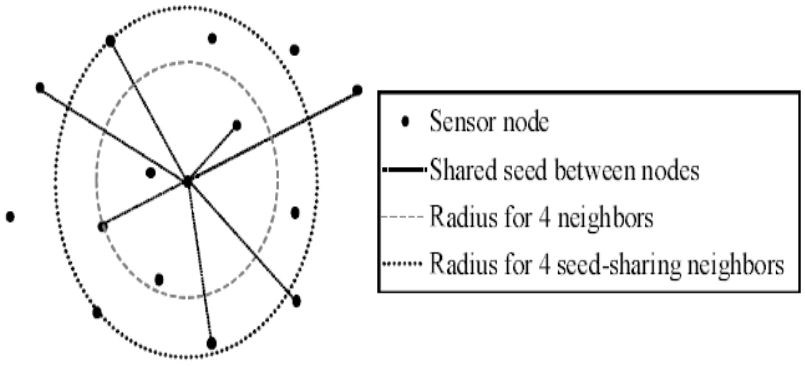


Figure.1 Sensor Nodes

WSNs have a wide and varied application; common desire features for most sensor applications include robust and reliable communications between the nodes, efficient energy consumption over the WSN's and increase the life time of the sensor nodes, scalability in terms of network size, dynamic programmability, dynamic network adaptively in response to changes in the prevailing operating conditions and low unit cost per sensor [4]. The latter invariably results in simple architectures, low processing capabilities and low memory capacities. Considering the often crosscutting design goals (e.g. energy/delay trade-off) of a particular WSN application this poses significant difficulties that differ greatly from those encountered with wireless ad-hoc networks of more capable nodes such as laptop or PDAs.

II. CHALLENGES IN WSNs

A wireless sensor network should sustain dynamic programmability, as tasks can vary in time and new tasks can become important during operation. There is a strong need for programming abstractions that simplify tasking, and for middleware that supports such programming abstractions. In general, existing programming paradigms and middleware such as CORBA [85] or ONC RPC [81] cannot be utilized in sensor networks due to limited resources, large scale of deployment, network dynamics, etc. The programmability is strictly linked to the data usability and type of service provided to the user, who should define how to mine data to provide meaningful information out of the large amount of sensorial data collected.

Quality of Service is an important issue that should be addressed carefully according to the set of applications targeted. For example, multimedia-type applications or sensor-based medical systems demand high reliability requirements and near real-time processing. For example, some ongoing experimentations with fall detection require extremely synchronized data processing between the accelerometer and a fine pressure sensor that can detect vertical variation of a few centimetres. Such applications should be supported by a real time operating system to meet deadline of tasks while the communication must possess a great packet delivery rate [1]. In contrast, other applications such as environmental monitoring might tolerate packet latency of seconds. The ultimate choice of a suitable operating system (OS) for wireless sensor networks is dictated by the application targeted [5].

Fault tolerance is one of the main challenges in wireless sensor networks that should be addressed at various layers. With respect to communication, networks might operate in lossy and hostile environments which might cause a temporal or permanent disconnection between two nodes. Fault tolerance is improved through a redundant deployment of nodes that possess abilities of self-management and self-healing. At the application layer, a mechanism of self-healing might catch array and pointer errors before they can corrupt RAM. In case of this unfortunate event, the node might decide to transmit all its data to a neighbour before rebooting. However, the central challenge is the Lifetime of wireless sensor networks. Energy resources are limited as nodes operate for long periods of time on same batteries. Energy management mechanisms increase the lifetime of a wireless sensor node, which is limited to just a few weeks or even days, depending on the type of application it is running and the size of batteries it is using. With the proper energy management, energy consumption for the same node, running the same application, can be made to last for months or years on the same set of batteries. Therefore performing medium access control (MAC) and routing protocols are key feature to extending network lifetime. This should also be associated with an acceptable packet latency and reliability of the system [6].

III. SECURITY IN SENSOR NETWORKS

Network security in sensor networks depends on the need to know what we are going to protect and what purpose we are using the sensor application. We proposed four security goals in wireless sensor networks which are Authentication, Availability, Confidentiality and Integrity.

A. Confidentiality is the ability to protect message from a passive attacker as well as active attacker, where the data communicated on sensor networks remain confidential.

B. Integrity refers to the ability to confirm the source of data, send to has not been tampered, altered or changed while it was send over the network.

C. Authentication of the data, it Need to know if the messages are from the authenticated node it claims to be from, determining the reliability of message's origin.

D. Availability is to determine if a node has the ability to use the resources and the network if it is available for the messages to move from one location to other.

IV. ATTACKs IN WSNs

Attacks against wireless sensor networks could be broadly considered from two different levels of views. One is the attack against the security mechanisms and another is against the basic mechanisms (like routing mechanisms). Previously. Sensor network security mechanisms can be divided into two categories:

Communication protocols

Key management

Network communication protocols deal with the cryptographic algorithms used to ability of availability, confidentiality, integrity, and authentication. Cryptography key management architectures handle the complexities of creating and distributing the secure keys used by communication protocols [9]. Wireless Sensor networks are vulnerable to security thread due to the broadcast nature of the sensor nods and data transmission mechanism. Furthermore, wireless networks have some more additional vulnerability because sensor nodes are often placed in a hostile area or dangerous environment where they are not physically protected. Basically wireless network attacks are classified as following two attacks like active attacks and passive

attacks.

Attacks against Privacy: The main problem in sensor network is data security, sensor networks does enable the collection of information from the various nodes. Actually, much sense information from wireless sensor networks could probably be collected through the direct or indirect medium of surveillance. Rather, sensor networks intensify the privacy problem because they make huge volumes of information easily available through remote network access. Hence, attacker need not be present physically at the deployment area. They can collect information at low-risk in anonymous manner [1].

Sinkhole attacks:

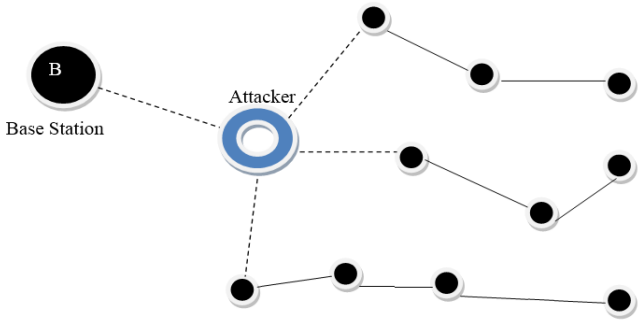


Figure. 2.Sinkhole Attack

In a sinkhole attack, the adversary's goal is to move all the network traffic to a particular area or node through an attacking node, so creating such network make metaphorical sinkhole with the adversary at the centre of the network area. Sinkhole attacks are made by making a compromised node look especially attractive to surrounding sensor nodes with respect to the network routing algorithm [8].

Wormhole attacks:

A devastating attack is known as the wormhole attack, where more than two malicious colluding sensor nodes does a virtual tunnel in the wireless sensor network, which is used to forward message packets between the tunnel edge points [11]. This tunnel establishes shorter links in the network. In which adversary documents forwards packets at one location in the sensor network, tunnels them to different location, and re-forwards them into the sensor network. In sensor network when sender node sends a message to another receiver node in the network .Then the receiving node tries to send the message to its neighboring nodes. The neighbor sensor nodes assume that the message was sent by the sender node (this is normally out of range), so they tries to forward the message to the originating node, but this message never comes because it is too far away [7].

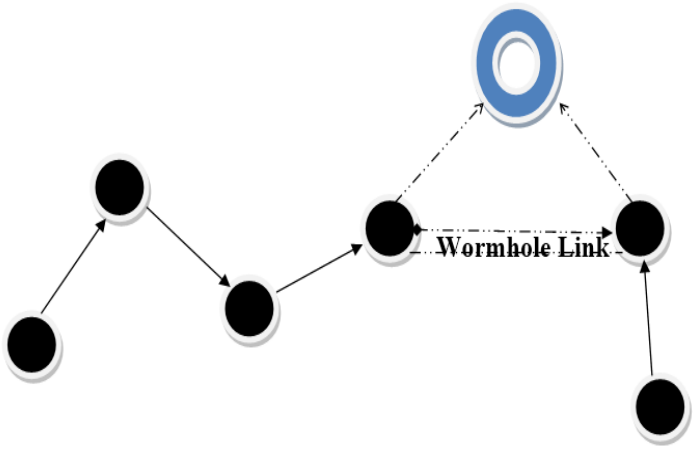


Figure.3 Wormhole Attack

V. COMMUNICATION PROTOCOLS

Protocols of medium access control can be categorized in 6 main types:

A. Carrier sense multiple access (CSMA);
B. Time division multiple access (TDMA);
C. Hybrid CSMA/TDMA;
D. Frequency division multiple access (FDMA);
E. Space division multiple access (SDMA);
F. Code division multiple access (CDMA).

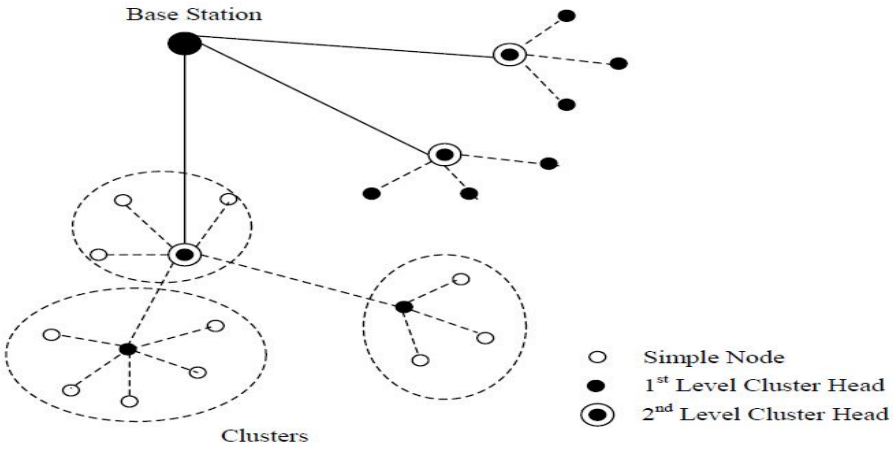


Figure.4 WSNs Nodes

In CDMA based protocols, the radio employs spread spectrum communication while concurrent transmission are still decoded correctly by assigning a specific code to each transmitter [10]. SDMA protocols are based on directional antennas or multiple antenna arrays to achieve a better signal to noise ratio towards the destination. FDMA approaches usually deploys multiple radios tuned at different frequencies to achieve better channel utilization. In general, CDMA, SDMA, and FDMA approaches utilize expensive hardware and are energy costly, and therefore they set against the requirements related to wireless sensor networks. As a result, this thesis focuses on TDMA and CSMA approaches, which are the main approaches used in WSNs [10].

VI. PROPOSED METHODOLOGY

I proposed a different hierarchical routing algorithm based on a three-tier architecture. Wireless Sensors nodes are grouped into clusters before to network operation. The cluster algorithm choose one cluster heads which has highest energy, mainly it is uses as a gateways, which has less constrained than other sensors nodes and assumed it should know the location of each sensor nodes. Sensor gateways maintain the states of the each sensor nodes and create multi-hop routes for transmitting secure data. A TDMA based MAC protocol is use for sensor nodes to send secure data to the network gateway. The network gateway informs every node about routing path in which it should listen to other nodes transmission and slots, which the node can use for its own transmission. The command node (sink) communicates only with the gateways. The sensor is assumed to be capable of operating in an active mode or a low-power stand-by mode. The sensing and processing circuits can be powered on and off. In addition both the radio transmitter and receiver can be independently turned on and off and the transmission power can be programmed based on the required range. The sensor nodes in a cluster can be in one of four main states: sensing only, relaying only, sensing-relaying, and inactive. In the sensing state, the node probes the environment and generates data at a constant rate. In the relaying state, the node does not sense the target but its communications circuitry is on to relay the data from other active nodes. When a node is both sensing and relaying messages from other nodes, it is considered in the sensing-relaying state. Otherwise, the node is considered inactive and can turn off its sensing and communication circuitry [11].

A. AES Encryption algorithms

The overall structure of AES encryption/decryption is shown in Figure

Volume 3 Issue V, May 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

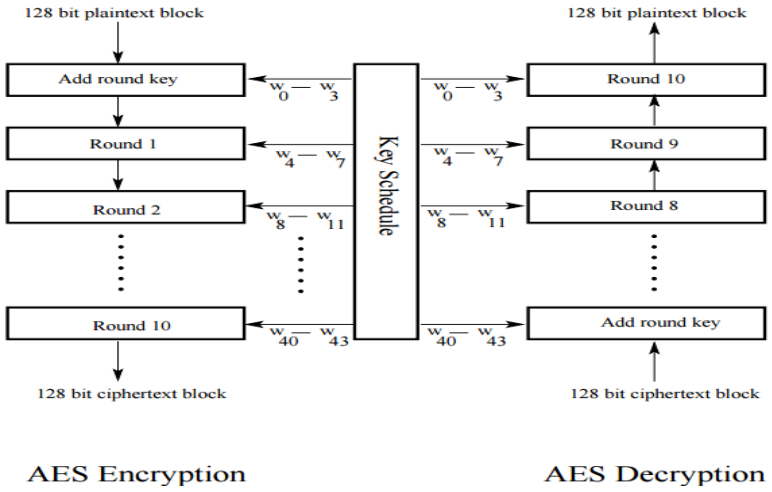


Figure 5: AES Algorithms

AES is a block cipher with a block length of 128 bits.
AES allows for three different key lengths: 128, 192, or 256 bits.
Most of our discussion will assume that the key length is 128 bits. [With regard to using a key length other than 128 bits.
Encryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.
Each round of processing includes one single-byte based substitution step, a row-wise permutation step, a column-wise mixing step, and the addition of the round key. The order in which these four steps are executed is different for encryption and decryption.

Factors	RSA	DES	3DES	AES
Created By	Ron Rivest, Adi Shamir, and Leonard Adleman In 1978	IBM in 1975	IBM IN 1978	Vincent Rijmen, Joan Daemen in 2001
Key Length	Depends on number of bits in the modulus n where n=p*q	56 bits	168 bits (k1, k2 and k3) 112 bits (k1 and k2)	128, 192, or 256 bits
Round(s)	1	16	48	10 - 128 bit key,12 - 192 bit key,14 - 256 bit key
Block Size	Variable	64 bits	64 bits	128 bits
Cipher Type	Asymmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher
Speed	Slowest	Slow	Very Slow	Fast
Security	Least Secure	Not Secure Enough	Adequate Security	Excellent Security

Table no.1 Features of Cryptography Algorithms

VII. RESULTS

A. *Comparison of AES algorithm*

Input Size (Bytes)	AES	3DES
2.5k	7	4
36k	13	6
45k	17	8
58k	23	11
70k	26	13

Table.2 Experimental Comparison of AES

Each value in AES and 3DES column is in Sec. It shows the time consumption in encryption and decryption.

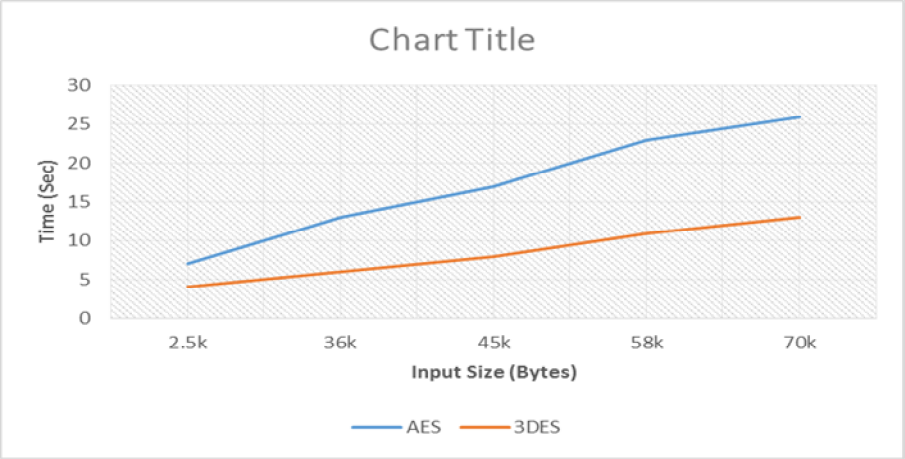


Figure. 7 Graph of Compared Value

From the above Figure. 7 shows the comparison graph between AES and 3DES, From above shows that the AES is more efficient than 3DES.

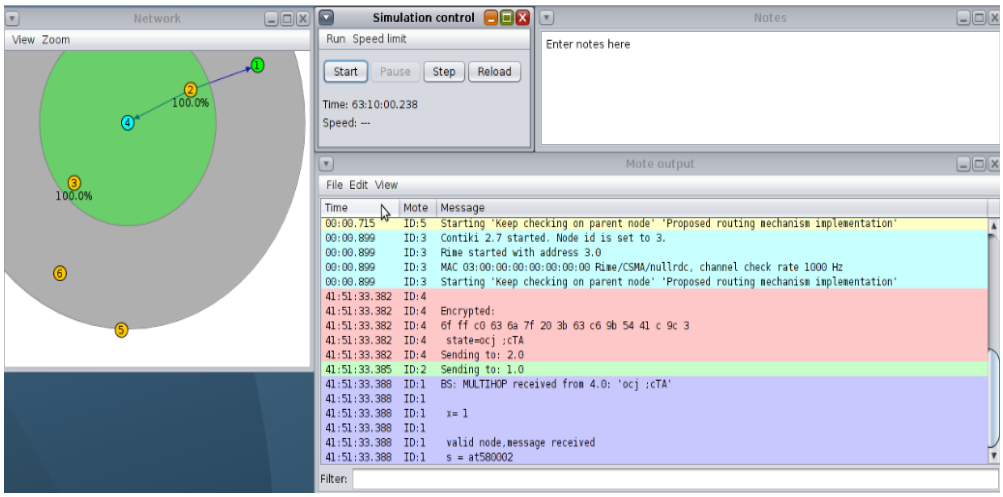


Figure. 8 Cooja Simulator Experimental detail

Figure no [6,7] shows the experimental comparison of the AES algorithm with the 3DES, its shows that the AES is better than the other cryptographic algorithm. Figure.[8] shows the how the AES algorithm implemented in Cooja Simulator. Cooja is a part of Contiki operating system and it's a light weight operating system for the wireless sensor networks. Implementation of the AES algorithm in the WSNs, it provide the secure data transfer in the sensor networks. It is very secure and efficient way to secure the sensor nodes information. It provide the authentication of nodes and authorization of the data in the sensor networks.

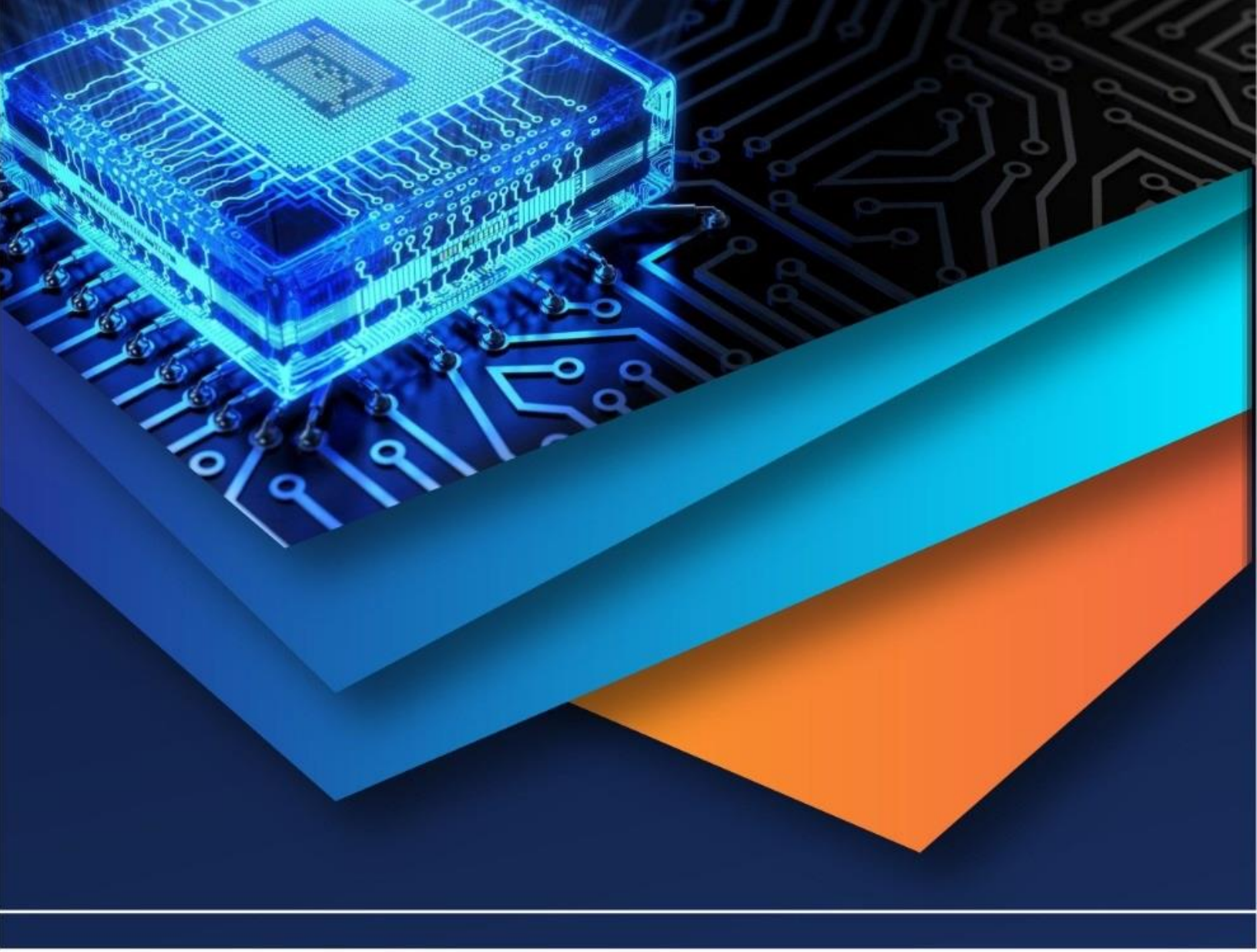
VIII. CONCLUSIONS

From the above discussion, we get to understand that the AES is an efficient and effective cryptographic algorithm that can use in sensor networks and it will secure the data transfer in the wireless Sensor networks. It is solution for the various attacks like authentication, authorization, data security and the node duplication attack.

REFERENCES

[1] Tingyuan Nie, Chuanwang Song and Xulong Zhi, "Performance Evaluation of DES and Blowfish Algorithms", IEEE International Conference on Biomedical Engineering and Computer Science (ICBECS- 2010), pp. 1-4, 23-25 Apr 2010..

[2] Behrouz A Forouzan, "Data Communications and etworking", cGraw-Hill, 4th Edition.
[3] Shashi Mehrotra Seth, Rajan ishra, "Comparative Analysis of Encryption Algorithms for Data Communication", International Journal of Computer Science and Technology, Vol. 2, Issue 2, pp. 292-294, June 2011.
[4] Daniele Puccinelli and Martin Haenggi"Wireless Sensor Networks:Applications and Challenges of Ubiquitous Sensing"IEEE Circuits And Systems Magazine third quarter 2005.
[5] K. Srinivasan, M. A. Kazandjieva, S. Agarwal, and P. Levis, "The β-factor: measuring wireless link burstiness," in Proc. 2008 ACM Conf. on Embedded Networked Sensor Systems.
[6] W.R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient Communication Protocol for Wireless Microsensor Networks", in IEEE Computer Society Proceedings of the Thirty Third Hawaii International Conference on System Sciences (HICSS '00), Washington, DC, USA, Jan. 2000,vol. 8, pp. 8020.
[7] The Contiki Operating System. [Online] http://www.sics.se/contiki/.
[8] ContikiSec: A Secure Network Layer for Wireless Sensor Networks under the Contiki operating System. Lander Casado, Philippas Tsigas. s.l. : Springer Berlin, 2009. ISBN: 978-3-642-04766-4_10.
[9] Apostolos, Pyrgelis. Cryptography and Security in Wireless Sensor Networks. [Presentation Slides] Greece : Department of Computer Engineering and Informatics, 2009.
[10] G. Abuaitah and B. Wang. Secvizer: A security visualization tool for qualnet-generated traffic traces. In Proceedings of the 6th International Workshop on Visualization for Cyber Security (VizSec), VizSec '08, pages 111–118, 2009.
[11] P. Bak, F. Mansmann, H. Janetzko, and D. Keim. Spatiotemporal analysis of sensor logs using growth ring maps. Visualization and Computer Graphics, IEEE Transactions on, 15(6):913–920, nov.-dec. 2009.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY