Article can be accessed online at http://www.publishingindia.com

A Study and Modelling for Improving Secure Communication in Wireless Sensor Networks

B. Vidhya*, Mary Joseph, D. Rajini Girinath***, A. Malathi******

Abstract

Storage nodes play a vital role in wireless sensor networks for carrying out the storage activity of data sent by the sensor node once after capturing the details of the environment and in turn to answer the sensor data related query to the network owner. Because of the less storage capacity on the sensor node, storage node takes the whole responsibility for pre-processing the data as well as to respond to queries returned by the owner. Duplicate sensor/storage node imposes a major threat to the wireless sensor networks. The proposed approach focusses on carrying out the effective techniques for data transfer by using Elliptic Curve Encryption for encrypting the image captured from the environment and also to transmit the encrypted critical text data from source to destination, aggregate Signature to validate the sender of the message for data verification, steganography to hide the encrypted content within an image. The proposed ideas are well suited for transferring the details secure in WSN.

Keywords: ECC, Steganography, Aggregate Signature, Wireless Sensor Networks (WSN), Reliability

Introduction

Wireless Sensor Network (WSN) architecture focusses on two parts namely sensor node and authority. Sensor nodes transmit the sensed data to storage node (SN). Unstable connection exists between the sensor and authority. Due to instability, an intermediate node namely storage node came into existence to cache the collected data from the sensor node as depicted in Fig. 1 (Yu, Ni, Chen, Gelenbe & Kuo, 2014). Questions posed by the owner will be responded by the storage node. The pictorial representation of the architecture has been illustrated in the below diagram Fig. 1. A group of sensor nodes collectively form a cluster and for the entire cluster, one storage node has been allocated to monitor the group of sensor nodes. Similarly for different clusters, each storage node is responsible for caching the collected readings from the sensor nodes. Each storage node on considering the network connectivity responds to the nearest storage node which in turn transmits the details to owner.

Top-k query processing has been introduced to calculate the most important data according to their priority. The most commonly used techniques in preference-based queries are the top-k query (Zhang, Shi, Zhang & Huang, 2014). A top-k query employs some functionality to rank the records in a dataset with attributes. K highest scores will be returned by the subset of queries. The advantage of this popular technique is that the user is able to obtain satisfactory information, both in terms of the number of results and the correspondence with the specified preferences.

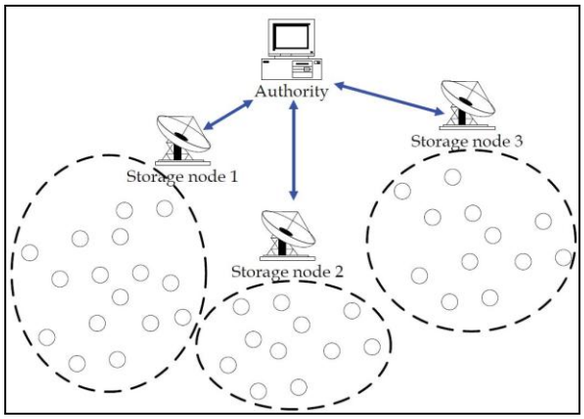
* PG Student, Department of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai, Tamil Nadu, India. E-mail: vidhya1.b@gmail.com

** Assistant Professor, Department of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai, Tamil Nadu, India.

*** HOD & Professor, Department of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai, Tamil Nadu, India.

**** Assistant Professor, Department of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai, Tamil Nadu, India.

Fig. 1: An Illustration of WSN Architecture



WSN plays a vital role in establishing a communication medium between virtual and non-virtual world. Sensor nodes are deployed at distinct locations to monitor the environment related conditions which can done only little computation and its main responsibility is to sense the environment and to report it to the leader node. WSN can also aggregate all the details of the sensor and thus achieves eliminating redundant data. It has been used in many applications like environment monitoring, industrial and civilian applications. Traditional computer world mainly concentrates on integrating with the physical world which is different from wireless sensor networks which mainly integrates with the physical world. Application development is not trivial in case for wireless sensor networks (Yu, Li, Cheng, Xiong & Shen, 2013).

Deployment of sensor nodes in different location will be monitored periodically to change the depleted batteries which have happened due to environmental conditions in the environment. Each sensor node deployed in the location will have a relationship with each other and it thus enables the communication between each of the sensor nodes. Main establishment of sensor nodes is, they have to operate without any manual intervention. Sensor can begin its communication once enough number of nodes has been deployed in different locations. The location details sensed by the network will be monitored by the network owner for querying the storage node which is the owner for a group of sensor nodes deployed in different locations (Li, Luo, Liu, Lee & Chu, 2013). Different kinds of architectures exist and one of them is hybrid architecture, in which the results of the sensor were used to control the detailed monitoring of the environment.

The functionality of the sensor node which is functioning individually is simpler since its main task is to monitor the environment details as well as to track the details of the environment. The functionality of sensing more complex data is the major challenge faced in the environment. In order to solve the challenge, all the sensor nodes need to communicate with each other to establish and merge the results published by each of the sensor node. The data collected by the different sensor nodes need to be aggregated and thus eliminate the functionality of the redundancy. The merging of the data needs to be checked as well for redundancy details (Hasan, Brunie, Bertino & Shang, 2013).

Characteristics of WSN

Main establishment of wireless networks is middleware. Middleware plays an important role in the establishment of sensor network operation. The important characteristics of sensor network are as follows (He, Chan & Tang, 2014):

- A size of cubic millimetre for deploying in minute areas is going to be discovered in future.
- Limited amount of resources due to their performance, size and energy of each sensor.

Due to depleted batteries, sensor will face a significant amount of sensor failures due to environmental conditions. The destructions caused in the WSN achieve the high level of dynamics in the sensor node environment. Hence frequent partitions of networks will be followed due to their change in the topology of the network. Mobile nodes will also have sensor network partitions. Even though separate partition exists between the mobile nodes, each node will not have any delays in transferring the information from one node to another. Communication failure exists and it is the main problem in WSN. Scalability is the main important problem in the sensor network and it can be resolved by eliminating the redundancy. Nodes have to operate mainly independent by interconnecting with remaining sensor nodes.

Design Principles of WSN

Below were the principles designed for the wireless sensor network:

- WSN communicate with neighbour nodes to achieve the data communication which is termed as localised algorithms.

- The above architecture works well in case of network size which is large and also sustain the network failures.
- An algorithm named adaptive fidelity mainly enables the communication based on the sensor node result quality.
- The problem in above algorithm can be resolved by selecting the various resource and quality requirements.
- In a communication which is targeting mainly sensor node data, authority will request the data details by mainly focussing towards the data produced by the sensor node. eg. temperature sensor which produces the data based on the specific temperature in the environment. In such a case, authority will be requesting the details of the sensor node locations where the temperature exceed the certain limit.
- The above type of communication is said to be data centric and it thus establishes more robustness in achieving the data quality.
- With the help of mixing the data from the different sensor nodes, the efficiency of the data can be improved and thus robustness can be achieved in a timely manner.

Information Security in WSN

Information security can be achieved using the below techniques:

Asymmetric Cryptography

Using asymmetric cryptography in the data transfer as described in Fig. 2 establishes security in the data transfer between the two communication medium. The sender and the receiver exchanges two pair of distinct keys and not the unique in case of symmetric cryptography for exchange of data between them.

Fig. 2: Encryption & Decryption Process

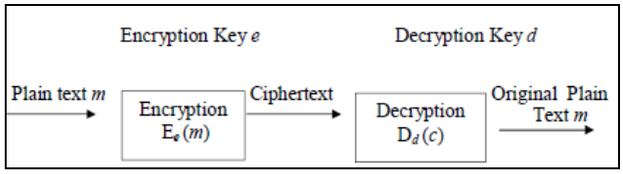
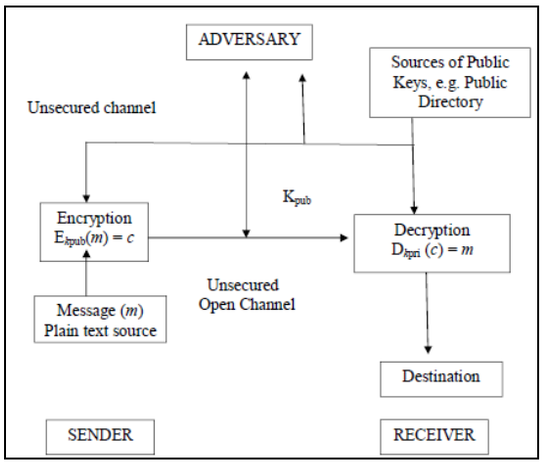


Fig. 3 describes the architecture for data communication between the sender and the receiver. Sender and receiver use different pair of keys, which establishes the security of data transfer. Adversary will not be able to know the information of anyone of the sensor node if the sensor node or the storage node gets compromised. Because of different keys which were exchanged using digital certificate, the data will never be known to the unauthorised persons.

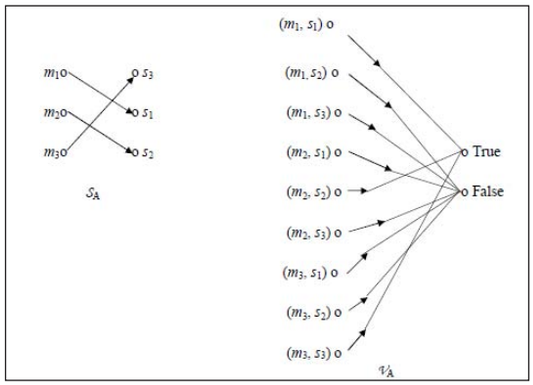
Fig. 3: Architecture for Data Transfer in Asymmetric Cryptography



Digital Signature

Digital signature is the concept of validating the authenticity of the sender and thus it achieves the verification of the data send by the sender for accepting it for further communication (Mahmoud, Taha, Misicand & Shen, 2013). The process of generating the signature has been depicted in the Fig. 4.

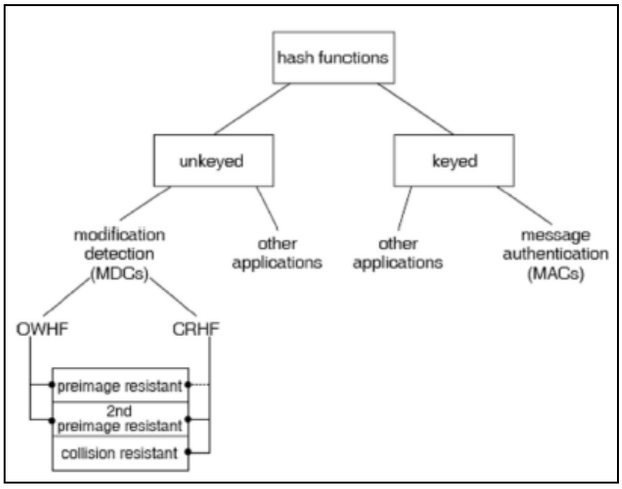
Fig. 4: Illustration of Signature Generation and Verification Function for a Digital Signature Scheme



Hash Message Authentication Function

HMAC has been used to generate the message digest for the verification of data which ensures that the message has not been modified in middle of data transfer. This ensures that adversary has not modified the data which were communicated from the sender to the receiver. SHA-1 has been considered for generating the message digest for the validation process.

Fig. 5: Illustration of Hash Function Process



Related Work

In order to detect the anomaly, intrusion detection systems has been discovered which should satisfy the below requirements (Butun, Morgera & Sankar, 2014):

- The intrusion detection system should not disclose any more new problems when compared to the existing problems
- The resources required for such a detection system is very little and hence it should not produce any processing overhead.
- It should not degrade often and it should process continuously without any manual intervention.
- Robustness and reliability needs to be maintained and it should achieve efficacy in the data generation phase.

Two secure protocols namely SET-IBS and SET-IBOOS have been generated for achieving and improving the data communication between the two nodes (Lu, Li & Guizani, 2014).

- SET-IBS and IBOOS reduce the security and computational processing overhead of the sensor nodes

Various attacks have been considered for showing the effectiveness of the above two protocol and hence it is suitable for achieving the robustness and reliability in the communication medium between the two nodes. With the help of dynamic programming method, optimisation of different nodes data can be aggregated efficiently and the algorithm named greedy has been designed for the purpose of executing the queries to save the computational processing overhead (Chen, 2013). Practical results have shown that the greedy algorithm has been chosen for achieving the process efficiency.

Proposed Algorithms

The proposed technique mainly focusses to improve the data security while transferring the top-k environment data to the clients using asymmetric encryption. ECC has been chosen for encryption and decryption of image as well as text message which is transferred between the storage node and network owner. The algorithms for generating the encryption as well as to generate the signature are given below.

Top-k Data Conversion Algorithm

- Get the string to encrypt the content
- Create adhoc random number to be added to the ASCII of char array
- Generate ASCII no by converting the letter of received string to ASCII.
- Add the random number generated value to each ASCII.
- Use any special character for identifying the separation between the string
- Use public key of encryption algorithm to generate the encrypted text.
- Obtain cipher text from the corresponding algorithm.
- Display the encrypted content into the console.

Top-K Query Signature Generation Algorithm

- Create BigInteger variables “g”, ”p” for storing the public key and “d” for storing the private keys.

- Create a key bit length to be assigned for generating the key length
- Create an object for generating the cryptographically strong pseudo random number
- Generate a BigInteger with key bit length that is highly likely to be prime and assign it to variable P.
- Generate a random BigInteger of length "keybit-length-1" and assign it to var "g" and "d".
- Compute public and private keys for generating the signature using the function

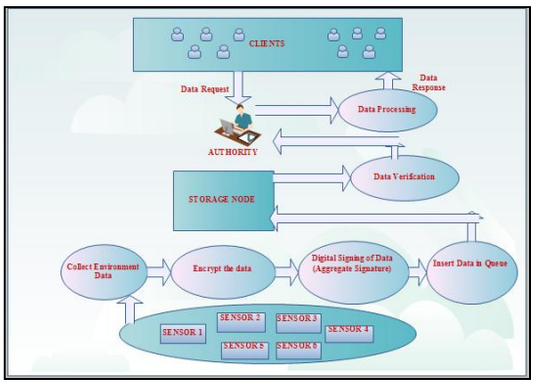
  g.modpow(d,p)
- Compute BigInteger values to be used for generating the signature.
- Generate the Signature using the function:

  y.modpow(a,P).multiply(a.modpow(b,p))
- Create two files "Aggregate Signature" and "Sensor node signature" and write the signature generated into each file location.

Proposed Model

The proposed model depicts the data sent from the sensor to owner has been processed at various stages to handle the data in a secure medium.

Fig. 6: An Illustration of Top-k Data Process Architecture in WSN



Implemented Modules

Input Data Generation

- **Sensor Nodes:** To collect the environment data
- **ECC:** For encrypting the sensed data
- **Aggregate Signature:** Verification of sensor identity.

Generated Data Verification Process

- **Storage Node:** Verify Aggregate signature
- Verification of Sensor node validity
- Report Adversary details to authority if any.

Steganography Data Generation

- Base Station to key in the details about the environment.
- Dummy Data Insertion
- **HMAC:** Generates hash data
- **Storage Node:** Responsible for Steganography data generation
- Cryptography combined with Steganography: Achieves secure data transfer from storage node to authority.
- Hiding Message Digested data within an image
- Submit it to Authority

Output Data Generation

- **Authority:** Responsible for processing the steganography data
- To unhide the data within an image.
- Decrypt the content to retrieve the original data
- Update Sensor content into the Database
- Fetches the data from Database upon top-k request from clients

Implementation Results

Different algorithm key sizes have been taken to measure the key size of the proposed technique ECC. Table 1 illustrates the different algorithm key sizes.

Table 1: Algorithm Key Sizes

S. No	*Symmetric Key Size (in Bits)*	*RSA Key Size (In Bits)*	*ECC Key Size (in Bits)*
1	80	1024	160-223
2	112	2048	224-255
3	128	3072	256-383
4	192	7680	384-511
5	256	15360	512+

Different file sizes were considered to check the computation time of the encryption and decryption process of Elliptic Curve Cryptography. Table 2 shows the representation of the file sizes considered.

Table 2: Sample Files for Analysis

S. No	File Name with Extension	File Size in Bits
1	File1. Jpeg	81182
2	File2. Jpeg	212992
3	File3. Jpeg	714342
4	File4. Jpeg	819200
5	File5. Jpeg	1105920

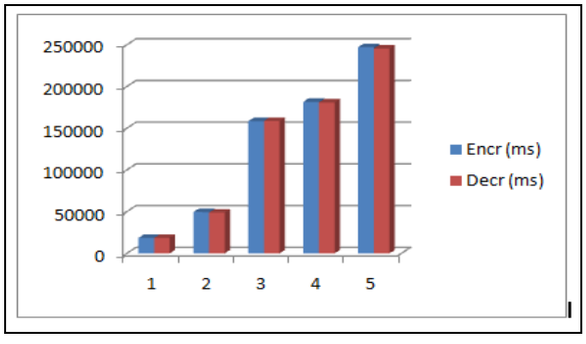
The time taken for encryption and decryption for ECC algorithm has been shown in Table 3 which shows the time taken for encrypting and decrypting the content for each of the sample file collected in Table 2.

Table 3: Performance Time by ECC

S. No	Data Bits	ECC Enc. in ms	ECC Dec. in ms
1	81182	18559	18541
2	212991	49525	48990
3	714341	158689	158890
4	819202	181465	180910
5	1105930	247319	245513

The above data can be represented pictorially in a graph for better understanding of the timing of encryption/decryption which has been described in Fig. 3.

Fig. 7: Pictorial Representation of Encryption/ Decryption Processing Time



Conclusion

The security issues of WSN have been studied and analysed to achieve the better security for transferring the details from source to destination. The proposed approaches implemented will thus enable the secure transfer of data in WSN medium and also to succeed from transferring the data in a secure medium without the knowledge of adversary. Adversary will never be able to get the details of the original data due to the effective techniques implemented namely cryptography combined with steganography. The proposed approaches are well suited to transfer the details in WSN.

References

Butun, I., Morgera, S. D., & Sankar, R (2014). *A Survey of Intrusion Detection Systems in Wireless Sensor Networks*. IEEE Transactions on Wireless Communications, 12(6), 2818-2822.

Cristofaro, E. D., & Pietro, R. D. (2013). *Adversaries and Counter-measures in Privacy-enhanced Urban Sensing Systems*. IEEE Systems Journal, 7(2), 312-320.

Hasan, O., Brunie, L., Bertino, E., & Shang, N. (2013). *A Decentralized Privacy Preserving Reputation Protocol for the Malicious Adversarial Model*. IEEE Transactions on Information Forensics and Security, 8(6), 950-960.

He, D., Chan, S., & Tang, S. (2014). *A Novel and Lightweight System to Secure Wireless Medical Sensor Networks*. IEEE Journal of Biomedical and Health Informatics, 18(1), 317-324.

Li, F., Luo, B., Liu, P., Lee, D., & Chu, C. H. (2013). *Enforcing Secure and Privacy-Preserving Information Brokering in Distributed Information* Sharing. IEEE Transactions on Information Forensics and Security, 8(6), 889-895.

Mahmoud, M. M. E. A., Taha, S., Misicand, J., & Shen, X. S. (2014). *Lightweight Privacy-Preserving and Secure Communication Protocol for Hybrid Ad Hoc Wireless Networks*. IEEE Transactions on Parallel and Distributed systems, 25(8), 2078-2088.

Lu, H., Li, J., & Guizani, M. (2014). *Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks*. IEEE Transactions on Knowledge and Data Engineering, 26(8), 1854-1864.

Yu, C. M., Ni, G. K., Chen, I. Y., Gelenbe, E., & Kuo, S. (2014). *Top-k Query Result Completeness Verification in Tiered Sensor Networks*. IEEE Transactions on Information Forensics and Security, 9(1), 109-123.

Yu, L., Li, J., Cheng, S., Xiong, S., & Shen, H. (2014). *Secure Continuous Aggregation in Wireless Networks*. IEEE Transactions on Parallel and Distributed Systems, 25(3), 763-773

Zhang, R., Shi, J., Zhang, Y., & Huang, X. (2014). *Secure Top-k Query Processing in Unattended Tiered Sensor Networks*. IEEE Communication and Information System, Huazhong University of Science and Technology, 25(3), 763-773.

Chen, T., & Chen, L. (2013). *Optimizing Multi-Top-k Queries over Uncertain Data Streams*. IEEE Transactions on Knowledge and Data Engineering, August.