ISSN No:-2456-2165

Security Management in Wireless Sensor Network (WSN)

Sumant Verma, Mr. Pradeep Baniya
Computer Science & Engineering Indore Institute
of Science & Technology Indore,
India

Abstract:- Wireless Sensor Network (WSN) plays a vital role in emerging sensing technology. They are used in various fields such as military operations, healthcare applications, traffic control, and home applications. Even sensor can monitor, pressure, humidity, noise level, temperature, soil makeup and other properties. Wireless Sensor Network can be of consist of different types of sensors like thermal, visual, infrared, acoustic and radar. Wireless Sensor Network (WSN) is broadcast nature of the wireless communication so it becomes easy for the attacker to send false data or false information to compromise the entire network due to which there are high chances that causes problem in making decision.

Here the solution proposed is MAC (Message Authentication Code), Authentication is necessary for many administrative tasks informally; data authentication allows a receiver to verify that the data really is sent by the claimed sender. If the message is from claimed sender then the message or information is accepted or if the message is from not from the claimed sender then the message or information is not accepted.

Keywords:- *Wireless Sensor Network (WSN), MAC (Message Authentication Code), Attacker, Security.*

I. INTRODUCTION

The Wireless Sensor Network (WSN) consists of sensors that are tiny in size and have the capability of sensing things and communicating with other devices, over a specific area. They are low cost solutions for variety of real world applications. Wireless Sensor Network (WSN) sensors are small in size and low power. Also the main problem of the sensor is that it has very low storage, so whatever algorithm or program is written for securing the network, it has to very small and efficient in order to work properly. Wireless Sensor Network (WSN) is broadcast in nature means the network can be compromised by the attacker. The attacks can target any node, this can lead to leak secret information and interfering message which ultimately violates security. Therefore authenticity is a mandatory service for securing Wireless Sensor Network (WSN), because message modification or message falsification is problems that need to be solved.

A. Architecture of Wireless Sensor Network (WSN):

Wireless Sensor Network (WSN) consists of following components:

- **Sensor Node**: - It is low powered, small in size and has low storage. It includes radio transceiver, an antenna, a microcontroller and for energy a battery.
- **Gateway**: - It enables communication between host application and field devices.
- **Network Manager**: - It is responsible for configuration of the network scheduling.

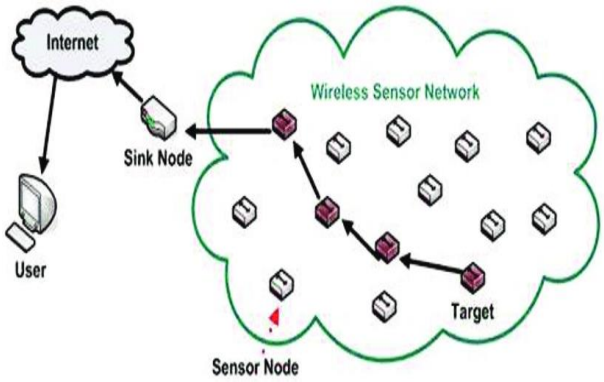

Fig. 1: Architecture of WSN

B. Advantages of Wireless Sensor Network (WSN):

- New nodes or devices can be added at any time.
- All nodes can be accessed through centralized monitoring system.
- Since it is wireless in nature so it is cost efficient as it does not require wires and cables.
- They can be used in variety of domains such as military, healthcare, agriculture, mines etc.

C. Disadvantages of Wireless Sensor Network (WSN):

- Sensors have low storage and low powered battery.
- It cannot be used for high speed communication due to low bandwidth.
- It is wireless in nature, so it can be hacked easily by the attacker.
- It is expensive to build such network.

D. Applications of Wireless Sensor Network (WSN):

- It can be used in environmental applications like to track movement of birds, small animals, and insects.
- It can be used in military applications.
- It can be used in health applications like to monitor a patient or monitor internal process of small animals.
- It can be used in agriculture applications like to monitor temperature, measuring water supply and so on.

ISSN No:-2456-2165

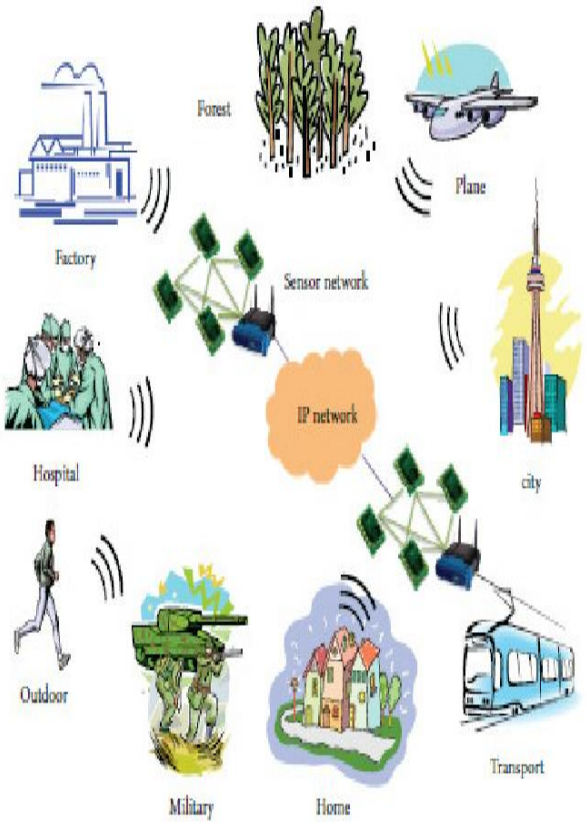

Fig. 2: Diagram of WSN Applications

II. RELATED STUDY

There are several proposals for implementing authenticity services on Wireless Sensor Network (WSN), the most are based on symmetric techniques and only a few ones involve public key cryptography indirectly. Symmetric cryptography offers low complexity in algorithms and small data pieces to manipulate and store. However scalability and flexibility are the drawbacks in these techniques. This approach has been explored in several proposals for implement security services using symmetric encryption, keyed and un-keyed hash functions and pre-distribution key techniques as proposed in the work of Du and Li among others.

Oliveira et al. proposed in a key distribution method that allows to two nodes to agree a common key. Oliveira's approach explodes the use of IBC to accomplish the key exchange.

- **Survey:** Many researchers have proposed the mechanism attacks. The research in field of security in Wireless Sensor Network (WSN) issues, challenges and solution which have been taken help are as follows:

Authors/Researchers	Description
Prachi Pathak and Amzad Quaz	Proposed directional antenna, cryptography and key management protocol. Classification of attacks in WSN.
Moises Salinas Rosales, Gina Gallegos Garcia, Gonzalo Duchen Sanchez	Proposed security solution through cryptography and MAC.
Prashant Shukla	Proposed security issues and challenges in WSN and provided the defense and counteraction research solution to the security.
Swati Bartariya and Ashutosh Rastogi	Identify the security threats and attacks in WSN with security solutions.
A.K. Nuristani and Jawahar Thakur	About security, challenges, solutions like MAC, key management, encryption.
Amit Kumar Gautam, Rakesh Kumar	Description on various trust management, authentication and key management schemes.
Kamlesh Kumar and Shibin David	Description on types of threats, challenges and solutions.
Jian Wang	Solving security problem by key management scheme.
Vishal Rathod and Mrudang Mehta	Solving security in WSN by trust management approach.
Shengjun Xie, Xiang Wang and Hua Shang	Clarifies structure of DC WSN for EIoT and prediction of possible attacks.
Fei Hu, jim Ziobro, Jason Tillett and Neeraj K. Sharma	Overview on secure routing, prevent of DOS and key management service.
Preetkamal Singh, Dr. OP Gupta and Sita Saini	Description about applications, challenges and security in WSN
Nidhi Chandra and Saima Maqbool	Security of WSN, its challenges and category of attacks.
Oladayo Olufemi Olakanmi and Adedamola Dada	Classification of WSN protocols and security and privacy issues.
Selcuk Uluagac, Christopher P. Lee and John A. Copeland	Description about confidentiality, authentication, integrity, access control, availability.

Table 1: Researchers/Authors with their methods and details

ISSN No:-2456-2165

III. PROPOSED SOLUTION

To know that the message or information is coming from actual sender we are using Message Authentication Code (MAC) in the Wireless Sensor Network (WSN). Here Message Authentication Code (MAC) contains cryptographic process. With the help of symmetric key the cryptographic process is implemented for sender and receiver. We have implemented in python language since it will take less memory as sensors consist of less and limited memory.

In the block diagram Fig 3, sender wants to send message and sender apply Symmetric Key (K) and generates MAC value say H1 then the message and MAC value H1 along with the message is received by the receiver. Now receiver will also calculates its MAC value say H2 with the same Symmetric Key (K) used by the sender. Then there will be comparison is done between MAC values H1 and H2. If MAC value H1 and MAC value H2 are same that means there is no change in the message by the attacker or hacker and we can accept that message. But if MAC value H1 and MAC value H2 are not same that means the message has been changed by the attacker or hacker and we cannot accept that message as the message is corrupted that can lead to misleading in taking important decisions.

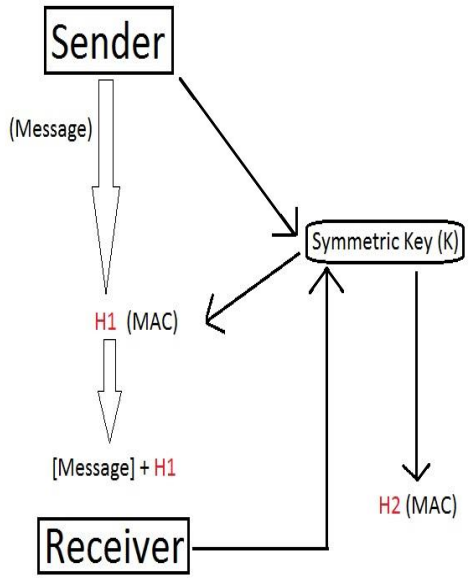

Fig. 3: Implementation Diagram

- **Proposed Program**

```
import hashlib
import base64

#Sender and Receiver share a secret key
secret_key = "secret key".encode()

#Sender generates MAC
message = "Information from sender!!!".encode()
sha256 = hashlib.sha256()
sha256.update(secret_key)
sha256.update(message)
h1mac = sha256.digest()

#Receiver receives and validates MAC
sha256 = hashlib.sha256()
sha256.update(secret_key)
sha256.update(message)
h2mac = sha256.digest()

if (h1mac==h2mac):
   print("---Message and MAC from Sender---")
   print(message,'***', h1mac)
   print("---Message and MAC from Receiver---")
   print(message,'***', h2mac)
else:
   print("Network Compromised")
```

S.No.	MODULE	DESCRIPTION
1.	hashlib	It is an interface for hashing messages easily. This contains numerous methods which will handle hashing any raw message in an encrypted format. The core purpose of this module is to use a hash function on a string, and encrypt it so that it is very difficult to decrypt it.
2.	base64	In Python the base64 module is used to encode and decode data. First, the strings are converted into byte-like objects and then encoded using the base64 module.

Table 2: Implemented Modules

S.No.	MODULE	DESCRIPTION
1.	encode	The encode() method encodes the string, using the specified encoding.
2.	update	Update the hmac object with *msg*.
3.	digest	This method is used to return the digested data which is passed through the update method.

Table 3: Implemented Methods

IV. CONCLUSION

This paper presents details study on the security of Wireless Sensor Network (WSN). Firstly, introducing about Wireless Sensor Network (WSN) in detail and then discussed about the security issue. Security is an important requirement because the application of Wireless Sensor Network (WSN) will be deeper and wider like in healthcare and military purposes. Wireless Sensor Network (WSN) product in industry will not get acceptance unless there is a full proof security to the network. There are limitations in sensors like low power energy and low space storage. To overcome the problem of security usually keeping in mind about the low storage, we provided Message Authentication Code (MAC) use, because of this it is guaranteed that the message is to from authenticated to the source. It takes less computing load, high security, less computing load, efficient utilization of resources such as memory, bandwidth, and power.

ISSN No:-2456-2165

REFERENCES

[1.] Jeevan Kumar and Sushanta Mahanty, Security in wireless network, IJERT, 2013
[2.] Nidhi Chandra and Saima Maqbool, Categorized security threats in WSN, International Journal of Computer Applications, February 2013
[3.] Prachi Pathak and Amzad Quaz, Issues, Challenges and Solution in WSN, International Journal of Electrical, 2017
[4.] Ankur Sirohi and Dr. Amit K. Agarwal, Security in (WSN), 2020
[5.] Zhang Huanan, Xing Suping and Wang Jiannan, Security and application of (WSN), ICICT-2020
[6.] Riaz Shaik and Shaik Shakeed Ahamad, Security Attacks and Challenges of (WSN), International Journal of Engineering & Technology, 2018
[7.] Saqib Ali, Taiseera Al-Balushi, Omar Khadeer Hussain, Improving The Resilience of WSNs Against Security Threats, IJT, 2018
[8.] Selcuk Uluagac, Christopher P. Lee and John A. Copeland,Designing Secure Protocols for WSNs
[9.] Fei Hu, jim Ziobro, Jason Tillett and Neeraj K. Sharma, Secure (WSN):Problems and Solutions, IEEE
[10.] Hyung-Woo Lee and Choong Seon Hong, Security in (WSN):Issues and Challenges
[11.] Preetkamal Singh, Dr. OP Gupta and Sita Saini, A Brief Study of WSN, Advances in Computational Sciences and Technology, 2017
[12.] Shengjun Xie, Xiang Wang and Hua Shang, Security Analysis on WSN in the Data Center for Energy Internet of Things, 2020
[13.] Vishal Rathod and Mrudang Mehta, Security in WSN, Ganpat University Journal of Engineering & Technology, 2011
[14.] A.K. Nuristani and Jawahar Thakur, Security Issues and Comparative Analysis of Security Protocols in WSN, JCSE, 2018
[15.] MOISES SALINAS ROSALES, GINA GALLEGOS GARCIA, GONZALO DUCHEN SANCHEZ, Efficient Message Authentication Protocol for WSN, Issue 6, Volume 8, June 2009
[16.] M. B. Apsara, P. Dayananda, C. N. Sowmyarani, A Review on Secure Group Key Management Schemes for Data Gathering in Wireless Sensor Networks, Vol. 10, No. 1, 2020
[17.] Amit Kumar Gautam, Rakesh Kumar, A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks, 09 January 2021
[18.] Oladayo Olufemi Olakanmi and Adedamola Dada, Wireless Sensor Networks (WSNs): Security and Privacy Issues and Solutions, Submitted: August 28th, 2018 Reviewed: February 6th, 2019Published: March 29th, 2020.
[19.] Prashant Shukla, Security Issues, Challenges and Solutions for Wireless Sensor networks
[20.] Mauricio Tellez Nava, Improving the security of WSN, 2016
[21.] Jaydip Sen, Security in Wireless Sensor Networks
[22.] M.B. Apsara, P.Dayananda and C.N.Sowyarani, A Review on Secure Group Key Management Schemes for Data Gathering in WSN, Vol. 10, No. 1, 2020
[23.] Jian Wang, Secured Communications in Wireless Sensor Networks
[24.] Swati Bartariya and Ashutosh Rastogi, Securtiy in Wireless Sensor Networks: Attacks and Solutions, IJARCCE.