# A Scheme for Source Message Authentication

**Manasa K, Lata S H**

*Abstract*- **Messages are transmitted over the network through motes. Message authentication is essential as the channel is not secure. It helps messages to travel all along the channel safely without the intervention of the obtruder. It ensures only intended sender should deliver the message to a particular receiver. Hop-by-hop authentication is very much necessary. If intermediate motes are authenticated, no problem of rectifying the whole message at the destination. There are several message authentication techniques like symmetric-key cryptography and public-key cryptography. Symmetric encryption is catagorized into block cipher and stream cipher. Security is not reliable in case of symmetric-key cryptosystem as the sender and receiver use the same key. To overcome this problem public-key cryptography is used. It uses two keys along with the signature. Security is reliable compared to symmetric encryption. It has huge calculations and transmission cost, scalability inadequacy as a drawback. To abode these argument, the polynomial evaluation based scheme came into existence. Here the degree of the polynomial decides the threshold. If the message transmission becomes larger than this threshold, the polynomial system fails. A substitute method is to add noise to the system for making difficult to solve the polynomial equations, but even this difficulty is solved by using error correcting codes. (Hence, in this paper message authentication is established using Source Anonymous Message Authentication (SAMA) on QR factorization is proposed.**

*Index Terms* : **Channel, obtruder, public-key cryptosystem, polynomial system, Symmetric-key cryptosystem, threshold.**

## I INTRODUCTION

In wireless sensor networks, message authentication is considered as an important aspect to counteract unjustified and bad messages from transmission [1], [2]. The nodes have the capacity to sense, manipulate data and interconnect with each other through a wireless connection in a wireless sensor network. Highly small, under mechanized sensing gadget appareled with programmed computation, many specification sensing is feasible with the advent of sensor automation. As the sensors cost is low, it helps to have a network of thousands of these sensors which enhance the security and exactitude of information and also the distance indemnity. Wireless sensor networks offer information about remote structures, widespread environmental changes, etc. Secure message transmission is possible over wireless sensor networks by message authentication. The symmetric-key method has a drawback of security. The public-key method suffers from scalability and huge calculations. To overcome these problems polynomial methods have put forth. Only a limited number of messages can be forwarded using this scheme. The threshold is detected by the polynomial degree. If the message forwarding exceeds this limitation, polynomial fails to work. Hence a new scheme called SAMA (Source Anonymous Message Authentication) using QR factorization for message authentication is employed. This scheme can transmit n number of messages without any limitation. There are two types of attacks mainly. Passive attacks and Active attacks.

Passive Attacks: Here the obtruder secretly listen the information, but not alter the information. Active Attacks: Here the intruder can alter the message as per their wish.

## II LITERATURE SURVEY

In [3], symmetric-key encryption is proposed. This paper says symmetric-key encryption is faster than asymmetric-key encryption. Here generation, modification, derivation of key time is reduced. Security of message transmission lies as a drawback. In [4], the performance of symmetric-key methods and public-key methods are analyzed. The analysis comes out to be, for short messages RSA (Rivest Shamir Adleman) at 1024 bits suitable which take lesser time with high level of security. For long messages elliptic curve cryptography (ECC) is suitable as

***Manasa K,*** *Digital Electronics, GMIT, Davangere, India, Mobile No. 9980801801.*
***Lata S H,*** *Electronics & Communication, GMIT Davangere, India.*

.

the length of the key is small. Smaller length of key in ECC is considered as its drawback. Amid symmetric-key method blowfish is considered the finest cryptographic method. In [5], Here various public-keymethods like RSA, DSA, Diffie-Hellmann, ECC are analyzed. ECC is found to be better, but it seldomly used for practical applications and its mathematical operation are tough. In this paper, [6] the security in ECC is based on difficult mathematics, but its complexity is eliminated by designing the framework of ECC. In [7] bivariate polynomial scheme, the secret sharing focus on matrix concepts of digital image. In [8] among all Rivest Cipher algorithms (RC) of symmetric encryption, RC6 is found to be best, but now a days due to the advancement in computational efficacy, in coming years the RC6 will be collapsed very easily.

## III PROPOSED METHOD

The proposed method concentrates on authenticity of the message using QR factorization, message integrity, packet transmission time. Authenticity of message tells us that the message is delivered from the intended source to the recipient. Message integrity is about the message is unaltered all along the channel. The transmission time of packets over single node to hop-by-hop multiple nodes is compared.

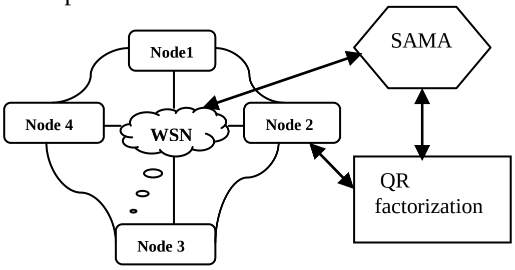

Fig 1 Architecture of the proposed system

Fig 1 shows the architecture of the proposed system. An unlimited message can be delivered hop-by-hop using Source Anonymous Message Authentication based on QR factorization over wireless sensor networks.

## IV METHODOLGY

Algorithm for time of transmission

1.According to the particular time random data is developed.
2. Set up a time.
3. Buffer the packets before transmission.
4.Message integrity and authentication is carried out.
5.Read timer is set to address the transmission time taken by each packet.

Message Integrity Algorithm

1.Header, payload and trailer are generated and connected to form a packet.
2. Set parity bit.
3. Bit errors are imported.
4.Good and corrupted packets are distinguished.

Message Authentication uses SAMA algorithm

1. Data to be sent is converted to matrix form.
2. A QR factorization is totted out.
3. A signature is verified.
4. Noise introduced in the channel.
5. Message authentication is achieved along with the noise.

The header is the additional data attached to the message which contains IP addresses of the sender and destination. The payload is the real data delivered to the destination.The trailer contains the checksum to validate the message. Header, payload and trailer is together formed a packet. This packet is delivered to the receiver from the intended along with verifying the message integrity. Authentication is done by SAMA using QR factorization. It involves signature validation, matrix multiplication to find the authenticity of a message.

## V RESULTS AND ANALYSIS

Simulink is created by mathworks. The facsimile is toted out in the Matlab 7.8 version which is amended in 2009 adopting Simulink.

Packets transmission time

For 12000 stop facsimile time, The time of packet transmission for one mote is 1.982 ms along with 5992 packet transmission. For 3 motes the time of transmission is 3.451 ms.

Message Integrity

Here good and corrupted packets all along the channel is identified. For 12000 stop facsimile time, gross packets forwarded is 1.189*10^4 with corrupted packets 17. PER (Packet Error Rate) will be 0.00143.

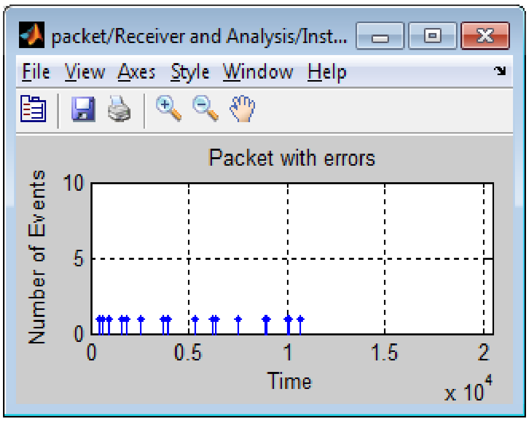
packet/Receiver and Analysis/Inst...
File View Axes Style Window Help
Packet with errors
Number of Events
10
5
0
0
0.5
1
1.5
2
Time
x 10^4

Fig 2 Error packets

In the Fig 2, it can be observed there are seventeen bad packets when the number of packets transferred is 1.189*10^4.

Message authentication using SAMA based on QR factorization.

Infinite messages are transmitted without any limitation of threshold.

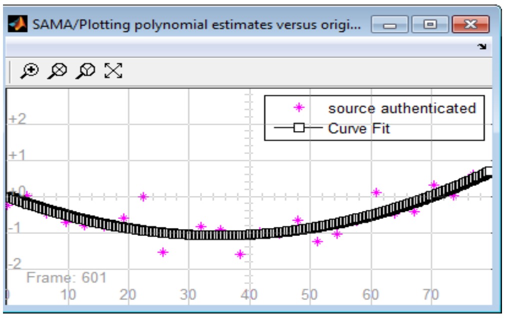

Fig. 3 Data points around the curve

In Fig. 3, 601 authenticated frames fit on the curve. Due to the presence of the noise, the data points are not exactly on the curve.

## VI CONCLUSION

SAMA established on QR factorization certifies the message authentication in hop-by-hop way without suffering threshold problem of the polynomial evaluation scheme. Message integrity is verified. Packet transmission time is determined for one node and multiple nodes. As the nodes increase the efficiency of transmission increases.

## ACKNOWLEDGEMENT

Happy to identify the individuals who helped me in formulating this paper. Special thanks to Mrs Lata S H (Asst. Professor, GMIT, Davangere) for supporting me all through this paper.

## REFERENCES

[1] F. Ye, H. Lou, S. Lu, and L. Zhang, “Statistical En-Route Filtering of Injected False Data in Sensor Networks,” Proc. IEEE INFOCOM, Mar. 2004.

[2] S. Zhu, S. Setia, S. Jajodia, and P. Ning, “An Interleaved Hop-ByHop Authentication Scheme for Filtering False Data in Sensor Networks,” Proc. IEEE Symp. Security and Privacy, 2004.

[3] Chu-Hsing Lin, Wei Lee, and Yi-Kang Ho," An Efficient Hierarchical Key Management Scheme Using Symmetric Encryptions**,"** Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA’05) 1550-445X/05 $20.00 © 2005 IEEE.

[4] M. Alimohammadi, and A. A. Pouyan, " Performance Analysis of Cryptography Methods for Secure Message Exchanging in VANET," International Journal of Scientific & Engineering Research, Volume 5, Issue 2, February-2014 912, ISSN 2229-5518.

[5] Nitin Jirwan, Ajay Singh, Dr. Sandip Vijay, " Review and Analysis of Cryptography Techniques,"International Journal of Scientific & Engineering Research Volume 4, Issue3, March-2013, ISSN 2229-5518.

[6] Xiaoqiang Zhang, Guiliang Zhu, Weiping Wang, Mengmeng Wang, " Design and Realization of Elliptic Curve Cryptosystem, "International Symposium on Instrumentation and Measurement, Sensor Network and Automation (IMSNA) 2012.

[7] Dan Tang, Jian Huang, " Secret Image Sharing Scheme Based on Bivariate Polynomial," International Conference on Uncertainty Reasoning and Knowledge Engineering, 2012.

[8] Sheetal Charbathia and Sandeep Sharma, " A Comparative Study of Rivest Cipher Algorithms," International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 4, Number 17 (2014), pp. 1831-1838. © International Research Publications House. http://www. irphouse.com.

**Manasa K** received her BE degree in Electrical & Electronics from UBDT College of Engineering, Davangere in 2006. Worked as a lecturer in BIET, Davangere and in Nitte Meenakshi Institute of Technology. Now pursuing MTech in Digital Electronics from GMIT, Davangere. Area of interest is networking.

**Lata S H** received her BE degree in Electronics and Communication and Mtech in Digital Communication & Networking from UBDT College of Engineering, Davangere. Presently serving GMIT as Asst. Prof., in Dept. of Electronics and Communication. Area of interest is networking.