ABSTRACT: In Wireless Sensor Networks (WSNs), the data discovery and dissemination protocol allows distribution and updating data in sensor nodes. But there exist two drawbacks in existing protocols: Centralized approach is not suitable because data dispense is done only by base station. Another drawback is lack of invincibility which leads to impairments in network. To overcome these drawbacks, this project put forward an enhanced distributed approach. This approach helps network owners to provide different rights to the multiple network users to directly disseminate data items all at a time to the sensor nodes and deal with a number of possible security vulnerabilities. This paper shows the design and implementation of a prototype which is developed using java.

KEYWORDS: Invincible Data Dissemination, Distributed, Wireless sensor networks.

INTRODUCTION

Wireless sensor networks (WSN) are basically distributed networks or a collection of sensor nodes which collect information are used to analyse physical or environmental conditions. Distributed data discovery and dissemination is an increasingly relevant matter in WSNs, especially in the emergent context of shared sensor networks, where sensing/communication infrastructures from multiple owners will be shared by applications from multiple users. These networks are owned by multiple owners and used by various authorized third-party users. Moreover, it is expected that network owners and different users may have different privileges of dissemination. In this context, distributed operation by networks owners and users with different privileges will be a crucial issue. Applications of WSN include habitat monitoring, industrial applications, battlefield surveillance, smart homes etc.

The sensor nodes in WSN need the updating of data. This can be done by using data dissemination protocols. Note that this is different from code dissemination protocol. But the existing protocols suffer from the single point of failure as dissemination is impossible when the base station is not functioning or when the connection between the base station and a node is broken. In addition, the centralized approach is inefficient, non-scalable, and vulnerable to security attacks that can be launched anywhere along the communication path.

The main purpose of this project is to propose an invincible data dissemination approach. This distributed approach provides security technique and formally proves the authenticity and integrity of the disseminated data items. Advantages of this approach are:

i. It allows the network owners to authorize the network users to disseminate the data.
ii. It is not vulnerable to attacks.
iii. They don’t rely on the base station.
II. RELATED WORK

In the existing approaches, Design of an application-cooperative management system for wireless sensor networks is a Dissemination protocol and is based on Trickle algorithm and establishes an independent trickle for each variable in the data was introduced in 2005[1]. In 2008, Data discovery and dissemination with Dissemination Protocol (DIP) was proposed which Detect and identify which nodes need which updates[2]. It is based on the concept of version number and key tuple for each data item. In 2009, DHV: a code consistency maintenance protocol for multi-hop wireless sensor networks which ensure that every node in a network will eventually have the same code[3]. Also enables protocol to decide when to begin transferring a new code. Later in 2012 DiCode: DoS-resistant and Distributed code dissemination in wireless sensor networks was put in forward to Distribute large binaries to reprogram the whole network of sensors[4]. In 2013, secure data discovery and dissemination protocol named SeDrip based on hash tree for wireless sensor networks were proposed[5]. It is Secure, lightweight, and DoS-resistant data discovery and dissemination protocol.

More importantly, all existing data discovery and dissemination protocols employ the centralized approach which leads to inefficient network.

III. SYSTEM ARCHITECTURE

System architecture comprises of five modules:

1. Data Owner: The Data Owner has to login to the system using his credentials later browse the required file, initializes nodes with digital signature and uploads to the end user.
2. Router: Router receives data from data owner. The router performs the following operations such as Initialize MAC for all packets and nodes, Receive Data, check for authorized users, Find Path based on the distance and check attackers.
3. IDS Manager: The IDS manager is nothing but Intrusion Detection System manager which is responsible to filter the malicious data and traffic data.
4. Receiver: the receiver can receive the data file from the Service Provider which is sent via Router. If malicious data is found in the router then it is not forwarded to the receiver.
5. Attacker: Attacker attacks the nodes and tries to modify the data.

As shown above, figure 1 represents the system architecture which show all the 5 modules. Relation between the five modules is also shown in the figure 1.
IV. IMPLEMENTATION

In this distributed approach Elliptic Curve Cryptography (ECC) is used for providing invincibility. Below steps describe the working of ECC:

**Key Generation**
1. Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver’s public key and the receiver will decrypt using its private key.
2. Now, we have to select a number ‘d’ within the range of ‘n’.
3. Using the following equation we can generate the public key: \[ Q = d \times P \]
4. \( d \) = The random number that we have selected within the range of \((1 \text{ to } n-1)\). \( P \) is the point on the curve. ‘Q’ is the public key and ‘d’ is the private key.

**Encryption**
1. Let ‘m’ be the message that we are sending. We have to represent this message on the curve. Consider ‘m’ has the point ‘M’ on the curve ‘E’. Randomly select ‘k’ from \([1 \text{ to } (n-1)]\).
2. Two cipher texts will be generated let it be \( C_1 \) and \( C_2 \).
3. \( C_1 = k \times P \)
4. \( C_2 = M + k \times Q \)
5. \( C_1 \) and \( C_2 \) will be sent.

**Decryption**
1. We have to get back the message ‘m’ that was send to end user: \( M = C_2 - d \times C_1 \)
2. \( M \) is the original message that we have sent.

The outcome of the project will be as follows:
1. Data owner browse the file that need to be sent to the end user. Later initiates the MAC for the data browsed. For security purpose the data will be encrypted and sent to end user. After each step the successful pop-up message will appear.

![Fig.2. Data owner activities](image-url)
2. Transferring data to the end user: This data transfer takes place after the data owners initiates MAC, encrypts it and sends to the end user. The transfer of data through nodes can be seen in figure as they are marked green in color once they receive and send data to next node.

![Data Dissemination](image)

Fig. 3. Data dissemination

V. RESULTS

This shows the time taken for transferring data to the end user with delay and also it shows the delay time taken when attacker is going to attack the nodes i.e. comparison between attacked nodes and safe nodes.

![Overall Delay](image)

Fig. 4. Overall Delay during transferring data
VI. CONCLUSION

In this paper, an invincible and distributed data discovery and dissemination approach is proposed. In order to pass the signature verification of sensor nodes, each user has to submit his/her private key and dissemination privilege to the network owner for registration. Authorized users are capable of carrying out dissemination in an adistributed manner. To provide flexibility, each user may be assigned a certain privilege level by the network owner. A sensor node can only accept data items disseminated by authorized users. Also, a sensor should be able to ensure that received data items have not been modified during the dissemination process. Thus, this distributed approach can formally prove the authenticity and integrity of the disseminated data items in WSN.

REFERENCES


BIOGRAPHY

Chaitra Nagappa Barki is currently pursuing M.Tech in Computer Network Engineering, Department of Information Science, SJB Institute of Technology, VTU, Bengaluru, India. Her area of interest includes Computer networks, Wireless sensor network etc.

Abhilash C.N. is currently working as Associate Professor Department of Information Science and Engineering, SJB Institute of Technology, VTU, Bengaluru, India. He obtained his Bachelor of Engineering in Dr.AIT, Bengaluru. He received the Master of Engineering Degree from UVCE Bengaluru, India. He has 9 years of teaching experience. Currently he pursuing in the Department of Computer Science and Engineering, UVCE, Bangalore University, Bengaluru. His research interests are Wireless sensor network, Ad hoc network, Computer network, etc.