ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Secure and Discovery of Distributed Information and Spreading In Wireless Sensor Networks

Pattanashetti Vijay Iranna[1], B.N.Veerappa[2]

M. Tech Student, Dept. of Studies in CS&E, UBDTCE, Davanegere, India[1]

Associate Professor, Dept. of Studies in CS&E, UBDTCE, Davanegere, India[2]

ABSTRACT: In wireless environment, it can easily discover the data and disseminate information. It has two types of approaches. These are centralized, distributed. The Centralized approach has basestation is responsible for sending information. The Distributed approach is very flexible. It enables multi-owner multi-user policy which is the key for distributed system. For this, a new protocol called "SDDISWSN" can be abbreviated as Secure and Discovery of Distributed Information & Spreading in WSNs which provides security i.e. Authentication, Data integrity & also reduces the communication cost.

KEYWORDS: Wireless Sensor Networks, SDDISWSN,Multi owner-multi user policy, Authentication, Data integrity.

I. INTRODUCTION

The wireless sensors network (WSN) always needs some control information, command. It may call query information about nodes in networks. Once the information is received, all other nodes will be having these values. Information discovering and placing in the next node. According to sensors networks, It makes chain of nodes to the destination. This concept is widely used by Indian army of the borders. It gives sensual information about the authorised military commandos time to time from change of information. Here we use temperature, control information, etc. be for we can use Wireless sensors networks. This might be binary tens of kilo byte information about control or the necessary information and code dissemination. The information needs two byte is usually for data send. It uses the protocol SDDISWSN as Secure and Discovery of Distributed Information and Spreading In Wireless Sensor Networks for providing security in distributed approach.

The Fig.1 in next page shows two approaches i.e. centralize and Distributed approaches to sending very important information like buggy or configuration information which is shown in the figure.

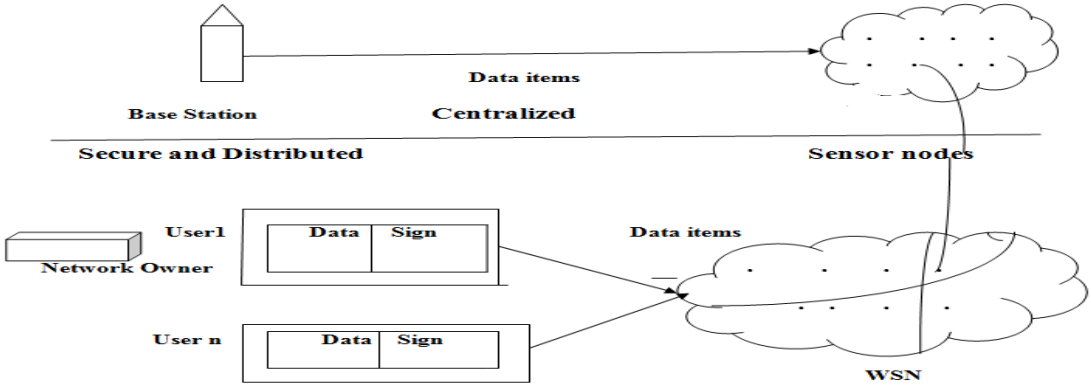

Fig 1: Line separating Distributed and centralized View.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

In centralized approach it uses the base station to send control information. If it fails, there is a problem that we have to face single point of failure. But, conversely other part describes distributed system with security. The security can be produced by using a protocol named SDDISWSN. The user will take permission from network owner and signs the data packets and it will be disseminated in the wireless sensor networks. The spatially located nodes will pass the data. Again we know that in wireless sensor network, we can send sensitive information. If we take for example buggy information (will be updated in all nodes) then we can control that geographical location. Similarly, for parameter like temperature etc.

Let us consider the nodes can be distributed among environment remotely. From Sensing, such data to nodes via WSN.It is good practical than manual intervention. In the literature many secure data discovery is spreading information has been introduced are considered as state of the art protocols. More existing protocols have centralized method. As shown in above figure, the base station will only disseminate information. The centralized approach is not efficient and vulnerable. In this work it is the need of authentication and DoS resistant data required a lot.

II. RELATED WORK

In[1] author proposed aSecure Data Discovery and Dissemination based on Hash Tree for Wireless Sensor Networks. After reading this paper, it came to know that the hash tree concept lagging from security and it needs a protocol which provides Security more. It uses the Merkle hash tree concept using this it produces hashed data. When it reaches to respective nodes, the data will be un- hashed. The correct data will be delivered to particular node. The Merkle hash tree is binary tree. It uses three phases. Those are System initialization phase, Packet pre-processing phase and Packet verification phase.

The tree with depth two can be e1||e2, e3||e4 and at level height with one. $e_{1\text{-}4}$is at height two. Like, this can be used for many nodes. This paper uses Merkle concept. Also they worked on puzzled approach for more security.

In[2] author proposed a Secure and Distributed Data in Wireless Sensor Network**,** When I go through this paper, it was come to know that, It is SDD(name of the protocol) Secure data discovery which is good as per consideration of results. They distributed the work into four phases. Those are system initiation phase, initializing the prime numbers p, q, private key and public key. The user joining phase can be intended to user with private key, public key and user identity. That will be sent to network owner. It sends the certificate to the user. Then data packet pre-processing takes place. Then finally at verification phase, received data will be verified. But it gives more delay and less security.

In[3] author proposed a Lightweight and Confidential Data Discovery and Dissemination for Wireless Body Area Networks. The survey of this paper, it is found that the protocol is not providing security for WBANS i.e. Wireless body area networks. These are application oriented networks. To handle this, it is developed, a protocol for only Lightweight and Confidential Data finding and spreading in Wireless Body Area Networks. It is practically feasible. Using simple symmetric algorithms the confidentiality can be gained. By looking at it, result is good.

The comparison between WBANs, traditional WSNs with respect to communication Resource, physical comprise of body sensor nodes, Mobility etc. It brings more instability and vulnerable.

In[4] author proposeda Secure and Distributed Data Discovery and Dissemination in Wireless Sensor Networks.This paper, it is detected vulnerability in data discovery and spreading information on wireless sensor networks. For distributed approach they developed protocol called DIDRIP (name of the protocol). They evaluated and analysed the protocol.

They implemented multi-owner multi network. The data dissemination with data discovery with buggy information they developed protocol DIDRIP but security point of consideration it is very less. They are four layers each layer does some work according functionality assigned. The first layer initializes system with various variables like primes, private, public key. Similarly with discussed papers, above layers in different literature survey. They

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

implemented different user privileges, authenticity and data integrity, user accountability etc. This protocol is computational and communicational.

III. METHODOLOGY

A. SDDISWSN

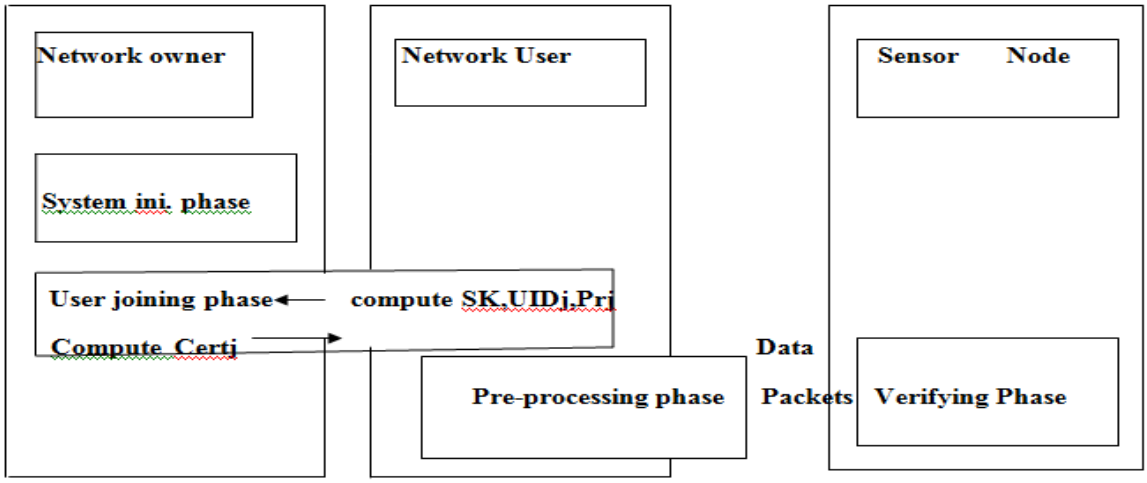

Fig 2: Different phases flow of information in SDDISWSN

There are four phases in the SDDISWSN protocol. The protocol can be pronounced as Secure and Discovery of Distributed Information and Spreading in Wireless Sensor Networks. Let see the four phases in Fig: 2, by it can be implemented according to protocol requirement. One issue is about security.The classes are OWNER, USER and SENSORNODE. Owner has properties give permission, read parameters, request, reply to user.

Let us see one by one. The read property will read the prime numbers, private key and public key and takes further action. If number generated is not prime then it rejects request. Otherwise, it puts into account and replies with certificate. The certificate has privileged user information. It is responsible for most working correctly. It can be combined in well suited functions i.e the functions in terms of phases explained.

1. System initialization phase

The parameters like public key, private key, and two prime numbers say as p,q will be assigned by random value or generated value. The parameters will be preloaded in the node. As the name itself indicates the node will be initialized with the prime numbers, private key value and private value. The private value and public value will be generated using the alphabets and numbers. Each time the unique combination of private and public key will be generated.

2. User joining phase

The user U_j will compute the parameters for j as private key, public key and sends three parameters identity of user U_j, public key of user U_j, and dissemination parameter for user j then the certificate will be generated. It means that the user joined the on-going process. If anybody tried to change the certificate, this will cause error in verification phase. It will be discussed next. The certificate contains signature and various parameters that was input. As above said there will be details of privileged user will be there.

3. Packet Pre-processing phase

Each packet will be formed as Data items which consist signing of data. It will be like both constructing data packets and signing. This is what packet pre-processing (Fig.1). With the help of hashing technique, we can process the

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

data items. Using chained hashing we may do this one and achieve packet pre-processing. In the sense layering with data and achieving no data change. As in thesis, it has been told the hash tree can be used for hashing.

4. Packet Verification phase

This is the phase in which the data packets will be verified. If it is same public key as per original it will give result as correct else there is wrong data packet trying to pretend like something original. Actually first authentication is done by Certificate with and integrity of data packet will be checked by validity digital signature. Likewise the data will be updated if it is verified successfully

IV. TEST CASES

The below table 1 contains the text cases. Each text case takes the input and processes it. If it is with standard case then the status of execution will be PASS else it will be FAIL. For example TC02. After running the project if there is no change in certificate and updating in sensor node then status of execution will be PASS. Likewise for all remaining test cases it will be processed.

Test case no.	**Description**	**Input**	**Output**	**Status of Execution (PASS/FAIL)**
TC01	Run project	Certificate change	No updating in sensor node	FAIL
TC02	Run Project	No change in certificate	Updating in sensor node	PASS
TC03	Run project	No generation of primes	No security will be enabled	FAIL
TC04	Run Project	No private & public key is generated	No user will be generated	FAIL
TC05	Run Project	No detection of user	No data is sent	FAIL

.Table 01: Test cases

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

V. RESULT AND DOCUMENTATION

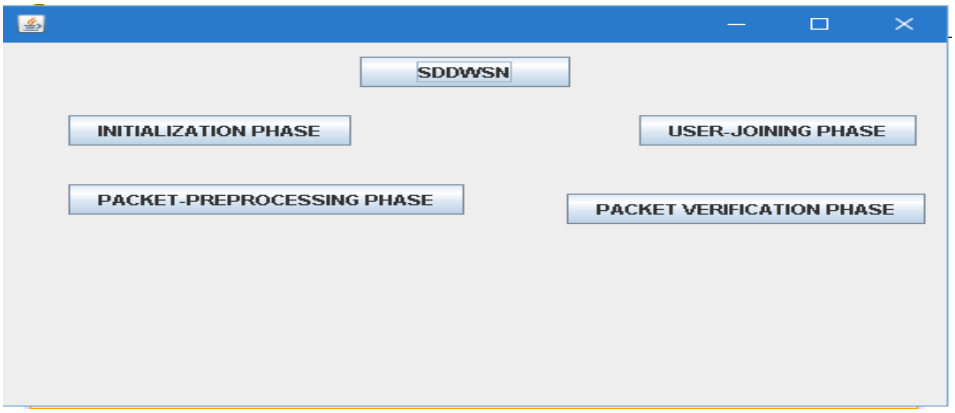

Fig.3: Figure showing four phases of SDDIWSN.

The protocol Secure data discovery and spreading in Wireless sensor networks (SDDISWSN). It has four phases. Each phase has separate functionality according to its name. This is shown in below snapshots. Four phases constitute the SDDISWSN. In order to work correctly it has been divided into four phases into protocol. The above diagram shows four functionality. Let us see one by one.

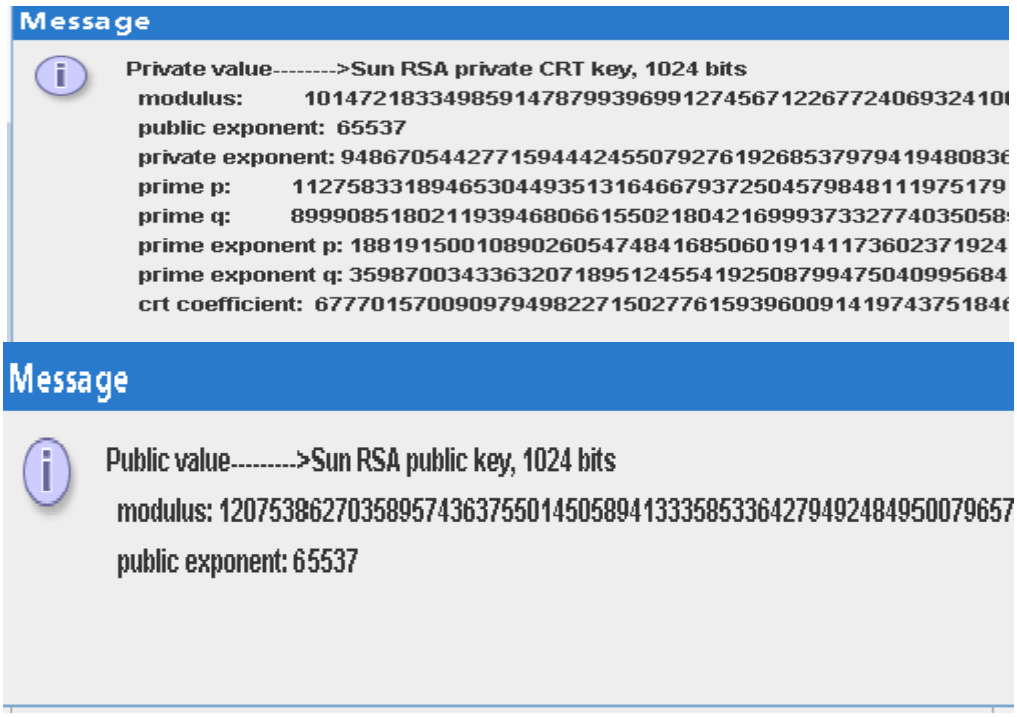

Fig 4: Frame showing Private and Public keys.

Both private key and public key shown in the figure in public there are two parts. One is modulus and another is exponent part.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

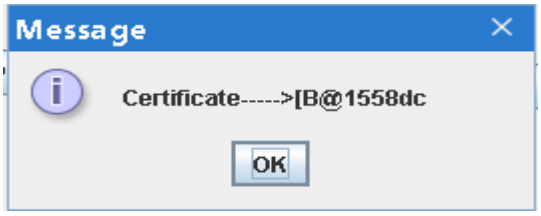

Fig5: Display User's Certificate

The certificate will be of user i.e.User joins the owner.

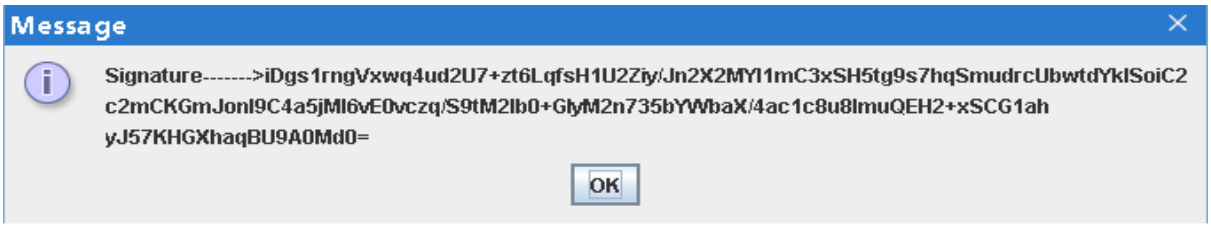

Fig 6: Generated Digital Signature.

This is digital signature for data integrity. This will be sent for every user and verification node.

Fig 7: Verification of data on receiving by Signature.

It sends the status whether if data integrity is preserved then it will return true else fail.

VI. CONCLUSION

The protocol, Secure and data Discovery of Distributed Information& Spreading in WSNs (SDDISWSN) implements public key cryptography, it concludes that, security is ensured. i.e. Authentication is proved by issuing Certificates and Data integrity is proved by RSA approach to digital signature. The computation cost is high but communication is very good.

REFERENCES

1. Daojing He, Sammy Chan, Shaohua Tang, and Mohsen Guizani " Secure Data Discovery and Dissemination based on Hash Tree for Wireless Sensor Networks" IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 12, NO. 9, SEPTEMBER 2013
2. S.Velmurugan, Dr. E. Logashanmugam on "Secure and Distributed Data in Wireless SensorNetwork", 2nd International Conference on Current Trends in Engineering and Technology, ICCTET'14
3. Daojing He, Sammy Chan, Yan Zhang,andHaomiao Yang, "Lightweight and Confidential Data Discovery andDissemination for Wireless Body Area Networks" IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS, VOL. 18, NO. 2, MARCH 2014
4. Daojing , He,Sammy Chan, Mohsen Guizani , Haomiao Yang, Boyang Zhou "Secure and Distributed Data Discovery and Dissemination in Wireless Sensor Networks", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 26, NO. 4, APRIL 2015

BIOGRAPHY

Pattanashetti Vijay Irannais a final year M.Tech student. Pursuing form University BDT college of Engineering, Davangere. His Interests are Computer networks, Aggorithms, Security.