Securing the Wireless Sensor Network Communication

Chaya P, Chandra Shekar P,

Abstract— Wireless sensor networks are a new type of networked systems, characterized by severely constrained computational and energy resources, and an ad hoc operational environment. When wireless sensor networks are deployed in a hostile terrain, security becomes extremely important, as they are prone to different types of malicious attacks. Due to the inherent resource limitations of sensor nodes, existing network security methods, including those developed for Mobile Ad-Hoc Networks, are not well suitable for wireless sensor networks. As a crucial issue security in wireless sensor networks has attracted a lot of attention in the recent year. This paper made a thorough analysis of the major security issue and implemented the most secure AES-256 algorithm for effectively securing the network and hence encrypting and decrypting data transferred between the nodes in a wireless sensor network.

Index Terms— **Wireless sensor network; AES; Decryption Encryption; Initialization Vector; security; threat; attack; benchmark**

I. INTRODUCTION

A. WIRELESS SENSOR NETWORK

Wireless Sensor Network (WSN) consists of hundreds or thousands of self-organizing, low power, low cost wireless nodes and is used in a variety of applications such as military sensing and tracking, environmental monitoring, disaster management, etc. However, when WSN is deployed in open, un-monitored, hostile environment [1], or operated on an unattended mode, sensor nodes will be exposed to the risk of being captured by an active adversary. Therefore, with the demanding constraints of nodes'limited capability, the key issue for WSN is designing viable security mechanisms *for* the protection of confidentiality, integrity and authentication to prevent malicious attacks, involved. Besides the inherent limitations in communication and computing, the deployment nature of sensor networks makes them more vulnerable to various attacks. Largely deployed sensor nodes may cover a huge area further exposing them to attackers who may capture and reprogram the individual nodes as shown in Fig.1. The adversary may use its own formula of attacking and induce the network to accept them as legitimate nodes. Falsification of original data, extraction of private sensed data, hacking of collected network readings and denial of service are also certain possible threats to the security and the privacy of the sensor networks. However, hardware and software improvements may address many of such security issues, but development of new supporting technologies and security principles are challenging research issues in WSNs.

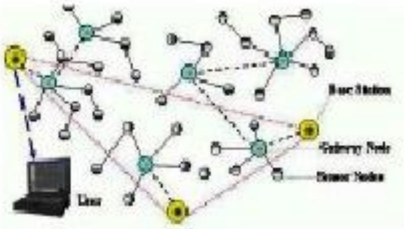

Fig 1. Scenario of wireless sensor nodes deployment.

B. AES SYSTEM

An AES system is a symmetric-key system in which the sender and receiver of a message share a single, common key, which is used to encrypt and decrypt the message. The data length of a key or message may be chosen to be any of 128 or 256 bits. The AES encryption/decryption algorithms are shown in Table AES operates on a 4x4 array of bytes (referred to as ―state‖). The algorithm consists of performing four different simple operations. Those are as follows:

- •Sub Bytes
- •Shift Rows
- •Mix Columns
- • AddRoundKey

Sub Bytes perform byte substitution, which is derived from a multiplicative inverse of a finite field. Shift Rows shifts elements from a given row by an offset equal to the row number. The Mix Columns step transforms each column using an invertible linear transformation. Finally, the Add Round Key step takes a 4x4 block from an expanded key (derived from the key), and XORs it with the ―state‖. AES is composed of four high-level steps. These are:

1. Key Expansion
2. Initial Round
3. Rounds
4. Final Round

The Key Expansion step is performed using Rijndael's key schedule. The Initial Round consists only of an Add Round Key operation. The Rounds step consists of a Sub Bytes, Shift

***Chaya P**, Department Of Information Science and Engineering, GSSS Institute Of Engineering And Technology For Women Mysore, ., Mysore, India.*

***Chandra Shekar P**, Department of Electronics and communication Engineering, ATME (Academy for Technical & Management Excellence), Mysore, India, 9538584312.*

Rows, Mix Columns, and an Add Round Key operation. The number of rounds in the Rounds step varies from 10 to 14 depending on the key size. Finally, the Final Round performs a Sub Bytes, Shift Rows, and Add Round Key operations. Decryption in AES is done by performing the inverse operations of the simple operations in reverse order. The structure of AES is as shown in the figure-2. Hence, for the AES algorithm, the length of the input block and the output block is same. It is a point to be noted here that no weak or semi-weak keys have been identified for the AES algorithm and there is no restriction on key selection, only the Key Expansion routine for 256-bit Cipher Keys is slightly different from for 128- and 192-bit Cipher Keys. Here in this application we are using 256-bit key AES, in which there are 14 iterations called the round key- for being used in the last stage of AES. First three stages are ―Sub Bytes‖,

―Shift Rows‖ and ―Shift Columns. The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either 192 or 256 key lengths. Design of AES is highly conservative that enables us to demonstrate its security against all known types of active and passive attacks.

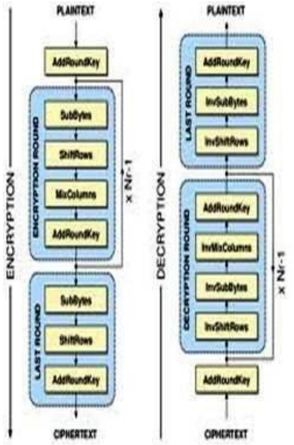

Figure 2. Structure of AES

II. SENSOR NETWORK SECURITY ISSUE

Two of the most security-oriented applications of wireless sensor networks are military and medical solutions. Due to the nature of the military, it is obvious that the data (sensed or disseminated) is of a private nature and is required to remain this way to ensure the success of the application. Enemy tracking and targeting are among the most useful applications of wireless sensor networks in military terms. The most up to date work can be found on the Defense Advanced Research Projects Agency (DARPA) website [2, 3]. The choice of which security services to implement on a given sensor mainly depends on the type of application and its security requirements. Amongst these, we examined:

- Authenticity - it makes possible that the message receiver is capable of verifying the identity the message sender, hence preventing that likely intruder nodes inject malicious data into the network.
- Confidentiality - it ensures that only authorized nodes access the content of the message.
- Integrity - it guarantees that should a message have its content modified during the transmission, the receiver is able to identify these alterations. In order to design a completely secure wireless sensor network, security must be integrated into every node of the system. This is due to the possibility that a component implemented without any security could easily become a point of attack. This dictates that security must pervade every aspect of the design of a wireless sensor network application that will require a high level of security [4].

III. SECURITY REQURIEMENT

The goal of security services in WSNs is to protect the information and resources from attacks and misbehavior. The security requirements in WSNs include:

- Availability, which ensures that the desired network services are available even in the presence of denial-of-service attacks require configuring the initial duty cycle carefully.
- Authorization, which ensures that only authorized sensors can be involved in providing information to network services.
- Authentication, which ensures that the communication from one node to another node is genuine, that is, a malicious node cannot masquerade as a trusted network node.
- Confidentiality, which ensures that a given message cannot be understood by anyone other than the desired recipients.
- Integrity, which ensures that a message sent from one node to another is not modified by malicious intermediate nodes.
- Nonrepudiation, which denotes that a node cannot deny sending a message it has previously sent.
- Freshness, which implies that the data is recent and ensures that no adversary can replay old messages. Moreover, as new sensors are deployed and old sensors fail, we suggest that forward and backward secrecy should also be considered:
- Forward secrecy: a sensor should not be able to read any future messages after it leaves the network.
- Backward secrecy: a joining sensor should not be able to read any previously transmitted message. The security services in WSNs are usually centered on cryptography. However, due to the constraints in WSNs, many already existing secure algorithms are not practical for use.

IV. SECURITY BENCHMARKS

We suggest using the following metrics to evaluate whether a security scheme is appropriate in WSNs:

- Security: a security scheme has to meet the requirements discussed above.
- Resiliency: in case a few nodes are compromised, a security scheme should still protect against the attacks.
- Energy efficiency: a security scheme must be energy efficient to maximize node and network lifetime.
- Flexibility: key management needs to be flexible to allow for different network deployment methods, such as random node scattering and predetermined node placement.
- Scalability: a security scheme should be able to scale without compromising the security requirements.
- Fault-tolerance: a security scheme should continue to provide security services in the presence of faults such as failed nodes.

- Self-healing: sensors may fail or run out of energy. The remaining sensors may need to be reorganized to maintain a set level of security.
- Assurance: assurance is the ability to disseminate different information at different levels to end-users [12]. A security scheme should offer choices with regard to desired reliability, latency, and so on.

V. IMPLEMENTATON

In this section, the important functions of the communication application are discussed. The application architecture is as shown in the fig 4.

A) Text Encryption & Decryption:

On connection establishment, using UDP protocol [7] by specifying IP address of an adhoc node, adhoc nodes can communicate using encrypted chat. Here the node, which wants to communicate with other node, should know must password in prior. The information, which travels on the unsecured network, is not in the plain text form, it is encrypted using password derived AES algorithm before sending. The cipher text generated from the algorithm is sent to the other node. On receiving, the receiver in the receiving side is notified, saying a new message received. The message displayed on the receiver node is a cipher text, which needs to be decrypted using the known password. Here the nodes wishing to communicate have to know the password. The nodes that are not aware of the password are not allowed to communicate.

B) File Encryption & Decryption:

The nodes establish communication setup either using TCP or UDP. By knowing the IP address, the file is sent form one node to the other. The file to be sent can be an image, text, audio or video file. Before sending the file, it is being encrypted. Therefore, the file, which goes through the unsecured network, is in the encrypted form, thus avoiding the intruder to know the contents of the file. The receiver decrypts the file using the password. On decrypting with the correct password, the authorized receiver will get the original file, which was sent from the authorized node. If the intruder gets the encrypted file via unsecured network, the file will be decrypted but it would give wrong output. If the intruder replaces the encrypted file with some other file, the authorized node will get to know, as it will not get decrypted. The original file, encrypted file and the correct password, all go hand in hand. If anyone among them is replaced, it can be found out very easily. Hence the file encryption & decryption process.

C) Voice Encryption & Decryption:

The nodes establish communication setup either using UDP. The call set up is established using the IP address. When the user wants to make a call, we send an Invite message and wait for an OK response. When we receive an OK, we start receiving/sending audio captured from the microphone. If the remote party rejects the call then a busy response is sent. To drop a call, we simply send a Bye message. The application will asynchronously receive/send call messages on specified port and synchronously receive/send audio data on specified port. In other words, the application listens on two ports: When we receive an OK, we start receiving/sending audio captured from the microphone. If the remote party rejects the call then a busy response is sent. To drop a call, we simply send a Bye message. The application will asynchronously receive/send call messages on specified port and synchronously receive/send audio data on specified port. In other words, the application listens on two ports:

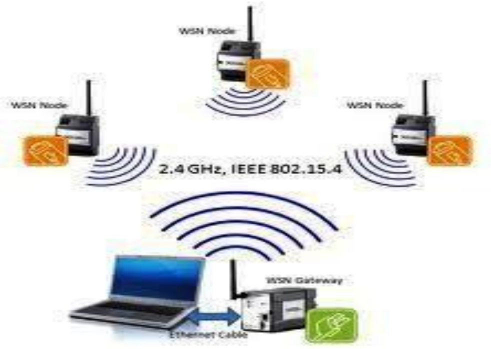

Fig.3 Design of the application

D) Video Encryption & Decryption:

In streaming mechanism, the file is sent to the end user in a (more or less) constant stream. It is simply a technique for transferring data such that it can be processed as a steady and continuous stream and it is called Streaming. Streaming video is a sequence of "moving images" that are sent in the form of bytes, before sending over the network, those bytes are encrypted and at the receiving end those bytes are decrypted before being displayed by the viewer as they arrive. If a user is receiving the video data as streams then he/she does not have to wait to download a large file before watching the video or listening to the audio.

VI. CONCLUSION

The implementation of password based AES-256 in wireless sensor networks provide the facility to encrypt the data transferred across the nodes to transmit data securely decrypt the data by the authorized nodes to get the original information. Making the AES algorithm password independent can be the future work

REFERENCES

[1] Seong-Yeon Lee and Jong-Nam Kim,‖Real-Time DMB Video Encryption in Recording on PMP‖, International Journal of Signal Processing, Image Processing and Pattern,Vol. 2, No.1, March, 2009

[2] Mamoona Asghar, Saima Sadaf, Kamran Eidi, Asia Naseem and Shahid Naweed ,―SVS - A Secure Scheme for Video Streaming Using SRTP AES and DH‖ , European Journal of Scientific Research ISSN 1450-216X Vol.40 No.2 (2010), pp.177-188

[3] Wail S. Elkilani, et.al,‖ Performance of Encryption Techniques for Real Time Video Streaming‖, Networking and Media Convergence, 2009. International Conference, 24-25 March 2009 pg: 130 - 134

[4] Jayshri Nehete, K.Bhagyalakshmi, M.B.Manjunath, Shashikant Chaudhari, T.R.Ramamohan, ―A Real-time MPEG Video Encryption Algorithm using AES‖, NCC 2003 9th national conference.

[5] Abdul Samiah, Arshad Aziz and Nassar Ikram,‖ An Efficient Software Implementation of AES-CCM for IEEE 802.11i Wireless Standard‖, 31st Annual International Computer Software and Applications Conference(COMPSAC 2007) ,0- 7695-2870-8/07

[6] Federal Information Processing Standards Publications (FIPS PUBS) are issued by the Name of Standard. Advanced

Mrs. Chaya P, received the B.E degree in Information Science and Engineering from Coorg Institute of Engineering , Ponnampet, Karnataka, India, in 2004, and the M.Tech. Degree in Softwarre engineering from SJCE, Mysore, Karnataka, India in 2011. She is currently working as Asst. Professor in Department of Information Science & Engineering, GSSS Institute Of Engineering And Technology For Women ,Mysore, Karnataka, India. Her Research interests include Network Communication and Big-data.

Mr. Chandra Shekar P, received the B.E degree in Electronics and communication Engineering from Coorg Institute of Engineering , Ponnampet, Karnataka, India, in 2004, and the M.Tech. Degree in VLSI Design and Embedded System from KVG College of Engineering, Karnataka, India in 2013. He is currently working as Asst. Professor in Department of Electronics and communication Engineering, ATME (Academy for Technical & Management Excellence) College of Engineering, Mysore, Karnataka, India. His Research interests include Wireless communication, Computer Communication and Network, Low Power VLSI, Digital Electronics, Analog and mixed signals.