International Journal of Soft Computing and Engineering (IJSCE)
ISSN: 2231-2307 (Online), Volume-9 Issue-4, November 2019

A Primitive Proposal of an Algorithm for IP and Mac Based Data Aggregation and message authentication in Wireless Sensor Networks

N.Shantha Kumar, Hareesh.K

Abstract: ***In wireless sensor networks(WSN) ,authentication of messages is the highly important function in preventing threats from un wanted , un authorized and corrupt messages from being sent. There are various message verification and authentication methods have been proposed as well as developed based on cryptography technology such as symmetric key cryptographic systems or public-key cryptographic systems. Also there are many different techniques available based on polynomial-based schemes, elliptic curve cryptography (ECC) and so on. All the above said methods have its own merits and demerits. In this research work a new method of authenticating the message by its IP and MAC address (together encrypting) and analysing the encrypted message to find the authenticity of the message and the node which has sent the message at collecting node will be carried out.***

Keywords :Wireless Sensor Networks(WSN),Data Aggregation Node(DAN), Data encryption standard (DES) and the Advanced encryption standards (AES),Cryptography,Encryption,Decryption, cipher text, Elliptic curve cryptography (ECC)

I. INTRODUCTION

Due to need for message authentication, to prevent threats of un authentified and morphed messages from being transferred in wireless sensor networks (WSN)[1], many message authorization methods have been formulated and developed which were related cryptographic technology. Symmetric key cryptographic systems or public-key cryptographic systems and also there are many different techniques available based on polynomial-based schemes, elliptic curve cryptography (ECC)[2] and so on. All the above methods have their own merits and demerits. In this research work a new method of authenticating the message by its IP and MAC address (together encrypting) and analysing the encrypted message to find the authenticity of the message and the node which has sent the message at collecting node has to be carried out.

A. Literature survey on Security of data in WSNs :

In WSNs security of data transmission is the major concern. Various security measures has been formulated to avoid the unauthorised injection of data into WSNs. Among these various security measures that have been proposed and formulated Cryptography[3][4] is the most important security system that is used widely.

Revised Manuscript Received on November 05, 2019.
* Correspondence Author
N.Shantha kumar*, Research Scholar, , Department of Computer Science and Engineering,Visvesvaraya Technological University,Belgaum,Karnataka E-mail:shanth86309@gmail.com
Dr.Hareesh.K, Associate Professor, Department of Computer Science and Engineering, Government Engineering College, K R Pet-571426.
Email: hareeshk.gec@gmail.com

B. Cryptography:

The phenomenon of converting readable format of data into unreadable format data and vice versa is called as Cryptography. The one who will have the secret key can convert the unreadable format of data into readable format of data.

Encryption: It is one of the most effective way of securing data. Encryption is the phenomenon of converting plain text into Cipher text(unreadable format).

Decryption: It is the phenomenon of converting the unreadable "Cipher text" into original readable format of data. Two very important categories of Cryptography are :

C. Symmetric key Cryptography:

In this Cryptographic system [5], [6] both the sender and receiver of the message transformation will share a unique, similar key which will be used for both encryption as well as decryption of the message. These cryptographic systems are simple and fastest , but the important drawback is , the exchange of key in a secured manner between both sender and receiver.

In this cryptosystem, plain text from the sender which has to be transmitted to receiver will be taken. Using any of the symmetric key algorithms eg.DES, the original text will be transformed into unreadable format of text (Cipher text). Here we make use of the secret key which will be shared among both sender and receiver. This unreadable secret format of data or text will be transmitted to the receiver. At the receiver end, the secured unreadable format of data will be transformed (decrypted) into original readable format of data using common key which was used for encryption.

An efficient and very famous symmetric-key cryptosystem is - the Data encryption standard (DES) and the advanced encryption standards (AES)

Data Encryption Standard (DES) : This Data encryption standard (DES),[7],[8] is one of the very effective and famous symmetric key encryption method. These standards were designed and implemented in 1975. Later on it was standardized by ANSI in the year 1981 as ANSI X.3.92[9][10]. This make use of a 56-bit key and utilises a block cipher process. This divides original text into 64-bit blocks and afterwards encrypts them.

Advanced encryption standard (AES): This is a symmetric 128-bit block text encryption process invented by Belgian Cryptographic experts Joan Daemen and Vincent Rijmen[11],[12]. As both the terms AES and Rijndael will be used very often in same meaning , very few variations exists among them .

Advanced encryption standard will be having a constant fixed size of block -128bits. The size of the key will be 128, 192, or 256 bits . But Rijndael may be specified using variable key and block size through a multiples of 32-bits. The minimum number of bits will be 128-bits and the maximum number of bits will be 256-bits .

D. Asymmetric cryptography:

Elliptic Curve Cryptography (ECC)

This cryptosystem ECC[13],[14], [15] defines a a fixed field in the group of solutions for an ECC y2=x3+ax+b together with an additive identity. When ECC was discovered, this algorithm has been explained and published general domain. Several experts found it as slow. Certicom focused on developing a still better development of the same algorithm keeping in mind the overall performance . After a very long,efficient and effective research , Certicom found and introduced the very first commercial toolkit to support ECC, and made it practical for usage in several applications.

II. PROPOSED WORK

A. Scope of Work :

In this research work a new method of authenticating the message in WSNs will be formulated. This has to be achieved by sending the message to the base station making use of both IP address and MAC address of the Data aggregation node (DAN). Analysing the encrypted message to find the authenticity of the message and the node which has sent the message at collecting node (Base station) has to be formulated.

B. Proposed Architecture:

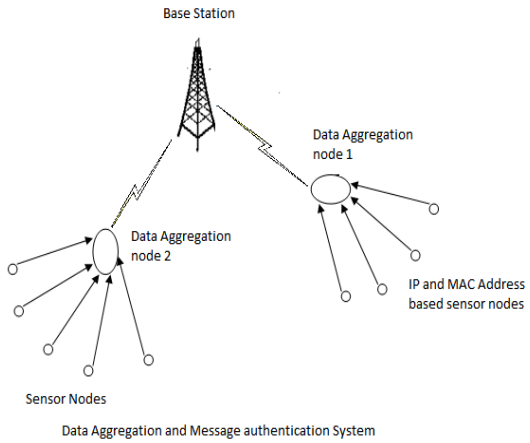

Figure 1: Framework of IP MAC-SDAMAS

The architecture mainly consists of DAN, Sensor nodes, and central base station. The sensor nodes will have the potential of sensing some feature or characteristic or attribute. It is capable of doing some limited processing of data. Also it can communicate with other neighbouring sensor nodes . The sensor nodes will be placed in 100s to 1000s in a given environment of application.

Data Aggregation Nodes are most important in WSNs. These nodes will gather required phenomenon from the deployed sensor nodes authentifies for fake or real sensor nodes using prescribed algorithm, then transfer the data to the Base station. Base station gathers the required set of data from DANs, while collecting the data it also checks for the genuinity of the sending DANs.

B. Methodology

The proposed model is as shown in the Figure.1. The sensor networks are divided into a disjoint set of nodes which can sense the environment under consideration. These sensible nodes gather the data through its surrounding area where been deployed . Later sends the collected set of data to DAN. At the DAN the data gathered from sensor nodes will be aggregated, which has the property of the network node (which is identified uniquely). DANs encrypts the aggregated data with its IP & MAC address. Later on DANs transmits the message (encrypted data along with IP & MAC address of DAN) to the Base station. Such DANs forms the WSN. At Base station the message is received and decrypted. Then the decrypted data has to be analysed for the genuines of sending DAN source, making use of the both MAC and IP address present at the received data.

Sensor nodes:

Sensor nodes are tiny devices which have the potential of sensing some phenomenon. It also carries out required processing of data. Then it also communicates among other sensor nodes. All nodes which are very sensitive will collect the data first from its surrounding environment where they has been deployed. Later they transmit the data to the DAN. Sensor nodes are usually placed in remote locations with the capability for extracting the energy from ambient sources to last long periods of time. These will perform, collecting sensitive data , communicating the processed data with other surrounding connected sensor nodes in the WSN.

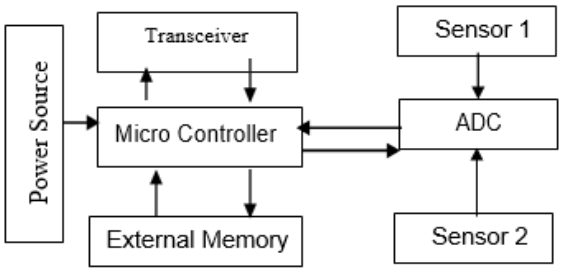

Figure .2 Sensor node's components

The sensor node will have the following components as shown in Figure.2 :

- Micro-controller
- Transceiver
- Power Source
- Sensors

Micro-controller

The micro controller carries out tasks of data processing. It coordinates the operations of remaining components as well.

Transceiver

ISM band provides free radio, spectrum allocation. The sensor nodes many a times makes use of ISM band Optical communication (Laser), Radio frequency (RF) and infrared are the mainly used wireless transmission media The infrared, just like lasers, they don't needs antenna but they are limited in their broadcasting capacity. Communication based on Radio frequency was the most appropriate that ensures almost all of the WSN applications. Transceivers combines the functionality of both transmitter and receiver.

Data is periodically collected and it is transferred to DAN[10]. In turn DAN is responsible for the secured data aggregation. According to the IF algorithm [5], the data aggregation will have required computation capability and can prevent sending data to DANs.

DAN Node

It is very important unit in WSN. The functions of DANs are to identify the genuine source, data aggregation, creating encrypted message and sending that message to the node which is identified as base station .Genuinity of nods is authenticated using IF algorithm[5]. The data from the sensor nodes will be collected by DAN. This will be aggregated and encrypted with the IP and MAC of DAN. The encrypted data along with IP and MAC address of DAN has to be transmitted to the Base station.

This research work lies in finding the genuinity of the source node (sensor) and the DANs. The data received from the sensor nodes has to be first checked for the genuineness,i.e.,whether the data is from fake node or the genuine node has to be verified. For this Algorithm 1 is proposed. Then once the genuineness of data is verified, it has to be aggregated by the DAN. After aggregation, the aggregated data will be encrypted along with the IP and MAC address of DAN. This encrypted data will be transmitted to Base station. At Base station the received data is decrypted, then the genuineness of DANs will be verified to avoid duplicate DANs.All these processes will be carried ut under Algorithm 2.

Base Station:

Base station [11] also plays a very important role in finding the genuine DAN. After receiving the encrypted data from the DANs, it will decode the encrypted data. Based on both IP address as well as MAC address obtained after the decryption of data, it will find and verify the gnuinity about the DANs. For encryption and decryption of the aggregated data standard encryption and decryption algorithm has to be adopted. The Algorithm 1 and Algorithm 2 are as shown below:

Algorithm 1:

To avoid the data receiving from nodes other than the genuine sensor nodes This algorithm will be designed with the information of the configuration of the sensor nodes, which is connected to the port of the DAN to finding the genuinity of sensor node.

Step 1 : In the WSN under consideration, data has to be collected from the sensory nodes,

Step 2 : Authenticate for the genuinity of the sending wireless sensor nodes referring IF algorithm[5].

Step 3 : Stop

Algorithm 2:

Here the IP-MAC of the DANs will be encrypted using the most efficient encryption algorithm which suits the application.

Step 1: Aggregate the data, which has been authentified in Algorithm 1

Step 2 : Encrypt the aggregated data along with the IP and MAC address of the DAN using the best suited encryption algorithm for this particular application.

Step 3 : The encrypted data has to sent to the base station

Step 4 : The received encrypted data needs to be decrypted .

Step 5 : Identify the genuinity of DANs

Step 6 : Stop

The performance of the methods used in our research work will be compared with performances of the existing frameworks

III. CONCLUSION

"A Primitive Proposal of an Algorithm for IP and Mac Based Data Aggregation and message authentication in Wireless Sensor Networks " by simulation , in this phase the results or outcomes of phase 1 and phase 2 will be thoroughly studied. Combining those two outcomes will be resulting in new algorithm .Implementation of Algorithm 1 is to avoid the data receiving from nodes other than the genuine sensor nodes. This algorithm will be designed with the information of the configuration of the sensor nodes, which is connected to the port of the DAN to finding the genuinity of sensor node. In implementation of Algorithm 2 IP-MAC of the DANs will be encrypted using the most efficient encryption algorithm which suits the application.

REFERENCES

1. Mohsen Razvani, Aleksandar Ignjativic Eliser Berno & Sanjay Jha " Secure Data Aggregation Techniquee for wireless Sensor Network in the presence of collusion Attacks" DOI 10.1109/TDSC.2014.2316816, IEEE Transactions on Dependable and Secure Computing.
2. Jian Li, Yun Li, Jian Ren, , and Jie Wu "Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks ",IEEE transactions on parallel and distributed systems, VOL. 25, NO. 5, MAY 2014.
3. Lei Yu, Member, IEEE, Jianzhong Li, Member, IEEE, Siyao Cheng,Shuguang Xiong, and Haiying Shen, Member, IEEE "Secure Continuous Aggregation in Wireless Sensor Networks", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 3, MARCH 2014.
4. Yan Sun, Hong luo and sajal k das " A Trust based frame work for Fault – Tolerent Data Aggregation in wireless multimedia sensor networks", IEEE Transactions on dependable and secure computing Vol 9 No 6 Nov/Dec 2012.
5. C. de Kerchove and P. Van Dooren, "Iterative filtering in reputation systems," SIAM J. Matrix Anal. Appl., vol. 31, no. 4,pp. 1812–1834, Mar. 2010.
6. S. Ozdemir and Y. Xiao, "Secure dataaggregation in wireless sensor networks: A comprehensive overview," Comput. Netw.,vol. 53, no. 12, pp. 2022–2037, Aug. 2009.
7. Z. Cai, S. Ji, J.S. He, and A.G. Bourgeois, "Optimal Distributed Data Collection for Asynchronous Cognitive Radio Networks," Proc. IEEE 32nd Int'l Conf. Distributed Computing Systems (ICDCS), pp. 245-254, 2012.

8. S. Ji and Z. Cai, "Distributed Data Collection and Its Capacity in Asynchronous Wireless Sensor Networks," Proc. IEEE INFOCOM, pp. 2113-2121, Mar. 2012.
9. y_ Y Ihuang, T. Lin, T. D. Nguyen, S.-I. Chu, and B.-H. Liu are with the Department of Electronic Engineering, National Kaohsiung University of Applied Sciences, 415, Chien Kung Rd. , Kaohsiung 80778, 2y'_T. Pham is with the Faculty of Information Technology, Pham Van Dong University, Quang Ngai 570000, Vietnam, "A New Overlap Circle Technique for Reducing Data Aggregation Time in Wireless Sensor Networks", 2017 International Conference on System Science and Engineering (ICSSE).
10. "Energy Efficient Data Compression and Aggregation Technique for Wireless sensor Networks", by B. Karthikeyan, R. Kumar, Srinivasa Rao2Inabathini ,School of Electronics Engineering, VIT University, Vellore, amilnadu, INDIA 2WIPRO Technologies, Chennai, Tamilnadu, INDIA
11. "A survey on privacy preserving data aggregation in wireless sensor networks", by D.Vinodha,Research Scholar, Anna University, Chennai Asso. Professor/CSE, S.A.Engineering,college, chennai, E.A.Mary Anita Professor/ CSE, S.A.Engineering College, Chennai.
12. "Efficient Data Aggregation in Wireless Sensor Networks with Multiple Sinks", by Gaukhar Yestemirova Robotics Department Nazarbayev University Astana, Kazakhstan , Sain Saginbekov Computer Science Department Nazarbayev University Astana, Kazakhstan. 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications.
13. "Preserving Data and Key Privacy in Data Aggregation for Wireless Sensor Networks", by V.Akila Computer Science and Engineering, Bharath University, Chennai , India; Dr.T.Sheela Information Technology, Sri Sai Ram Engineering College, Chennai , India
14. "Symmetric Concealed Data Aggregation Techniques in Wireless Sensor Networks using Privacy Homomorphism: A Review", by Josna Jose Assistant Professor College of Engineering, Cherthala, Joyce Jose Assistant Professor College of Engineering, Cherthala, Muhammed Ilyas H Assistant Professor College of Engineering, Cherthala.
15. " Reliable Routing Data Aggregation using Efficient Clustering in WSN " by Sneha Kamble Department of Computer Engineering G.H. Raisoni College of Engineering Management Pune, India, Tanuja Dhope Department of Computer Engineering G.H. Raisoni College of Engineering Management Pune, India. 2016 International Conference on Advanced Communication Control and Computing Technologies (ICACCCT)

AUTHORS PROFILE

N.ShanthKumar is a Research Scholar, Department of Computer Science and Engineering, Visvesvaraya Technological University, Belgaum, Karnataka. He received his B.E in Computer Science and Engineering from PESIT, Bangalore and M.Tech in Computer Science and Engineering from SJBIT, Bangalore. He has more than 10 years teaching experience in various reputed Engineering Colleges and universities. . He has authored many research papers in National reputed journals and conferences. His area of interest includes Computer networks, Data Communications, Web Technologies , Research methodologies, Data science, Database management systems, Software Engineering, Information Security, Entrepreneurship and management. His current research work includes Security in Wireless Sensor Networks.

Dr. Hareesh.K is a Associate professor in the Department of Computer Science and Engineering, Government Engineering College K.R.Pete, Karnataka, India. He received his Ph.D degree from Jawaharlal Nehru Technological University, Anantapur, A.P, India. M.Tech in Computer Science and Engineering from Visvesvaraya Technological University, Belgaum, India, and B.E in Computer Science and Engineering from Bangalore University. He has more than 20 years extensive academic, Industry and Research experience. He has authored more than 20 research papers in International / National reputed journals and conferences. His current research focuses on Network performance and analysis, Advanced Computer Networking, Mobile / Wireless Communication, Wireless Sensor Networks, Network Security, multimedia applications, P2P Networks and Web Technologies