International Journal of Innovative Research in Information Security (IJIRIS) ISSN: 2349-7009(P)
Issue 05, Volume 04 (May 2017) SPECIAL ISSUE www.ijiris.com ISSN: 2349-7017(O)

Reliable and Efficient Data Discovery and Dissemination Using Decentralized Approach in Mobile Wireless Sensor Networks

Poornima Bhat H[1], Vinita Soaries[2], Shifana Begum[3]
[3]Asst.Professor, [1,2] Final Year UG Student,
Dept. of CSE, Srinivas School of Engineering,
Mangalore,India

Abstract*- Data dissemination is the process by which queries of data are routed in the sensor network. The data collection by sensor nodes has to be communicated to the base station or to any other node interested in the data. Data discovery and dissemination protocol for WSNs is responsible for updating configuration parameters of and distributing management commands, to, the sensor nodes. All existing data discovery and dissemination protocol suffer from two drawbacks. First, they are based on the centralized approach; in centralized approach only the base station can distribute data items, such an approach is not suitable for emergent multi-owner--multi-user wireless sensor networks. Second, those protocols were not designed with security in mind and hence adversaries can easily launch attacks to harm the network. This paper proposes the first secure and distributed data discovery and dissemination protocol called DiDrip. It allows the network owners to authorize multiple network users with different privileges to simultaneously and directly disseminate data items in to the sensor nodes based on the design objective we propose DiDrip. This is the first distributed data discovery and dissemination protocol, which allows network owners and authorized users to disseminate data items into WSNs without relying on the base station. Here implements the multi hop data transmission in the network while transmitting data prioritization given to the data. There are three types of data packets low, medium and high by using dynamic algorithm and improves the quality of service.

***Key words*- MWSN, Distributed Data Discovery, DiDrip, DSDV.**

1. INTRODUCTION

A wireless sensor network sometimes called a wireless sensor and an actuator network [1], that are spatially distributed autonomous sensors to monitor physical or environmental conditions [2], such as a temperature, sound, pressure, etc. and cooperatively pass their data through the network to a main location. The Wireless Sensor Networks is built "nodes"- from a few to several hundreds or even thousands where each node is connected to one sensor. Each sensors network node has several parts; a radio transceiver with an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. The cost of sensor nodes is similarly variable ranging from a few to hundreds of dollars, developing on the complexity of the individual sensor nodes, size and cost contains on sensor nodes, result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. These sensor nodes pass the information that they collect to a prime location called base station. In most systems, a WSN communicates with a LAN or WAN through a gateway like medium. The gateway is actually a bridge between the WSN and various other sensor networks. This allows the data to be stored by devices and which can be taken up for processing later. After a wireless sensor network is deployed there is usually a need to update buggy or old small programs or parameters stored in the sensor nodes. This can be achieved by the so called data discovery and dissemination protocols, which facilitates a source to inject small programs, commands, queries, and configuration parameters to sensor nodes. Note that it is different from the code dissemination protocol [3] [4]. All proposed protocols assume that the operating environment of the WSN is trustworthy and has no adversary. In this paper mainly consists of two approaches first one is centralized and the second one is distributed in centralized approach data items can only be disseminated by the base station. The disadvantage of centralized approach is there may be chances of suffering the single point of failure as dissemination is impossible when the base station is not works properly or when the connection between the base station and node is broken.

Motivations by the above observations, this paper has the following main contributions:

The need of distributed data discovery and Dissemination protocols is not completely new, but previous work did not address this need. We identify these security vulnerabilities in existing data discovery and dissemination protocols. Based on the design objectives, we propose DiDrip. It is the first secure and distributed data discovery and dissemination protocol, which allows network owners and authorized users to disseminate data items into the WSNs without relying on the base station. In particular, we apply the provable technique to formally prove the authenticity and integrity of the disseminated data items in DiDrip. Also demonstrate the efficiency of DiDrip in practice by implementing it in an experimental WSN with resource limited sensor node. This is also the first implementation of a secure and distributed data discovery and dissemination protocol.

III. PROBLEM STATEMENT

3. ***Data discovery and dissemination of security*** vulnerability

3.1 Review of existing Protocols

The underlying algorithm of both DIP and DRIP is Trickle. This requires each node to periodically broadcast a summary of its stored data. When node has received an older summary, it sent an updates to the source. Once all nodes have unchanging data then the broadcast interval is increased exponentially to save energy. In other words, Trickle can disseminate newly injected data very quickly. Among existing protocols the Drip is the simplest one and it runs an independent instance of Trickle for each data item.

3.2 security vulnerabilities

An adversary can first place some intruder nodes in the network and then use them to alter the data being disseminated. This may result in some important parameters being erased or the entire network is being rebooted with wrong data. For example, consider a new data item (key, version, data) being disseminated. When a raider receives this new data item, then it can broadcast a malicious data item <key, version*, data*> where version*> version. If data* is set to 0, the parameter identified by key will be erased from all sensor nodes. Alternatively, if data* is different from data, all sensor nodes will update the parameters according to this forged data item. Note that the above attacks can also be launched if an adversary compromises some nodes and has access to their key materials.

Fig.1 Existing System architecture

IV. PROPOSED SYSTEM

4.1 DiDrip

DiDrip is the first secure and distributed approach of data discovery and dissemination of data items to the sensor nodes. The application by multiple users share the communication infrastructure and sensing infrastructure of the multiple owners and the different users. There are four phases in DiDrip, system initialization phase, user joining phase pre-processing phase and packet verification phase.

Fig.2 Proposed System architecture

4.1.1 System Initialization Phase

Here we defining type of the algorithm used for public key operations and achieve strong robustness of packets against various maliciousattacks. Admin of a DiDrip will take care of topology maintenance, algorithm used for cryptography.

4.1.2 User Joining Phase

Here nodes and privileged owner are registering with Admin node for communication between multiple nodes. User which registered as a owner will disseminate packets to get node status to check nodes are attacked or not.

4.1.3 Packet Pre-processing Phase

When the owner needs to disseminate data items is must construct the data packets using algorithm defined in system initialization phase. Nodes also needs to be follow up same algorithm to transmit a data to destination.

4.1.4 Packet Verification Phase

Here nodes after receiving a data from sender node checks for reliability, consistency of a received packet by verifying received packet integrity. By decrypting received packet using public key. If verification of packet successful than only nodes considering received packet is free from any kind of attack.

4.2 HACKER SCENARIO

4.2.1 Scenario 1 :- IP Spoofing

Here hacker will spoof the IP address of a valid any node of a network and acts hacker as a valid node. He can transmit and receive that. To provide solution here, we are using a unique identification of a device (Motherboard Id, BIOS Id, Hard Disk ID). Suppose Hacker receives a data, we are provided security for data converted into cipher text using AES algorithm. Without knowing key value not able to decrypt it.

Scenario 2 :-Brute Approach for IP broadcast

Here hacker will write a brute force approach for IP broadcast, brute force program will continuously pinging all the IP address in range. To provide solution here we are validating IP address and action string of a request and format a request data.

V. LITERATURE SURVEY

D. He, C. Chen, S. Chan and J. Bu Proposed "Dicode: denial-of-service- resistant and distributed code dissemination in wireless sensor networks," which circulate large binaries to reprogram the whole network of sensors. Considering the sensor nodes could be distributed in a comfortless environment, remotely disseminating such small data to the sensor nodes through the wireless channel is a more preferred and practical approach than manual mediation.

Disadvantage: through the wireless channel Remotely disseminating such small data to the sensor nodes is a more preferred.

T. Dang, N, Bulusu, W. Feng and S. Park proposed "DHV: A code consistency maintenance protocol for multi-hop wireless sensor network," an efficient code consistency maintenance protocol to certify that every node in a network will ultimatly have the consistent code. The proposed protocol assumes that the operating environment of the WSN is trustworthy and has no adversary.

Disadvantages: Adversaries exist in reality and impose threats to the normal operation of WSNs. These are based on the centralized approach.

D. He, S. Chan, S. Tang, and M. Guizani Proposed "Secure data discovery and dissemination based on hash tree for wireless sensor networks," identifies the security vulnerabilities in data discovery and dissemination when used in WSNs identifies the security vulnerabilities in data discovery and dissemination when used in Wireless Sensor Networks. The proposed system protocol provide instantaneous authentication without packet buffering delay, and tolerate compromise.

Disadvantage: This paper suffers from the single point of failure as dissemination is impossible when the base station is not functioning or when the correction between the base station and a node is broken.

VI. WORKING

6. Design and implementation

We can choose Drip for performance comparison.

6. 1Experimental setup

According to this paper we have written programs that will event functions of network owner, user, and sensor node. The network owner and user side programs are JAVA programs using Netbeans 9.X IDE and running on laptop PCS under Windows10 with 2GB RAM environment. For front end Swings/AWT API and for networking Sockets API are used.

6.2 Registration Module

6.2.1 Node Registration Module

While registering, we are passing Node Name, Password and Unique Identification values like (Motherboard ID,BIOS ID, Hard Disk Id) for data dissemination purpose. Server will provides a key for registered nodes for Encrypting/ Decrypting a content.

6.2.1 Node Registration Module

While registering, we are passing Node Name, Password and Unique Identification values like (Motherboard ID,BIOS ID, Hard Disk Id) for data dissemination purpose. Server will provides a key for registered nodes for Encrypting/ Decrypting a content.

6.3 Server Node Operation Module

To update IP address and routing table of a network, here node has to enter its password to update details.

Fig.3 Node Registration Snapshot

6.3.1 Sender/Receiver

Here user will select a text file name. If text file having content then we will read a text file content and encrypting it(cipher text).User has to select a destination node and calculate the shortest path using Find Path Button. Here shortest path algorithm will work. To calculate a shortest path, we have implemented a our new generic algorithm.

6.3.2 Verify Path

Here we are sending a request to User node to validate calculated path is secure or not. User nodes will responds to requested node as path secure or not.

6.4 User Registration Module

In Fig.3 User will register with Server using Name, Password and Unique Identification values like (Motherboard ID,BIOS ID, Hard Disk Id) and serverwill produces a Secret Encryption key for communicating with Server to get data dissemination details of a Nodes and providing key for communication.

Fig. 4 User Registration Snapshot

Fig.5 Server Node Snapshot

In Fig.4, Server can check the status of Nodes using Check status which will gives Node name, password, Data dissemination details. Server/Admin will configure a Routing table values/IP address of a Nodes and Users.

6.5 Data Transmission Module

Consider a scenario where Node 1 wants to transmit a data to Node4:-

- Node 1 will select text file.
- Node 1 will select a destination node and calculate a shortest path.
- Node 1 will send a request to the Users1 for validate path.
- Once User1 response as a success then Node1 will generates a packet like -

Plain Text + Cipher Text + Enc Key + plain text Mac + Cipher Text Mac = Packet

At the Receiver End

- Node 4 will receives the data
- Verify the data whether received packet is valid or not

Received packet like :- Plain Text + Cipher Text + Enc Key + Mac code

Step 1 :- Node 4 will first takes Plain text and generates a cipher text and cross check with received cipher text.

Step 2 : - Takes cipher text and generates a plain text and cross check with received plain text.

Step 3 :- Generates MAC(Message Authentication Code) for received plain text and cross check with received Plain MAC code.

Step 4 :- Generates MAC(Message Authentication Code) for received cipher text and cross check with received Cipher MAC code.

Once all these steps successful than only Node 4 will consider received data is valid One.

VII. CONCLUSION AND FUTURE WORK

In this paper we have identified the security vulnerabilities in data discovery and dissemination when used in Wireless sensor networks which have been not addressed in previous research. Also some of data discovery and dissemination protocols have been proposed, but none of those approaches support distributed operation. Therefore, in this paper, a secure and distributed data discovery and dissemination protocols named DiDrip has been proposed. Besides analyzing the security of DiDrip, this paper has also reported the evaluation of DiDripin an experimental network of resource-limited sensor nodes, which shows that DiDrip is feasible in practice. We have also given a formal proof of the authenticity and integrity of the disseminated data items in DiDrip. Also due to the open nature of wireless channels, we can easily intercept.

REFERENCES

[1]. Ashwini and Dr.Chandrakant Naikodi, “Integrity of Data Discovery and Dissemination to Improves the Quality of Service in WSNs”,vol 5, pp.790-991, May 2016.

[2]. F. Akyildiz and I. H. Kasimoglu, “wireless sensor and actuator network: research challenges: Adhoc networks, vol 2, No. 4, pp. 351-367, oct 2004.

[3]. “Environmental and temperature monitoring”, centrak.

[4]. J. W. Hui and D. Culler,“The dynamic behavior of a data dissemination protocol for network programming at scale,” in Proc. 2nd Int. Conf. Embbeded Netw. Sensor Syst., 2004, pp.81-94.

[5]. D. He, C. Chen, S. Chan, and J. Bu, “DiCode: DoSresistant and distributed code dissemination in wireless sensor networks,” IEEE Trans. Wireless Commmun., vol. 11, no. 5, pp. 1946-1956, may 2012.

[6]. A. perrig, R. Canetti, D. Song, and J. Tygar, “efficient and secure source authentication for multicast,” in Proc. Netw. Distrib. Syst. Security symp., 2001, pp. 35-46.

[7]. Y Chen, I. Lin, C. Lei, and Y. Liao, "Broadcast authentication in sensor networks using compressed bloom filters," in Proc. 4th IEEE Int. Conf. Distrib. Comput. Sensor Syst., 2008, pp. 99-111.

[8]. D.He,S.Chan,S Tang, and M. Guizani, "Secure and distributed data discovery and dissemination based on hash tree for wireless sensor networks," IEEE Trans. Wireless commun., vol.12, no. 9,pp. 4638-4646, Sep. 2013.

[9]. A. Perrig, R. Canetti, J. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in Proc. IEEE Security Privacy, 2000, pp. 56-73.

[10]. G. Tolle and D. Culler, "Design of an application-Cooperative management system for wireless sensor networks," in Proc. Eur. Conf. Wireless Sensor Network., 2005, pp. 121-132.

[11]. R. Merkle, "Protocols for public key cryposystems," in Proc. IEEE security privacy, 1980, pp. 122-134

