iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** X **Month of publication:** October 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 X, Oct 2018- Available at www.ijraset.com

Secure Route-Authentication Technique in Wireless Sensor Networks

Mallikarjunaswamy N J[1], Latha Yadav T R[2], Dr. Keshava Prasanna [3]
[1]*Assistant Professor, S.I.E.T, Tumkur. Research Scholar, Visvesvaraya Technological University, Belgaum*
[2]*Assistant Professor, A.I.T, Tumkur, Research Scholar, Visvesvaraya Technological, University, Belgaum*
[3]*Professor, Dept of CSE, C.I.T, Gubbi, Tumkur*

Abstract: ***Wireless sensor networks are self organized, autonomous, automatic discovery of services, highly scalable, reliable, Infrastructure less service. Mainly applicable in the field of defense, healthcare. A previous affairs mainly concentrate on source-authentication technique that gives the authentication to the only to the source node. Proposed work claims new route authentication method to secure both source and intermediate devices, which avoids malicious data to distribute over the internet. The application's like reprogramming in the air technique needs route authentication, which provides more secure distribution of data over a public network.***
Keywords: Route-authentication, H-MAC.

I. INTRODUCTION

Wireless sensor network(WSN) is an Ad-hoc like infrastructure less network and distributed system, in which each and every node organize itself to come up with the new system. Every node requires its own fixed frequency range to communicate with its neighbor one. Sensor nodes are unattended devices that are severely constrained in terms of battery level, memory requirement and tradeoff between security and energy consumption are major concerns for all application.

In order to secure the transmission WSN uses security requirements such as authentication, integrity, and confidentiality plays very important role in infrastructure less network. In this connection confidentiality is the conversion of original data into cipher text. Converted data is not in the form of user readable form. Which intern composition of hexadecimal values, numbers and special characters. This paper is organized as follows: Section II presents the related work and section III presents the proposed methodology. Section IV presents the rout authentication. Section V contains the conclusion.

II. RELATED WORK

Wireless sensor networking is a wide technology to observe and extract data from the outside environment and process according to the user instruction and get the results, finally store the data in memory of the device. On demand node sends the data in to the air for the betterment of the network. However, these benefits come with various limitations, vulnerabilities, and risks.

To distinguish legitimate data from intruder's data, confidentiality techniques are frequently used to verify the received data in a communication system. There are several message confidentiality schemes in wireless sensor networks have been proposed. The confidentiality techniques used in the severely constrained wireless sensor network environments.

Ayman[1] proposed hybrid cryptographic technique suitable to construct authentication scheme, which combines symmetric and asymmetric based. This approach is very suitable for the both the users of symmetric and asymmetric cryptographic users. both cryptographic operations mainly uses XOR based operations gives less computational compare to existing cryptographic operations. Both schemes mainly depend on key length and processing speed.

Haider [2] proposed secure hash based authentication, which uses the secure algorithm that combines both MD5 and SHA1 function algorithm. The 2AMD-160 compares the best on behalf of both algorithm of message digest and secure hash.

Lin xu [3] proposed bidirectional authentication scheme for the users of WSN. Which reduces propagation overhead interns of secure communication uses famous structure of markle tree protocol, which gives better and efficient way of authentication. Each node responsible for authenticating the data. it is much suitable in terms of strength of security and makes computation complex. Statistical methods very much suitable to achieve level of security. Jarrod trevathan [4] aims to generate short digital signature based on message authentication code verification done through hierarchical based cryptographic operations. This scheme proposes power, storage and computation that in turn constrain an authentication scheme. Mathematical properties are identified to enrich the security aspects in terms of providing confidentiality.

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

III. PROPOSED METHODOLOGY

Each sensor node should validate the source when it receives the reprogramming data. Source authentication is achieved with the help of MAC and HASH values.

Once the reprogramming data is prepared by base station then it will be encrypted by modified RSA. After that encrypted data will be given as input to hash function. In our work hash function is creating hash value by XOR each character in each row of the program data and XOR'ed with private key of receiver sensor node's private key. Hash & MAC function is explained below.

A. Hash Function

1) Example

a) Inputs: Private key of destination sensor, reprogram data, GPS of the receiver node

b) Output: Hash code

2) Assumption

a) Input data: program data.

b) Private Key: 75 (for sensor-20 only).

c) Hash program: MD5 or SHA1.

3) MAC function: This Mac function is used to generate the Source_MAC with the help of hash value, private key of the receiver node and total rows in the reprogramming data.

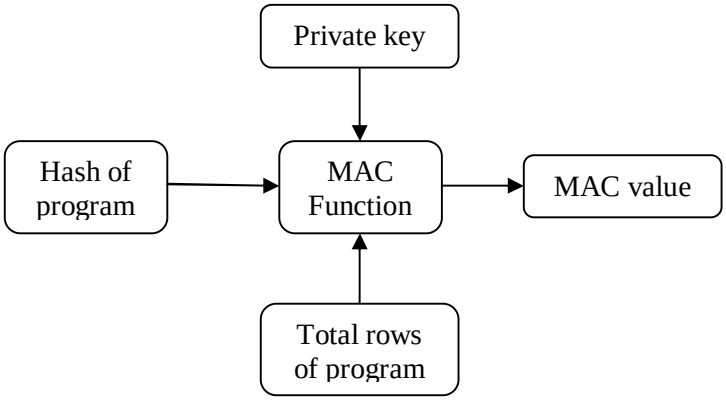


Fig 1: Generating MAC value

As depicted in Fig 1, MAC function takes the input like hash value generated by the MD5 or SHA1. Total number of lines in the program. Preloaded private key with the size of minimum of 8 bit and the maximum of 128 bit of information.

IV. ROUTE AUTHENTICATION

Once data is ready to transfer and Source MAC and HASH code generated then Base station will starts route authentication process. Route authentication also achieved by comparing MAC of source with individual MAC at each hop. By doing verification at each hop if any attack occurred in middle of the route data will be dropped in next hop itself without forwarding to next hop to avoid energy consumption.

Steps: This process will initiate after finding the path to reach receiver node.

1) Get private keys of all hops in the route.

2) Get GPS value of each hop and unique ID of the node.

3) For each hop Private key, its GPS value and ID will be XOR'ed to generate flag.

4) Based on number of hops, 'n' flags will be generated in above steps.

5) All of the flags are concatenated with '||' symbol to generate route_MAC.

A. At base station

Route message authentication code is generated at base station using private key, GPS, node ID, sending and receiving hop ID. The route_MAC length is mainly depends on the private key length of the initial setup. The Fig 2 shows the flow chart of generating route_MAC.

B. At Each Node

Route message authentication code is compare with hash message authentication code if it is matches successfully then every node successfully propagate the original form of the data without make use of more security.

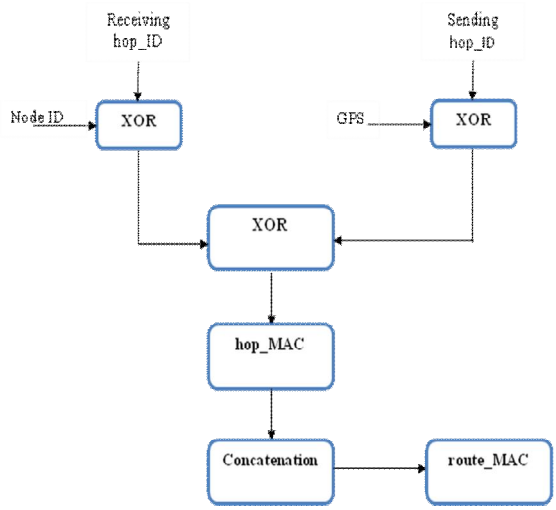


Fig 2:route_MAC at Base station

C. At Each Node

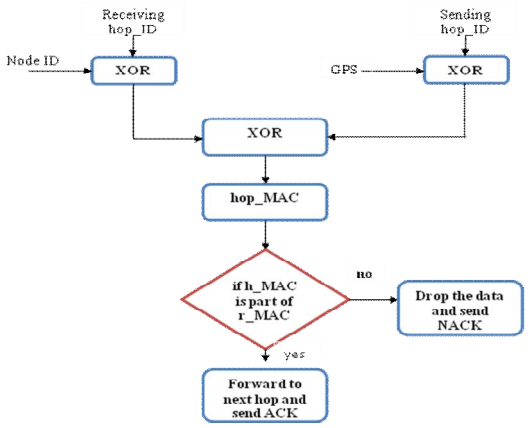
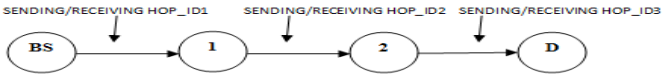


Fig 3: h_MAC at each node

D. Sample Data

The below illustrates sample date of authenticating both source and intermediate nodes.



AT Base Station:

Step 1→for node1, receiving_hopID1 ⊕ Node_ID1 ⊕ GPS ⊕ sending_hopID2= hop_MAC1.

Step 2→for node2, receiving_hopID2 ⊕ Node_ID2 ⊕ GPS ⊕ sending _hopID3 = hop_MAC2.

Step 3→for node3, receiving_hopID ⊕ Node_ID (des) ⊕ GPS = hop_MAC3.

Broadcast route MAC→ hop_MAC1|| hop_MAC2|| hop_MAC3.

AT Each Node:

Step 1→at node1, generated hop_MAC1 — Verified Route

Step 2→at node2, generated hop_MAC2 — Verified Route

Step 3→at node1, generated hop_MAC3 — Verified Route

Where
BS – Base station (source node).
D – Destination node.
1, 2 – Intermediate nodes.
Base station is the powerful node that has highest memory power and frequency range compare to the any node that play role on intermediate position in the network.

V. CONCLUSION

The proposed scheme ensures source authentication and route authentication. System generation describes the metrics that used in the research work, whereas the source authentication describes the functionality of the source entity. Finally path verification is done through route authentication process.

REFERENCES

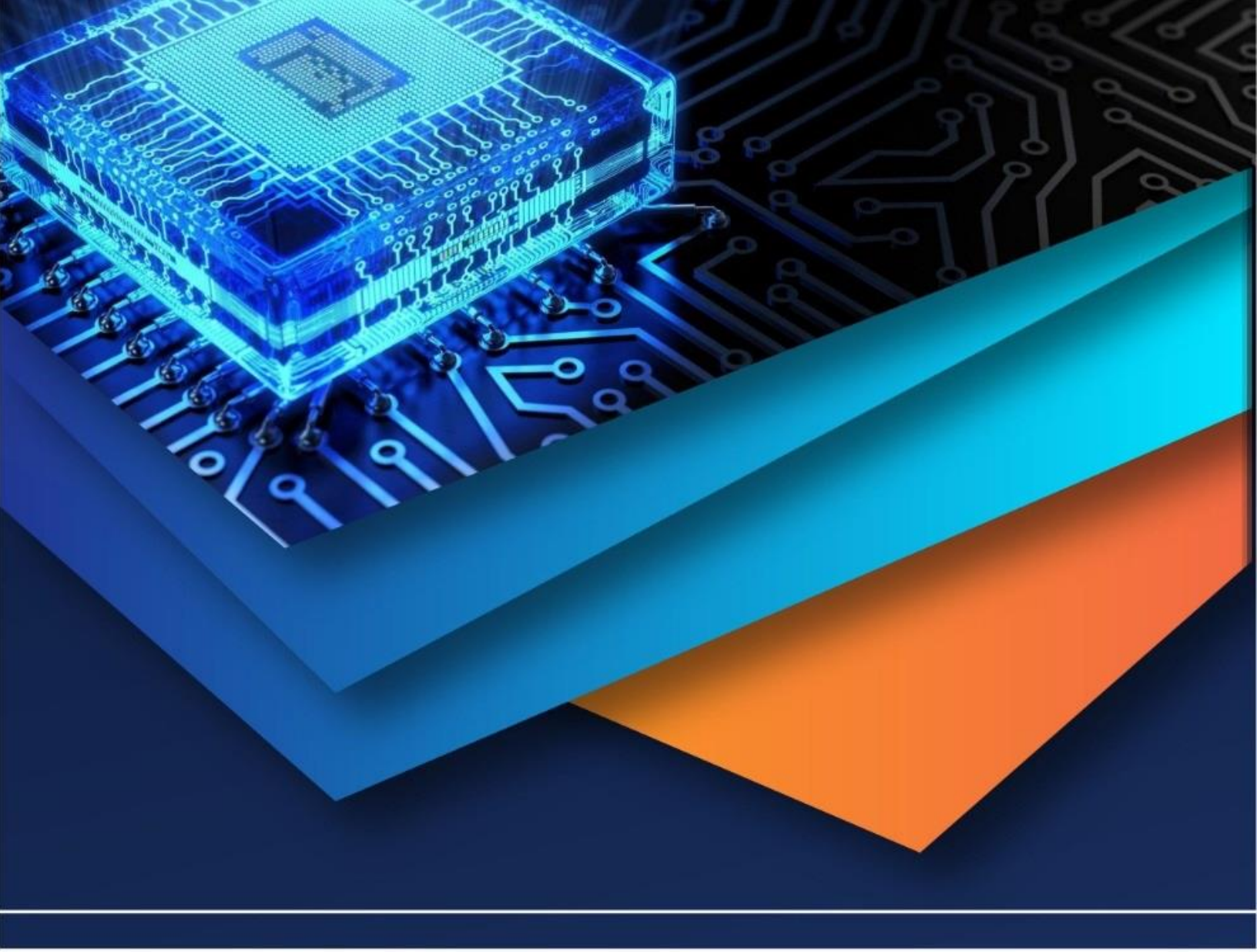
[1] Ayman Tajeddine, Ayman Kayssi "Authentication Schemes for Wireless Sensor Networks" IEEE Conference, 2014, pp. 13-16.
[2] Haider M, Hala B Adul-wahab, "Secure and time efficient Hash based Message Authentication Algorithm for Wireless Sensor Networks ," IEEE, 2014, pp. 3-7.
[3] Lin xu, mi wen, "A Bidirectional Broadcasting Authentication Scheme for Wireless Sensor Networks," 2015, pp. 200-204.
[4] Jarrod Trevathan, Hossein Ghodosi, "Efficient Batch Authentication for Hierarchical WSN" IEEE, 2017, pp. 217-222.

AUTHOR'S PROFILE

Mallikarjunswamy received BE from Visvesvaraya Technological University and M.Tech in computer science and engineering in the year 2011 and pursuing Ph.D in VTU. Teaching and Academic experience of 8 years. Life membership in Indian Society for Technical Education.

Latha Yadav T R received BE from Visvesvaraya Technological University and M.Tech in Digital Electronics in the year 2013 and pursuing Ph.D in VTU. Teaching and Academic experience of 5 years.

Dr. KeshavaPrasanna received B.E from Bangalore University and M.Tech in Information and Technology in the year 2005 and Ph.D from Tumkur University in the year 2014. Teaching and Academic experience of 18 years. Life membership in Indian Society for Technical Education (ISTE).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY