iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** XII **Month of publication:** December 2018

DOI:

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 6 Issue XII, Dec 2018- Available at www.ijraset.com

Mobile Node Security in Wireless Sensor Networks using Three Phase Authentication Scheme

T.C. Swetha Priya
Assistant Professor, Department of Information Technology, Stanley College of Engineering and Technology for Women, Hyderabad, Telangana, India

Abstract: ***Wireless Sensor Networks are widely used today in many applications for their effective monitoring of physical or environmental conditions and their better data gathering capacity. A Wireless Sensor node is made up of sensor nodes that communicate using signals and which support a bit of mobility. Because of the advent of Technology, this mobility can create some security issues. Because of the mobility, much efforts have to be made in locating and tracking the node's conditions which can also lead to some authentication problems. A vulnerability arises when authentication cannot be provided to a node and any node is given permission to access data. So, a better method is needed for securing the mobile nodes. The proposed system presents an efficient authentication scheme for mobile nodes using the concept of hashing and Cryptography. This method proposes a new authentication scheme for recognizing a malicious node. It provides a more efficient security scheme compared to other security solutions. The proposed system protects severe attacks on sensor nodes and helps in achieving best performance of nodes. It also adds identity and time stamp for nodes into the authentication mechanism. With this method, old nodes can be differentiated from new nodes.***

Keywords: Wireless Sensor Network, Certifying Authority, hash, Base Station, Elliptic Curve, Authentication.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have low cost and easy deployment features and so are preferably used in various fields like science and technology for collecting information regarding the behaviour of human beings and in monitoring the physical and environmental conditions related to temperature, weather, moisture, traffic, disasters, fire accidents, etc.

Wireless Sensor Network is made of sensor nodes that may vary from small to large size gathering the data at the place where they are implanted and sends the information gathered to the main sink node (Figure 1). At the sink node, the data will be analysed and data is disseminated properly. Sensor nodes are developed in such a way that they work in very strict environments. Every sensor node in the network consists of machinery like a controller, external memory, power source, transceiver, and one or more sensors. But apart from the advantages a WSN has it too suffers from some perils. Some of the constraints are with respect to size of a sensor, cost of deployment, memory, less storage capacity, energy, more power consumption computational speed and communication bandwidth.

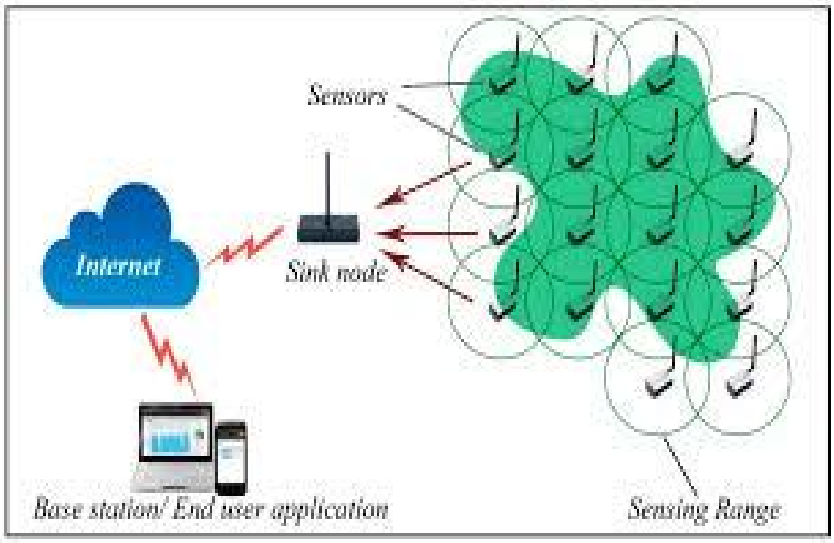


Figure 1. Wireless Sensor Network

Attacks against WSNs are classified into two types: Active and Passive Attacks. In passive attacks, attackers hide their identity and appear as valid users, can destroy the proper functioning of the network elements and interfere the transmission link to collect data. Some of the types of Passive attacks can be eavesdropping, traffic analysis, malfunctioning of nodes, node tampering and destruction.

This type of attacks cannot be detected easily. In active attacks, an intruder has the capability to modify the data. Such type of attacks can be easily detected and prevented. Some of the types of Active attacks are jamming, Denial-of-Service (DoS), Sybil attack, hole attacks like wormhole, Blackhole, Sinkhole, etc.) and flooding.

A proper access control mechanism has to be implemented and it must have 2 level security : Authentication of Nodes [14] and Proper Key Generation and Establishment[16].

This paper proposes the design and implementation of an efficient node authentication protocol for the mobile nodes in WSN. The proposed system comprises of three phases: Mobile node Initialization, Mobile node Registration and Mobile node authentication. This solution proposes a less computational overhead associated with secure cryptographic one-way hash functions.

II. WSN SECURITY REQUIREMENTS

To achieve security, the WSN has to satisfy some basic security requirements (Figure 2) :

A. Authentication

It gives assurance that the communication is authentic.It guarantees that the information sent is from the actual sender that the receiver that it has contended for. During the connection establishment itself this guarantees that the sender and receiver are authentic. Next it assures that no intermediary has involved in the communication and pretending to be a sender producing unauthorized communication

1) Peer entity Authentication: It assures authentication of peer nodes involved in the communication. It is mainly useful in connection oriented applications during data transmission phase. It also assures that no intermediary has involved in the communication and pretending to be a sender or is there any resending of data from the past communications producing unauthorized communication.

2) Data origin Authentication: It assures the authentication of source or the sender nodes involved in the communication. It cannot provide security over the redundancy or the alteration of data. It helps in the mailing applications where the source authentication plays a major role.

B. Access Control

It prevents the use of resources or data by any unwanted or malicious user under severe conditions of access[1].

C. Confidentiality

It is securing the data that is under communication from invisible attacks like passive attacks.

1) *Data Confidentiality:* It secures data from unwanted or unknown malicious users.
2) *Connection Confidentiality:* It secures data from unwanted or unknown malicious users over a connection.
3) *Connectionless Confidentiality:* It secures the user data from unwanted or unknown malicious users in a block of data.
4) *Selective-Field Confidentiality:* It secures the user data from unwanted or unknown malicious users in the selected blocks of data or over a connection .
5) *Traffic Flow Confidentiality:* It secures the user data from observing the flow of traffic over a connection.

D. Data Integrity

It guarantees that data has not been altered or is not corrupted by any of the adversaries. It also prevents unauthenticated access to network and data.

E. Nonrepudiation

It prevents source and receiver of rejecting the message that they have sent or received. It also prevents denial of information from any of the communicating parties in all aspects of data transmission.

1) *Nonrepudiation , Origin:* It assures that the message is sent by the intended source
2) *Nonrepudiation, Destination:* It assures that the message is sent by the intended receiver.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue XII, Dec 2018- Available at www.ijraset.com

Figure 2. Security Requirements for Wireless Sensor Network

III.RELATED WORK

In this section, a brief analysis of the existing authentication schemes[7][22] are as follows :

A. Secured Network Encryption Protocol

This method consists of two entities : a base station and a master key for generation of keys. Every node communicates a pair of key with base station and remaining keys are calculated from master key. Confidentiality and integrity is assured in this method. But it cannot handle DoS attacks and node authentication effectively.

B. MAC Authentication of a message

The MAC calculated is appended to the packet while transmission. If shared key encryption is considered, the MAC is calculated using shared key that is known to both sender and receiver. The sender adds a message M with shared key K and calculates MAC. At receiver side packet along with MAC, is received. Receiver also finds a MAC and compares it with whatever is sent by sender. If they match message is authenticated else the message is identified to be corrupt. But it do not identify whether the node is authenticated or not.

C. Fast Authenticated Key Establishment Method

It uses Elliptic Curve Cryptography (ECC) to provide encryption. This method was chosen because it uses small key lengths which are needed to provide ample amount of security. To authenticate keys, digital certificates are used to find whether the public key is of a authorized node or not. But this method do not provide complete security to nodes.

D. Lightweight Extensible Authentication Protocol

This method is used for switching data when nodes have different security requirements. The key levels used in this scheme are pair of keys shared between nodes, private keys, group key and cluster key. It provides security for data inside the network and data origin authentication. But this method fails to protect from Denial of service attacks and providing security to base nodes.

E. User Authentication

If a sensor node wants to exchange data with neighbouring nodes, it register with base station. After successful verification a key is generated between sensor node and sink. But the key remains same for any data transmission. But this method has some flaws. They are : less Scalability, Late authentication causes DoS attack, delayed authentication, poor performance if network has large number of nodes.

IV.PROPOSED SYSTEM

The proposed system presents an efficient node authentication protocol involving key generation and management. It is divided into 3 phases : Node Initialization, Registration of Nodes and Authentication of Nodes. The notations used in this proposed method are tabulated in Table 1.

TABLE I : Notations used

SYMBOL	NOTATION
n	Node Number
ID_n	Node Identity
K_b	Base Station Secret Key
H( )	Hash Function
k_n	Secret Keys of nodes
K_p	Base Station Public Key
E_c	Elliptic Curve
c	Prime number
P	Point on Elliptic Curve
K_b	Base Station Private Key
Q	Public Key of Node 2
C_{Noden}	Certificate of Node n
S_{Noden}	Digital Signature of Node n
T_{noden}	Timestamp of Node n
$Address_{noden}$	Address of Node n
$Ticket_{noden}$	Ticket given to Node n
||	Concatenation Operator
mod	Modulus operator

A. Node Initialization

First the sink node or base station node sends a hello message to all the nodes in the network, then the nodes will give a response to hello message. An entry is made in the routing table. This phase is repeated periodically until all the node entries are made into the routing table.

Consider there are n nodes, i.e., 1,2,3,…n with their identities as ID_1, ID_2, . . . , ID_n. Generally, integer numbers are used as the node identities. A Secret key K_b is chosen by Base Station node and a hash value, $H_p(K_b)$ is calculated p times using the chosen key by using the hash function chosen by the node. After this calculation, the base station generates n number of secret keys $k_1,k_2,k_3,…k_n$ for n nodes. Then BS calculate the hash values, $H_p(k_i)$ for all nodes p times using the secret keys of nodes $k_1,k_2,k_3,…k_n$. The responsibility of Base Station is to store the hash value of BS and the corresponding node Secret keys and hash values into each node's routing table entry.

Then an AODV request message is sent to all nodes to find the route from one node to all the other nodes. All nodes will send a route reply back to the node to inform the network about their presence in the network[5].

B. Registration of Nodes

The second phase in the proposed design is each node that wants to enter into the network has to register itself with the base Station by presenting the Certificate given by the Certifying authority(Figure 3). Here the base station will act as a Certifying Authority by adding a security timestamp. For Certificate Verification of nodes, the Base Station will choose a set of network parameters : an Elliptic Curve[2] E_c where c is a prime, Cyclic group point P on elliptic curve[2][13], Certifying Authority i.e., the Base Station Private key K_b which is not shared with anyone else and Base Station Public Key K_p [12]

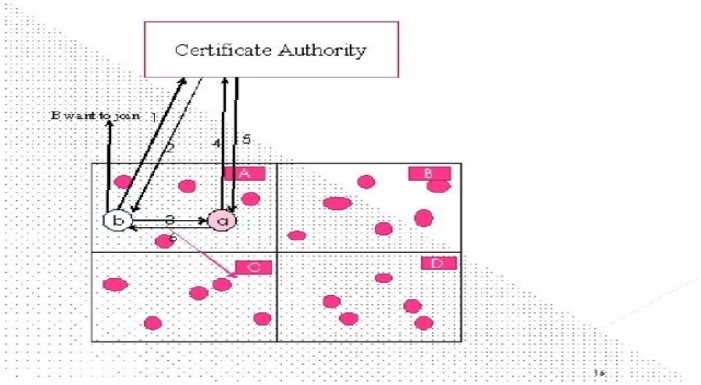


Figure 3. Node Registration with Certifying Authority Scenario

Before Certifying the nodes, they have to get registered with the Certifying Authority or the Base Station in this design specifying that they are involved in the network communication. But the Base Station will not automatically register the nodes but it just makes an entry in its database. Then, after the authentication of nodes then the registration of nodes is considered successful.

C. Authentication of Nodes

Let us consider two nodes want to communicate information, then the base station or the Certifying Authority has to generate Signature and verify the Digital Signatures of the nodes.

For Authentication between Two nodes :

1) "Node 2" requests certificate and time stamp from the certifiying authority.
2) The Certifying Authority provide a certificate along with time stamp to "Node 2".
3) "Node 2" sends the certificate to its neighbor node for authentication.
4) "Node 1" checks the time stamp by using the certificate.
5) "Node 1" checks the identity and validity for authenticating the "Node 2" by using the certificate.
6) Then, both the Node 1 and Node 2 start exchanging the information.

The algorithm used in the Proposed system is as follows :

a) Steps followed at Node 2

i) Node 2 has a Private Key k_2
ii) Node 2 computes Public Key $Q= k_2 * P$
iii) Node 2 sends its Public Key to the Base Station.
iv) Base Station provides Certificate to Node 2 that includes

$$C_{node2} =[ID_2, T_{node2}, \text{Address}_{node2}, \text{Ticket}_{node1}, k_2, Q]$$

v) Node 2 sends this message using Digital Signature to Node 1 as

$$S_{node2}=K^{-1}[H(ID_2||T_{node2}|| \text{Address}_{node2}||\text{Ticket}_{node1}||k_2|| Q]+ k_2 * C_{node2}) \pmod c$$

So the Signature is (C_{node2}, S_{node2})

Now the Node 1 checks the identity of Node 2 by verifying the signature and the validity of Time stamp.

b) Steps followed at Node 1

i) Node 1 first compares the Node 2 's Timestamp T_{node2} with its own Timestamp T_{node1}. And if $T_{node2} >= T_{node1}$ then Node 2 is identified as a new node.
ii) To authenticate new node Node 1 first compare T_{node2} with the present time t. If T_{node2} is out of date, Node 1 simply drops the message. Otherwise the Node 1 continues verifying the identity of Node 2.
iii) The Node 1 sends the certificate it has received from Node 2 to the Base Station and the Base Station will authenticate the identity by extracting the message sent by Node 2.
iv) Both the hashes are compared and if they are similar then the node is authenticated. Otherwise the node is an adversary and will not be allowed to join the network.

After Authentication, both the nodes can exchange the information using a secure method.

V. CONCLUSION

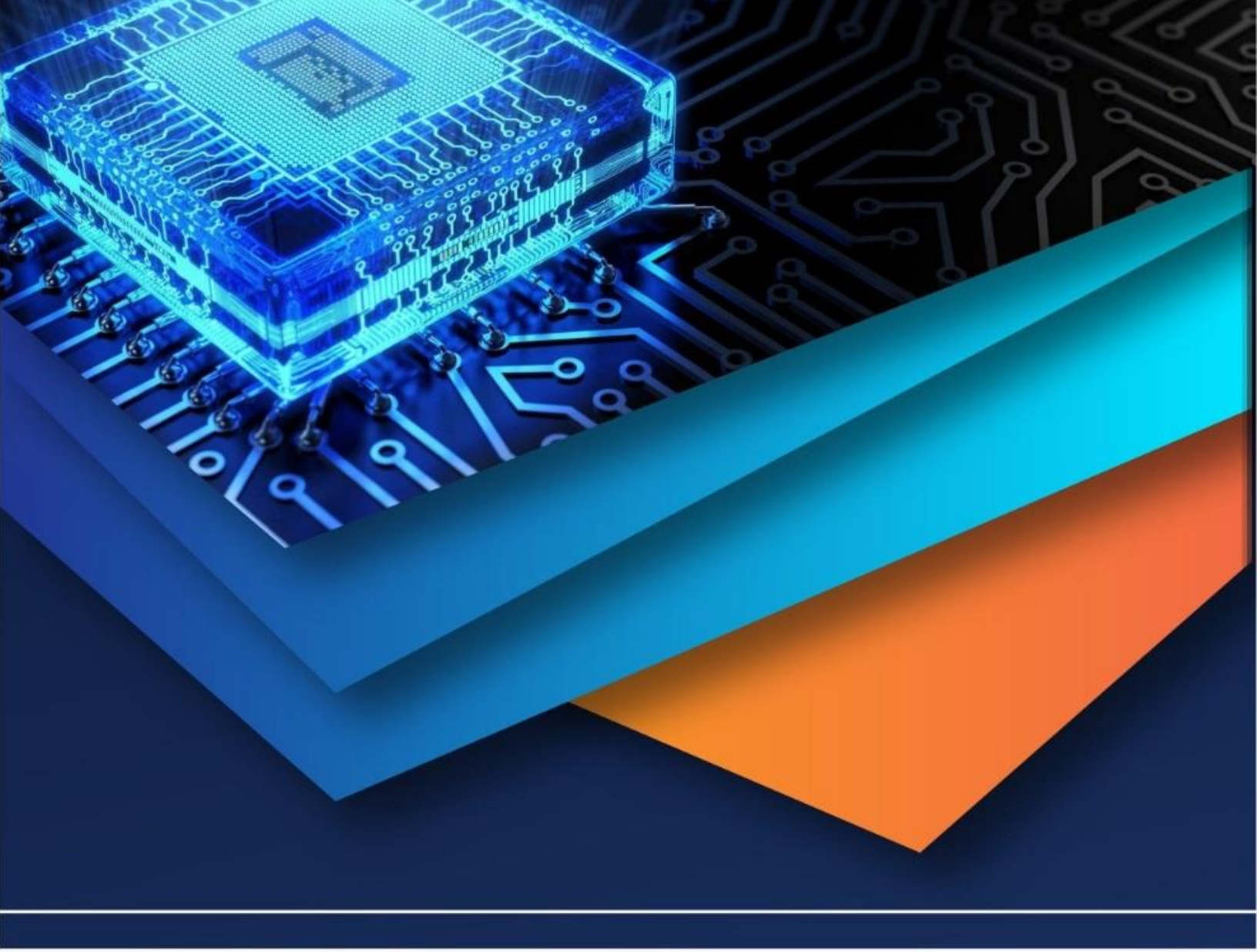
The proposed system provides security to the network by authenticating nodes [20][21]. As in this method, implementation of both the Cryptography and Hashing concepts is combined , it can provide a more efficient method of node authentication for mobile nodes. Authentication is one of the most important security requirements in WSN which helps in protecting mobile nodes. So, the proposed method mainly focuses on securing the mobile nodes by provide authentication to mobile nodes before the information is visible to the nodes. The computational overhead of this method is also less because it involves less number of computations. This reduces the energy and memory requirements of the nodes. So the proposed method is one of the efficient method in authentication of mobile nodes in Wireless Sensor Networks.

VI. FUTURE WORK

In the future researches, the node authentication for mobile nodes can be extended to the nodes in the Wireless Vehicular Area Network Systems[22] where the situation becomes more challenging in very harsh environments because in Wireless Vehicular Network the mobile nodes will be vehicles moving in a very high speed and providing high security in such environments is important. Because in such environments there will be high mobility and also it is difficult to identify the position of vehicles and the Base Station because the vehicles move from one area to another.

REFERENCES

[1] H. F. Huang, A Novel Access Control Protocol for Secure Sensor Networks, Computer Standards & Interfaces, vol. 31, pp. 272–276, (2009).
[2] H. Moon and Khan Ummer, Authentication Protocols for WSN using ECC and Hidden Generator, International Journal of Computer Applications, (0975–8887) vol. 133, no. 13, (2016).
[3] L. Lamport, Password Authentication with in Secure Communication, Comm ACM, vol. 24, pp. 770–772, (1981).
[4] Y. Zhou, Y. Zhang and Y. Fang, Access Control in Wireless Sensor Networks, Ad Hoc Networks, vol. 5, pp. 3–13, (2007).
[5] Ye, H. Lou, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," in Proc. IEEE INFOCOM, Mar. 2004.
[6] W. Zhang, N. Subramanian, and G. Wang, "Lightweight and compromise resilient message authentication in sensor networks," in Proc. IEEE INFOCOM, Phoenix, AZ., Apr. 15-17, 2008.
[7] Rashmita Rautray and Itun Sarangi " A Survey on authentication Protocols for Wireless Sensor Networkss". International Journal of Engineering Science and Technology. 2011.
[8] Perrig, R. Szewczyk, J.D. Tygar, V. Wen, D.E. Culler, SPINS: Security protocols for sensor networks, Wireless Networks 8 (September) (2002)
[9] N. Koblitz, Elliptic curve cryptosystems, Mathematics of Computation 48 (1987) 203–209.
[10] Karlof, N. Sastry, D. Wagner, TinySec: a link layer security architecture for wireless sensor networks, in: The Second ACM Conference on Embedded Networked Sensor Systems (SensSys'04), Baltimore, Maryland, November 2004.
[11] Tanveer Zia and Albert Zomaya,"A security Framework for Wireless Sensor Networks", IEEE Applications Sym-posium, Houston, Texas USA, February 2006.
[12] Ning P, Wang R and Du W (2005), ―An efficient scheme for authenticating public keys in sensor networks‖, Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, Chicago, IL, USA, pp. 58-67.
[13] Shish Ahmad,Mohd. Rizwanbeg,and QamarAbbas,‖Energy Saving Secure Framework for Sensor Network using Elliptic Curve Cryptography ‖,IJCA Special Issue of Mobile Ad-hoc Networks,pages 167-172,2012.
[14] Al-mahmud and R. Akhtar. Secure sensor node authentication in wireless sensor networks. International Journal of Computer Applications, 46(4):10–17, May 2012. Published by Foundation of Computer Science, New York, USA.
[15] J. Daemen and V. Rijmen. The Design of Rijndael: AES - The Advanced Encryption Standard. Springer-Verlag, 2002.
[16] M. L. Das. Two-factor user authentication in wireless sensor networks. IEEE Transactions on Wireless Communications, 8(3):1086–1090, 2009.
[17] T. Kavitha and D. Sridharan. Security vulnerabilities in wireless sensor networks: A survey. Journal of Information Assurance and Security, 5:31–34, 2010.
[18] J. Zhang, R. Shankaran, M. A. Orgun, A. Sattar, and V. Varadharajan. A dynamic authentication scheme for hierarchical wireless sensor networks. In MobiQuitous, volume 73, pages 186–197. Springer, 2010.
[19] Anita Daniel. D and Emalda Roslin. S, "A review on existing security frameworks with efficient energy preservation techniques in Wireless Sensor Networks," 2015 International Conference on Communications and Signal Processing (ICCSP), Melmaruvathur, 2015, pp. 0658- 0662.
[20] Yang Xiaomei and Ma Ke, "Evolution of wireless sensor network security," 2016 World Automation Congress (WAC), Rio Grande, 2016, pp. 1-5.
[21] S. Anbuchelian, S. Lokesh and M. Baskaran, "Improving security in Wireless Sensor Network using trust and metaheuristic algorithms," 2016 3rd International Conference on Computer and Information Sciences (ICCOINS), Kuala Lumpur, 2016, pp. 233-241.
[22] F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," Comput. networks, vol. 38, no. 4, pp. 393–422, 2002.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY