Cryptography Based Authentication For Secure Data Transmission In Wireless Sensor Networks

Dr.R.Prema
Assistant Professor/Department of ECS
Karpagam University, Coimbatore, India

Dr.S.SairaBanu
Assistant Professor &HOD/Department of ECS
Karpagam University, Coimbatore, India

***Abstract*— WSNs consists of a group of self organizing, lightweight sensor nodes that are used to cooperatively monitor physical or environmental conditions. Commonly monitored parameters include temperature, sound, humidity, vibration, pressure and motion. Each sensor node in a WSN is equipped with a radio transmitter, several sensors, a battery unit and a microcontroller. Although WSN research was initially motivated by military applications, wireless sensor networks are now used in many industrial and public service areas including traffic monitoring, weather conditions monitoring, video surveillance, industrial automation and healthcare applications. Because of the size and cost constraints on sensor nodes, they are limited by energy, bandwidth, memory and other**

Index terms - WSN, Cryptography, Encryption and Decryption.

I. INTRODUCTION

Sensor nodes consist of five main components as shown in Chien-Yuan Chen et al. [1] such as a computing unit, a communication unit, a sensing unit, a memory unit, and a power supply unit. The computing unit consists of a microprocessor. The microprocessor is responsible for managing the communication protocols, processing collected datafrom the on-board sensors, and performing the power management. Each sensor node has a single communication unit that is able to transmit and receive packets. This unit combines the functionality of both transmitter and receiver. The communication frequencies of the sensor nodes are between 433 MHz (in some early generations of sensor nodes) and 2.4 GHz (the most commonly used frequency) in Wattenhofer et al. [2]. The communication unit has four operational states: transmit, receive, idle and sleep. A sensing unit is usually a sensor board that consists of one or more sensors. Sensors must have extremely low power consumption. Some commonly used sensors are temperature sensor, humidity sensor, light sensor, barometer, 2-axis accelerometer, microphone, and GPS receiver. There are two types of memory units based on different needs for storage in a sensor node. The microprocessor itself contains some on-chip memory used to store system software. There is also typically flash memory available where users can store their own applications and data. The power unit provides power to other four units described above. In the MicaZ mote, for example, it consists of two AA batteries, either rechargeable or non-rechargeable. Although all sensing, computing and communication operations consume energy, data communication requires more energy than sensing and computing. Thus, reducing data communication between sensor nodes can improve the energy efficiency and extend the lifetime of sensor networks in Kwok-Wo Wong et al. [5].

II. LITERATURE REVIEW

In [1], Chien-Yuan Chen, Cheng-Yuan Ku, and David C.Yen found ways to use the LLL algorithm to break the RSA system even when the value of d is large. According to their proposed cryptanalysis, if d satisfies $|X - d| < N0.25$, the RSA system will be possible to be resolved computationally.

In [2], R. Wattenhofer, L. Li, P. Bahl, and Y.-M. Wang proposed a topology control algorithm based on discretization of the coverage region of a node into cones. The idea is to select appropriate transmitter power levels to guarantee network connectivity while at the same time transmission energy is saved.

In [3], Y. Xu, J. Heidemann, and D. Estrin puts a node into sleep mode whenever its active collaboration in the current network task is not required is another way to save energy. The geographical adaptive fidelity (GAF) algorithm conserves energy by turning off nodes that are equivalent from a routing perspective, thereby keeping a constant level of routing fidelity.

In [4], C. Schurgers, V. Tsiatsis, S. Ganeriwal, and M. Srivastava utilise sparse topology and energy management (STEM) protocol which puts the nodes aggressively into sleep mode and only wakes them up when they are needed to forward data. Data fusion is a technique that can be used to reduce the amount of redundant information prevalent in dense

sensor networks. By combining data with equal semantics, unnecessary power consumption due to transmission and processing of duplicate data is prevented.

In [5], Kwok-Wo Wong, Sun-Wah Ho, and Ching-Ki Yung, customized the chaotic cryptographic scheme to reduce the length of the ciphertext to a size slightly longer than that of the original message. Moreover, they introduced a session key in the cryptographic scheme so that the length of the ciphertext for a given message is not fixed.

In [6], Chang-Doo Lee, Bong-Jun Choi, and Kyoo-Seok Park proposed a block encryption algorithm, which is designed for each encryption key value to be applied to each round block with a different value. This algorithm needs a short processing time in encryption and decryption, has high intensity, and can be applied to electronic commerce and various applications of data protection.

In [7], L. Li, J. Y. Halpern, P. Bahl, Y.-M. Wang, and R. Wattenhofer proposed a topology control algorithm based on discretization of the coverage region of a node into cones. The idea is to select appropriate transmitter power levels to guarantee network connectivity while at the same time transmission energy is saved.

In [8], Mark G. Simkin discusses five encryption techniques: transposition ciphers, cyclic substitution ciphers, Vigenere ciphers, exclusive OR ciphers, and permutation ciphers. Accompanying these discussions are explanations of how instructors can demonstrate these techniques with spreadsheet models.

In [9], Jun Wei, Xiaofeng Liao, Kwok-wo Wong, and Tao Xiang proposed a new chaotic cryptosystem. Instead of simply mixing the chaotic signal of the proposed chaotic cryptosystem with the ciphertext, a noise-like variable is utilized to govern the encryption and decryption processes. This adds statistical sense to the new cryptosystem.

In [10], Osama Mahmud Abu Abbas, Khalid Mohammad Nahar, and Mohammad Ahmad Tubishat, uses Arabic letters and their diacritics for encrypting English messages and vice versa. A pseudo random generator is used to generate integer numbers to represent each character in Arabic language. The same numbers are used again after sorting them to represent the English characters. The conclusions that extracted indicate the efficiency of ARAE system according to security and time performance.

III. CRYPTOGRAPHY IN WIRELESS SENSOR NETWORKS

Due to the limitations of power, computation capability and storage resources, it is found to be a challenge of identifying a suitable cryptography for wireless sensor networks. Confidentiality of data is often critical in many WSNs, since the information transmitted by a sensor node may contain private information such as telehealth monitoring of a patient. Two fundamental categories of ciphers, symmetric and key ciphers and asymmetric (or public) key ciphers use different mechanisms to achieve security in Jun Wei [9]. Asymmetric cryptography depends on the difficulty of a mathematical problem and symmetric key cryptography focuses on the structure of simple iterative cryptographic operations. Symmetric key ciphers are generally used in the encryption of data transmitted by a sensor node, because of its less energy requirements in Kwok Wo Wong [5].

Symmetric key cryptographic algorithms include two types of ciphers, stream ciphers and block ciphers. A stream cipher operates on one bit of data by XORing the generated key stream bit with a plaintext bit, whereas a block cipher operates on a block of data by iterating through rounds of simple cryptographic operations. A symmetric key block cipher uses same cipher key for both encryption and decryption. The cipher key can be embedded inside the sensor device before its deployment or established by a specialized key agreement at the beginning of communication in Chang Doo Lee [6].

IV. PROPOSED METHODOLOGY

Depending on the environment where nodes are deployed, appropriate protection measures should be taken for data confidentiality, integrity and authentication between communicating entities, considering the cost, storage energy and communication efficiency requirements. To support such security services, one needs key management techniques that are resilient to both external and internal attacks. It is an important challenge to design secure and efficient key establishment techniques for wireless sensor networks (WSN).

Security is an important factor for performance and energy efficiency in many applications. Security serves as an important role in war zone, premise protection surveillance, airports, hospitals etc. Due to the property of sensor devices, the sensor networks may easily be compromised by attackers who send forged or modified messages. To prevent information and communication systems from illegal delivery and modification, message authentication and identification needs to be examined through certificated mechanisms. The messages transmitted from the sensor nodes over a wireless sensor networks should be authenticated by the receiver. The technique of cryptography is used for this mechanism. It is a challenge for the researchers to find out suitable cryptography for wireless sensor networks due to the limitations in power efficiency, computation efficiency and good storage capabilities.

4.1 *Cryptography Based Secure Transmission in wireless Sensor Networks*

The basic idea of the proposed cryptosystem method depends on set theory. The encryption is defined as a relation between the language alphabetic and a set of sets "one set for each alphabetical element", while the decryption is a relation

from a set of sets to the language alphabetic.

As an example the set of sets is the set of residue classes for a given number N. Hence, the encryption process is defending a relation between the language alphabetic and the prime modular classes P for a given N integer number, where N>P, N represents a secret information between the sender and the receiver, which each of them agree on using a secret channel. The sender uses the proposed encryption algorithm to send a message to the receiver, through unsecured channel, and the receiver uses the proposed decryption algorithm to read the received message.

4.2 ENCRYPTION PROCESS

The encryption process consists of a block cipher with a block length of 128 bits. Encryption consists of 10 rounds of processing for 128 bits keys. Each round of processing includes one single byte based substitution step, a row-wise permutation step, a column-wise mixing step, addition of round key, modular classes for plain text and permutation for the corresponding class. This uses a substitution-permutation network. It involves byte-level substitutions followed by a word-level permutation. The substitution and permutation method allows for a fast software implementation of the algorithm.

For encryption, each round consists of the following four steps; substitute bytes, shift rows, mix columns and add round key. The last step consists of XORing the output of the previous steps with four words from the key schedule. Digital signature is a mechanism by which a message is authenticated. A private key is used to encrypt and send the message along with public key or round key. For digital signature hashing is used. Hashing produces message digest. Hashing algorithms are used for encryption.

1. Entropy

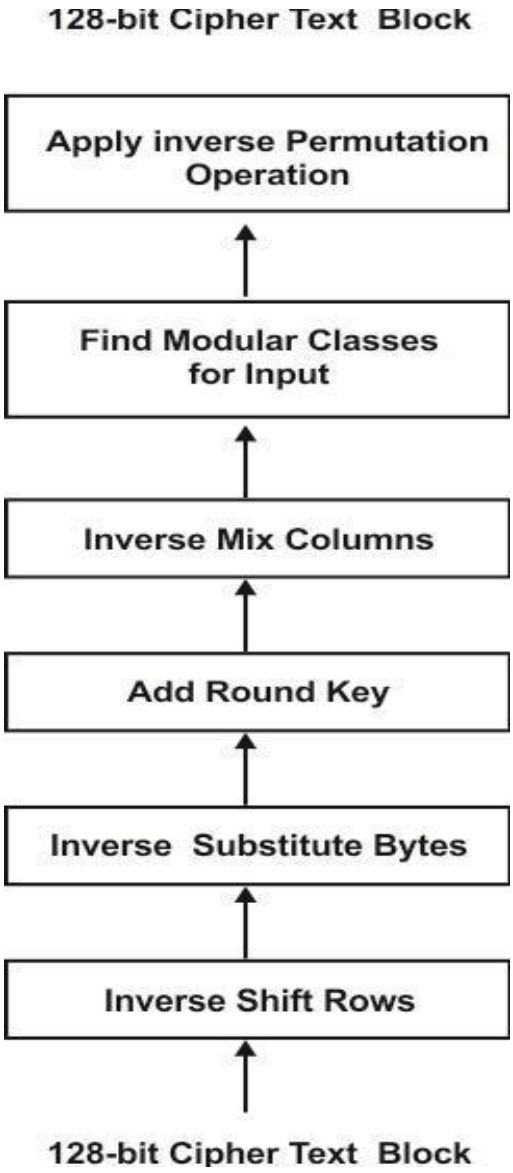
The entropy of the plain text is defined as the amount of information in a message, and it is a function of the probability distribution over the set of all possible messages:

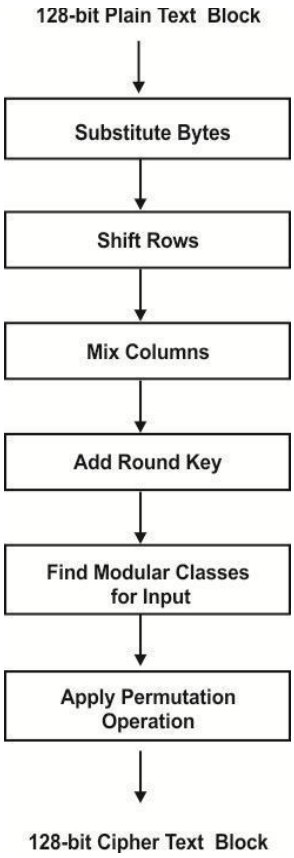
Let $x_1,\ldots,x_n$ are n possible messages occurring with probability $p(x_1),\ldots,p(x_n)$. Entropy of a given message is:

$$H(X)=\sum_{i-1}^{n} p(X=x_i)\log_2 p(X=x_i)$$

4.*3 DECRYPTION PROCESS*

- For decryption, each round consists of the following four steps; Inverse shift rows, Inverse substitute bytes, Add round key and Inverse mix columns. The last step consists of XORing the output of the previous steps with four words from the key schedule.
- Before any round-based processing for encryption, the input cipher text is XORed with the last four words of the key schedule.
- Byte-by-byte Inverse substitution is carried out in each round of decryption process. It reduces the correlation between the input bits and the output bits at the byte level.
- Inverse shift row transformation is used to shift the rows of the state array.
- The Inverse round key is used for inverse add round key transformation.
- Find the modular classes for the input N
- Apply an inverse permutation operation to the input cipher text to obtain the plain text.





V. NETWORK MODEL

.

The network model depicts the transmission of packets from source to sink. Node 0 is selected as a source node and Node 49 is selected as a destination node. The quality of the link is calculated for each node. The data is transferred towards the destination through the optimal path. The centre node is identified. The alarm information is collected by the centre node to establish quality of the link. The centre node broadcasts the alarm information to all other nodes.

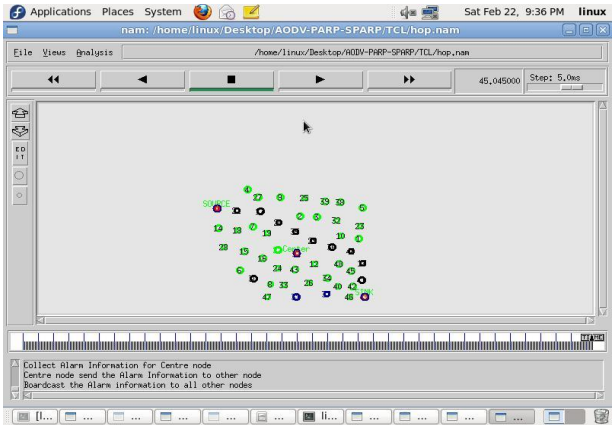


Figure 5.1: Transmission of Packets from Source to Sink

The path is selected according to the quality of the link. The alarm information is collected by the centre node to establish quality of the link. The centre node broadcasts the alarm information to all other nodes. The packets are transmitted from source to sink.

5.1 TOTAL POWER CONSUMPTION

It is the average energy consumption of all the sensor nodes in the network.

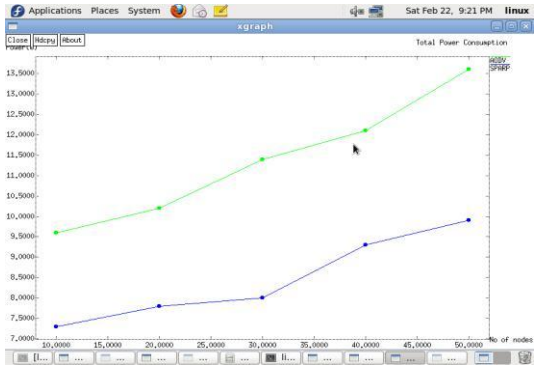


Figure 5.1: No. of Nodes vs Total Power Consumption

The graph drawn in Fig.4.2 for proposed work along with AODV proves that the proposed protocol consumes less power when compared with AODV protocol.

VI. CONCLUSION

In the proposed protocol, to prevent information and communication systems from illegal delivery and modification, message authentication and identification is examined through certified mechanisms. The messages transmitted from the sensor nodes over a wireless sensor networks is authenticated by the receiver. The technique of cryptography is used for this mechanism. The sender uses the proposed encryption algorithm to send a message to the receiver, through unsecured channel, and the receiver uses the proposed decryption algorithm to read the received message. The novel cryptosystem based Secured Power Aware Routing Protocol enhances Quality of Service (QoS) such as packet delivery ratio, and reduces the power consumption between the nodes when packets are transmitted.

REFERENCES

[1] Chien-Yuan Chen, Cheng-Yuan Ku b and David C.Yen, "Cryptanalysis of large RSA exponent by using the LLL algorithm", in Proceedings of The Tenth National Conference on Information Security, Taiwan, Pages: 45-50, 2000.

[2]R. Wattenhofer, L. Li, P. Bahl, and Y.-M. Wang. Distributed topology control for power efficient operation in multihop wireless ad hoc networks. In Proc. IEEE INFOCOM, pages 1388–1397, Apr.
2001.

[3] Y. Xu, J. Heidemann, and D. Estrin. Geography-informed energy conservation for ad hoc routing. In Proc. ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), pages 70–84, July 2001.

[4] C. Schurgers, V. Tsiatsis, S. Ganeriwal, and M. Srivastava. Topology management for sensor networks: Exploiting latency and density. In Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), pages 135–145, June 2002.

[5] Kwok-Wo Wong, Sun-Wah Ho, and Ching-Ki Yung, "A chaotic cryptography scheme for generating short ciphertext", Physics Letters A, Volume 310, Number 1, Pages:67-73, 2003.

[6] Chang-Doo Lee, Bong-Jun Choi and Kyoo-Seok Park, "Design and evaluation of a block encryption algorithm using dynamic-key mechanism". Future Generation Computer Systems, Volume: 20, Issue: 2, Pages: 327 - 338, 2004.

[7] L. Li, J. Y. Halpern, P. Bahl, Y.-M. Wang, and R. Wattenhofer. A cone-based distributed topology-control algorithm for wireless multi-hop networks. IEEE/ACM Transactions on Networking, 13(1):147–159, Feb. 2005.

[8] Mark G. Simkin, "Using Spreadsheets to Teach Data Encryption Techniques", AIS Educator Association, Volume 1, Number 1, pages 27 - 37, 2006.

[9] Jun Wei, Xiaofeng Liao, Kwok-wo Wong, and Tao Xiang, "A new chaotic cryptosystem", Chaos Solitons & Fractals 30 (5): 1143-1152 Dec 2006.

[10] Osama Mahmud Abu Abbas, Khalid Mohammad Nahar, and Mohammad Ahmad Tubishat, "Arae Cipher System", Computer Science Department, IT Faculty, Yarmouk University, Jordan, 2007.