Implementation of Hybrid Security and Compressive Sensing Scheme for Message Authentication Based on Robustness

[1]Sonu Maria Siby, [2] M.Ashik
[1] Final Year Student, M.E Communication Systems, [2].Assistant Professor
EASA College of Engineering & Technology, Navakkarai, Coimbatore-641115

***Abstract* - Wireless Sensor Network is one of the most emerging fields in communication. The important area of research in wireless sensor network is regarding the efficient utilization of energy and security. There are various cryptographic techniques for the secure transmission of information. The use of cryptographic techniques such as encryption and hashing will increase the energy consumption of sensors, thus reduces the energy constraint problems in the WSN. A hybrid security scheme is introduced since the traditional chaos based schemes are not directly applicable for wireless sensor networks. The scheme consists of 8 bit integer chaotic block encryption and a chaos based message authentication codes which will promotes the security and performance of data gathering scheme in WSN. Compression is mainly employed in order to reduce the burden of sensors.**

***Index Terms* - Hybrid Security, Cryptographic Techniques, Chaotic Block Encryption, Message Authentication Codes**

1. Introduction

Wireless sensor network can be defined as a network which consists of a number of sensor nodes that are wirelessly connected to each other. These small, low cost, low power and multifunctional sensor nodes can communicate in short distances and are grouped into clusters for the proper network operations. Data are transmitted mainly in the form of messages. There requires the security the security for the transmission of data in WSN which is based on confidentiality, authentication, integrity and availability with encryption and hashing scheme.

Message authentication codes are mainly used for the authentication purposes. MAC are very sensitive to any change of message they are appended to, If there is a change in any bit of the message it will also changes the message authentication codes. Hence there requires the verification of messages that the bits of the received message authentication codes and of the recalculated message authentication code from the received messages are equal. There are cryptographic algorithms which will introduces robustness into the messages that are protected by the message authentication codes and also corrects the message corrupted due to the noisy channel.

2. Related Work

Network security can be achieved by compressing the data with the data compression algorithms before the encryption. Compressive sensing technology can be employed for the data compression in wireless sensor networks in order to minimize the total energy consumption of a system. In the multimedia communication there requires security to the system without any authorized access to the system. Encryption is performed for the purpose of security in the compressive sensing technique which provides a secure and fast solution for the data protection. In order to increase the encryption performance a hybrid security strategy is employed that combines a chaotic block encryption and a light weight MAC that results in avoiding the data redundancy resulting from padding in encryption and hence can be used in WSN.

Cryptographic algorithms plays a major role in providing high security to information while transmission of data. These algorithms will provide data security and authentication for users during the transmission. There are also protocols which provide the strength for these cryptographic algorithms for the purpose of operation and routing. This new security protocols can be used along with the symmetric and asymmetric cryptographic techniques. The main issue in WSN is to reduce the energy constraint problems thus encryption and hashing is used for the energy consumption. There are many steps for the purpose of saving energy in WSN such as

- Schedule the state of the nodes
- Change the transmission range of the sensor nodes
- Use efficient routing methods
- Use proper data collecting methods
- Avoid unwanted data

Efficient utilization of energy and security are the two important areas in wireless sensor networks. For the proper network security data compression algorithms can be used before the encryption of data. Data compression is a process of reducing the amount of data, which removes the redundancy, repeatability, and irrelevancy of original data. Thus compressive sensing technology is used for data compression in wireless sensor networks.

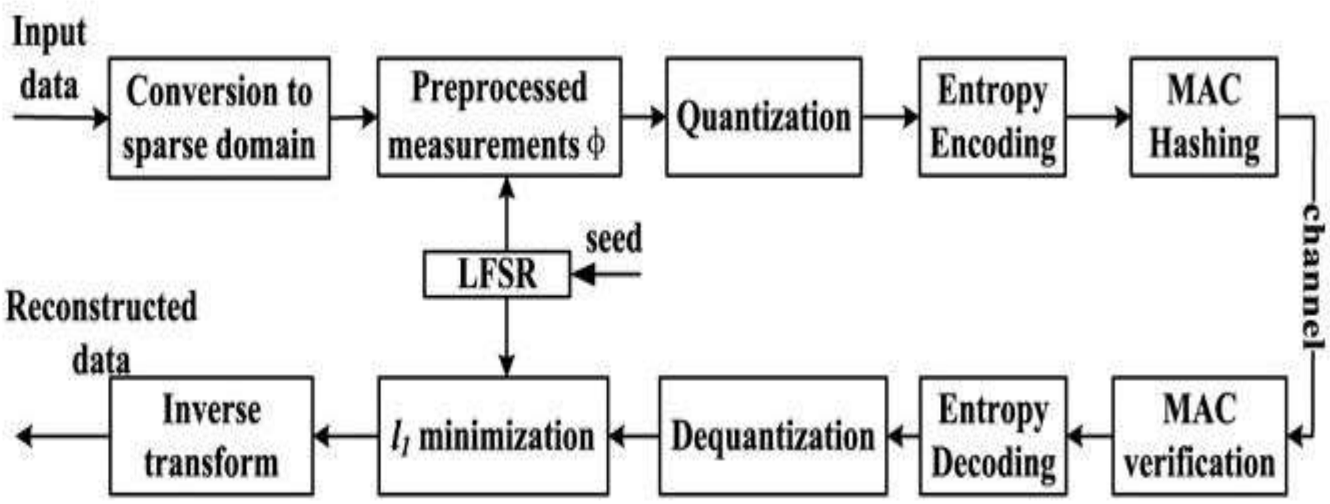
For the secure transmission of data in communication systems MACs are used. MACs are the symmetric cryptographic algorithms that provides data integrity and the authentication of data origin. MACs are constructed in such a way that any modification of the message results in change in the original data in a MAC, thus there requires the proper verification algorithm.

Chaotic block encryption technique is a simple nontraditional encryption technology which provides a secure and fast solution for the data protection that can be widely used in wireless sensor networks. Chaotic block encryption and message authentication codes are combined in the hybrid security scheme in order to increase the encryption performance.

Thus hybrid security compressive sensing data gathering scheme mainly consists of two operations which is mainly consists of two operations which is mainly performed for the purpose of security which includes hybrid security with encryption and hashing and the compressive sensing technique.

3. System Model

Hybrid security and compressive sensing scheme is one of the important scheme that is applied for the purpose of data collecting in which two operations are taken part in hybrid security scheme such as encryption and hashing. The other operation is compressive sensing in which data are being collected in which data volume can be reduced and security can be maintained.



Block Diagram of HSCS System

In this scheme data collected are encoded within the sensor nodes, then HSCS is followed, CS is conducted then the hybrid security strategy as encryption algorithm and MACs are implemented before the transmission of data. After sampling the signals they are compressed with the compressive sensing technique, as encryption algorithm is used for encryption. To prevent the malicious modifications cryptographic hash algorithm is performed. In the receiver side the inverse hashing will neglect the few transmitting errors which can be done by the software counter. Then the authentication verification is passed if the number of incorrect cases is under an allowable level.

4. Concept of Protocol Architecture for Hybrid Security

There are various types of cryptographic algorithms that provides high security to the system. These algorithms will provide data security and users authenticity. This new security protocol is designed mainly for the better security purpose using a combination of both the symmetric and asymmetric cryptographic techniques. It provides the cryptographic primitives such as integrity, confidentiality and authentication. With the help of elliptic curve cryptography, the given plain text can be encrypted. Through the secured channel elliptic curve cryptography and the derived cipher text can be communicated to the destination.

Simultaneously the hash value is calculated through MD5 for the same plain text which is converted into cipher text by elliptic curve cryptography. This hash value is then encrypted with the help of dual RSA and the encrypted message of this hash value is also sent to the destination. Thus the new hash value is calculated with the MD5 for the received original messages and is compared with the decrypted hash message for its integrity. Hence it can be ensured that either the original text being altered or not in the communication medium which is the primitive feature of this hybrid protocol.

Algorithms used ensures that the signals with the more irregular and quickly varying statistics can be recovered. With the help of this approach from the small amount of compressed data a large distributed network can be recreated with the better accuracy. Adhoc On Demand Distance Vector protocol initiates the route discovery process only when desired by a source node.

5. Advantages

- Energy consumption of the system is increased.
- Improved Robustness.
- Complexity of the system is decreased.
- Improved authentication scheme.
- Reduced the error during transmission together with the correction of messages corrupted due to a noisy channel.

6. Conclusion

The hybrid security system designed is mainly for the purpose of providing the security to the system while transmitting the data. The scheme has significant performance in security and compressing the data. Hybrid security compressive sensing is mainly suitable for the wireless sensor networks and it reduces the energy consumption of the system. By using the proper parameters we can thus reduce the complexity and cost of a system and also by using the proper algorithms robustness of the message authentication codes can also be increased.

References

[1] Jin QI, Xiaoxuan Hu, Yun Ma, Yanfei Sun, 'A Hybrid Security and Compressive Sensing-Based Sensor Data Gathering Scheme', 2015 IEEE Acess.

[2] Nandini. S. Patil, Prof. P. R. Patil 'Data Aggregation in Wireless Sensor Network', 2010 IEEE International Conference on Computational Intelligence and Computing Research.

[3] Xi Xu, Rashid Ansari "Power-efficient Hierarchical Data Aggregation using Compressive Sensing in WSN" International Journal of Advances in Science and Technology in 2011

[4].Yuanyuan LIU, Lu ZHU, Wenliang TANG2 'The Data Aggregation of Wireless Sensor Networks Based on Compressed Sensing and Cluster',Journal of Computational Information Systems 9: 9 (2013) 3399–3406.

[5] V. Abolghasemi, S. Ferdowsi, and S. Sanei, "A gradient-based alternating minimization approach for optimization of the measurement matrix in compressive sensing," Signal Process., vol. 92, no. 4, pp. 999–1009, Apr. 2012.

[6] M. Codreanu, M. Juntti and M. Leinonen, "Distributed correlated data gathering in wireless sensor networks via compressed sensing," in Proc. ACSSC, Pacific Grove, CA,USA, Nov. 2013, pp. 418–422.

[7] M.Duarte and Y.Eldar, "Structured compressed sensing: From theory to applications," IEEE Trans. Signal Process., vol. 59, no. 9, pp. 4053–4085, Sep. 2011.

[8] R. Szewczyk, A. Mainwaring, J. Polastre, J. Anderson, and D. Culler, "An Analysis of a Large Scale Habitat Monitoring Application," Proc. ACM Second Int'l Conf. Embedded Networked Sensor Systems (SenSys '04), pp. 214-226, Nov. 2004.

[9] E. Candes and M. Wakin, "An Introduction to Compressive Sampling," IEEE Signal Processing Magazine, vol. 25, no. 2, pp. 21 -30, Mar. 2008.

[10] D. Donoho, "Compressed Sensing," IEEE Trans. Information Theory, vol. 52, no. 4, pp. 1289-1306, Apr. 2006.

[11] J. Haupt, W. Bajwa, M. Rabbat, and R. Nowak, "Compressed Sensing for Networked Data," IEEE Signal Processing Magazine, vol. 25, no. 2, pp.92-101, Mar. 2008.

[12] C. Luo, F. Wu, J. Sun, and C.W. Chen, "Compressive Data Gathering for Large-Scale Wireless Sensor Networks," Proc. ACM Mobi Com, pp.145-156, Sept. 2009.

[13] Lindsey, S. and Raghavendra, C., PEGASIS: Power Efficient Gathering in Sensor Information Systems, In: Proceedings of IEEE ICC 2001, 2001. [3] Yang, Y. and Wu, H.H.and Chen, H., SHORT: Shortest Hop Routing Tree for Wireless Sensor Networks, In: IEEE ICC 2006 proceedings, 2006.