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 6, June 2016

Implementing Authentication, Data integrity in Wireless Sensor Networks

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

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

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

ABSTRACT: In wireless network environment, there are two possibilities one is centralized and other Distributed nature delivering buggy information. The centralized has base station which sends the information. Another good is Distributed nature where the data can be sent without missing but it needs security in terms of authentication, Data integrity and less communication cost. This all done by a protocol called "SDDISWSN" can be abbreviated as Secure and Discovery of Distributed Information & Spreading in Wire Sensor Networks. It implements many owner-many user.

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

I. INTRODUCTION

Wireless sensor network are used to track applications of civilian or military. The WSNs are expected to process, store and sensed data on demand of the network. The network user supposed to get some information before start of network. The Wireless Sensor Network is key technology in Military, Hospital in various domains. The WSNs consists of sensor nodes. These sensor nodes are used for sensing & Actuating applications. The nodes have tendency to perceive light, humidity, vibration etc. The WSN's due to its capability of small size and less energy requirement, The WSN can be deployed in underground, underwater & terrestrial. The WSN operate in Stationery and Mobile networks applications like remote sensing, medical health care institutions. The limited resource of nodes i.e. memory, computation, bandwidth energy makes challengeable.

The Fig1 shows the architectural model of wireless sensor networks. This can be deployed in above environments for particular applications. In consists a network of sensor nodes forms the WSN network and Data items, base station, different users. The sensor node has memory, energy and bandwidth which make to participate actively. There are two approaches one is Centralized and Distributed. In centralized approach, the base station is responsible for sending information but it faces with a problem of single point of failure (SPOF). As base station is only one, if it fails every other modules won't work.

While other distributed, the most of drawbacks centralized will be resolved here. There will be 'n' number users. The network owner gives permission to the user and there by user will send the data. The data item will be formed by signing. It implements many owner-many user. There can be any number of network owner and similarly for users will be. The concept of sub-networking adds a feature in case the networks fails. The gap will be filled by other sub-network. Once it is reached in the destination. It will be verified. Here it is the need of security importantly Authentication, Data integrity etc. The security can be produced by a protocol. Hence the security is essential in distributed network.

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 6, June 2016

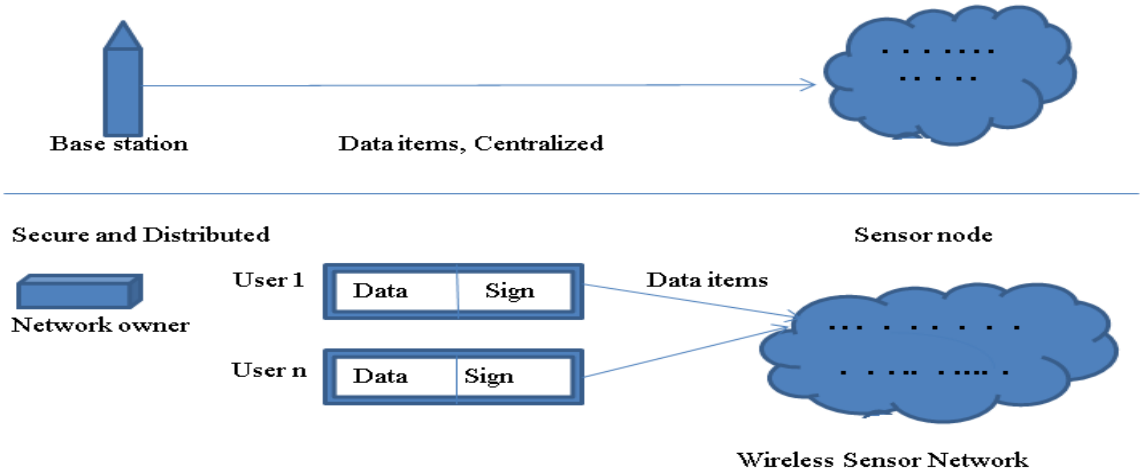

Fig 1: Line separating Distributed and centralized View.

II. RELATED WORK

In[1] author proposed protocol. The protocol finds vulnerability in discovery and dissemination of information. Such vulnerability adversary updates like critical sections and denial of service. The protocol is based on assumptions like data disseminate at the source. At base station it is not compromised & is trust worthy but base station has unlimited computational power.The sensor node performs limited number of cryptographic operations.The protocol depends on Merkle hash concept. The function is divided into three layers. For equivalent to Merkle concept, there is puzzled approach.

In[2] author developed protocol called SDD. First secure and dissemination protocol. It is built, keeping in mind the security. As it is for multi-owner multi-user. It allows network owners to authorize for data to users disseminate the data. The SDD has information flows fromnetwork user to sensor node. It has four phases. Those are system initiation phase, user joining phase, Packet pre-processing phase and Sensor verification phase. The delay is reduced.

In[3] author try to find some features to add into traditional WSNs.Those are Communication, Resource, physical compromise of body networks and Mobility. For encryption one way key hash chains is used. The whole protocol functionality is divided into three phases.

In[4] author developed the protocol which satisfies features like distributed, authentication and integrity of data items, scalability etc. He valuated the protocol and analysed the same. He built several models which are Network model, Trust model and Threat model. The protocol functionality is divided into four phases. Those are system initiation phase, user joining phase, pre-packet processing phaseand packet verification phase.

III. METHODOLOGY

A. SDDISWSN

The above sequence diagram shows there are three classes. Those are OWNER, USER and SENSOR. The interaction between these classes forms a sequence which can be divided into four phases of functions. Each class has different properties. For example, the class OWNER has Request, Reply, give permission etc. let us see one by one.

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 6, June 2016

1. System initiation phase

There will be parameters like p, q are randomly initialized. From these p, q variables the Private key and Public key will be derived. The p, q will be prime numbers. Likewise system initializes the variables Pr_k, Pu_k.

2. User joining phase

The user produces the user identification, and private key to the network owner. The owner accepts it. The user will join the phase is called as user joining phase. The owner replies with certificate. This certificate enables authentication.

3. Packet Pre-processing phase

Each packet will be signed then called as Data items. The construction of data packets forms the data items. By using hashing technique, the processing of data items takes place. Maintaining the original data is the purpose of packet pre-processing phase.

4. Packet Verification phase

The privileged sends the data to the sensor. The sensor verifies with the help of digital signatures.
If the public key is same as original then verification is success. There is no data change in the packet. Likewise data integrity is verified. The data will be updated.

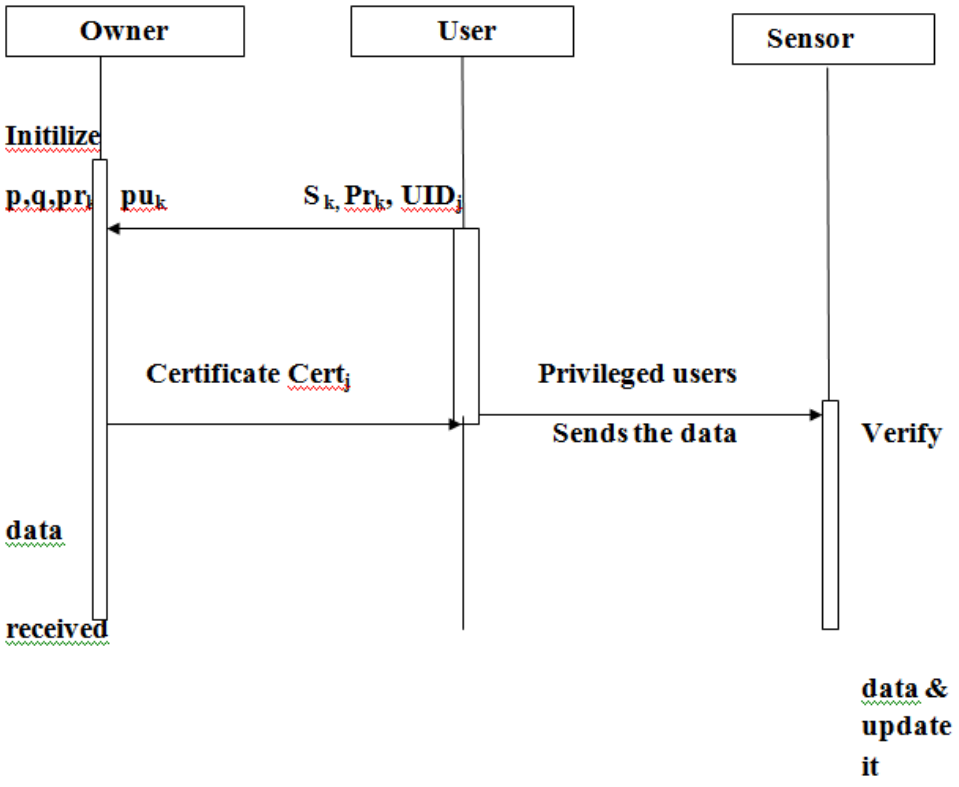

Fig 2: Different sequential flow of information in SDDISWSN

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 6, June 2016

IV. PSEUDO CODE

Step 1) Initialize p, q with prime numbers.
Step 2) Calculate Private key, public key.
Step 3) With UID,SK¸ Private Keyrequest for registrationto network owner.
Step 4) On registration, the owner sends certificate to the user.
Step 5) Using digital signature the packet pre-processing will be done.
Step 6) On reaching sensor node the packet will be verified and data will be updated.
Step 7) End

V. RESULTS AND DOCUMENTATION

The enhancement of securediscovery of distributed information spreading in wireless sensor networks(SDDISWSN) is done through 4 phases. These phases are divided according to functionality. The Fig. 3 discusses about the same. On clicking phase1 the system initiation phase will be activated i.e. initiation of prime numbers p, q will be started. Same for all phases it will be done. That equivalent function will be performed.

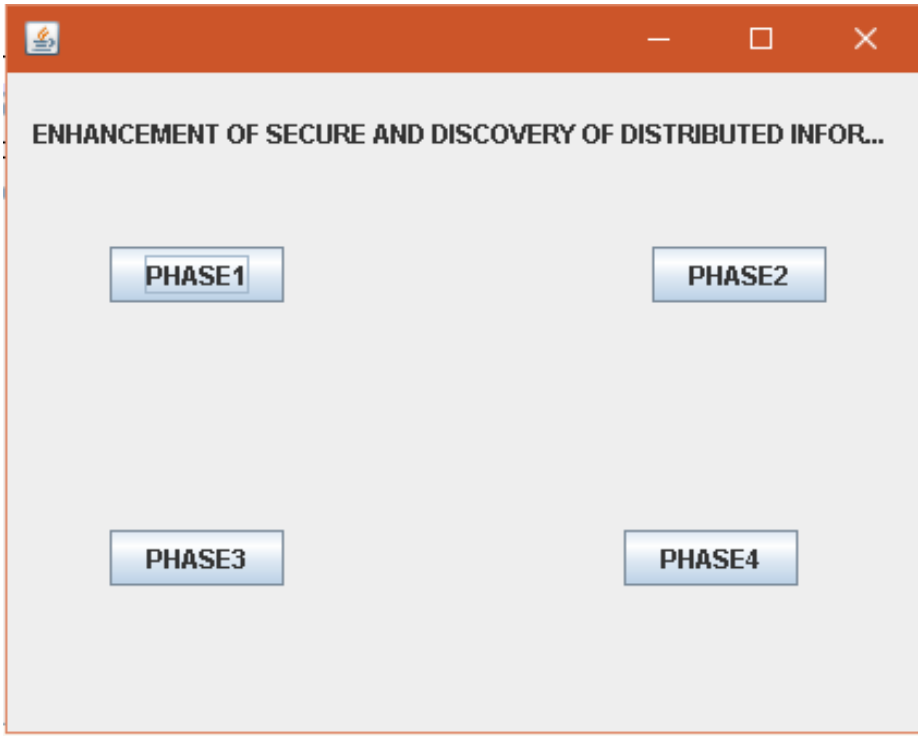

Fig 3: Different phases of SDDIWSN

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 6, June 2016

The above Fig 3 Shows four buttons each has different functionality. Phase1 is the initializing the prime numbers. Similarly other phase's different functionality. Let us see one by one. It is RSA approach which forms private key and public key is combination of numbers, special characters and letters etc.

Fig 4: Private key

It is obtained by prime numbers p, q and alphanumeric character. On initiation of variables p,q the initiation phase is over. This is unique for each data transmission.i.e. in Fig 4.

Fig 5: Public key

Similarly as that of private key, it same for is public key. The combination of Private key and Public key is unique. The two key has exponent has modulus and exponent parts and similarly has a length of 1024 bits.

Fig 6:Certificate

On producing private key, public key and user identification (UID). The respective user will get Certificate. This certificate acts as Authentication for many users. The change in certificate causes no updating of data. The certificate contains the serial number other details.If change in certificate causes not to update in data.This change can be found by packet verification phase.

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 6, June 2016

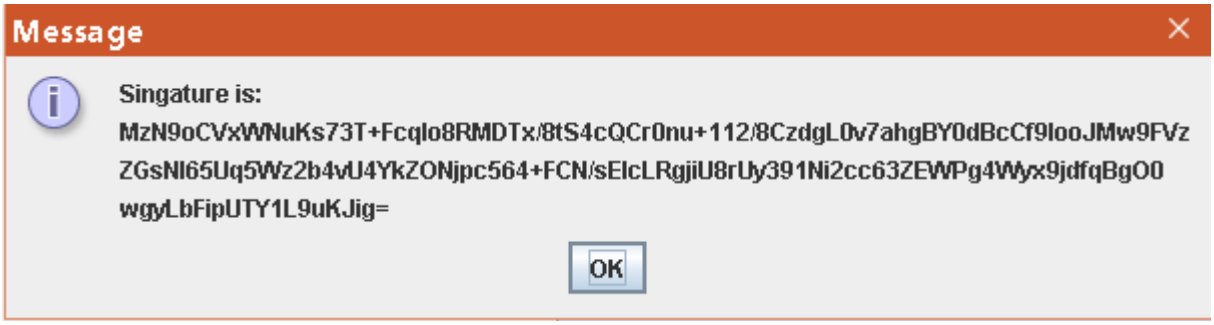

Fig 7: Digital Signature

The Fig 7 shows the signature i.e. digital signature. The signature is used for signing the data. Those will be signed data items which will move to destination in wireless senor networks. The digital signature is used to check data integrity. Whatever the data is to be sent, that should not be modified. To detect this data integrity, the digital signature holds good.

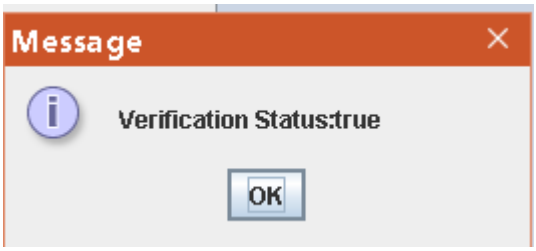

Fig 8: Verifying status

The above screen shots all are pertaining to SDDISWSN protocol. First the private key and public key is created. Then user with these values sends to owner. The owner will accept it and sends the certificate. This will be treated as authentication. Using digital signature packet verification will be done. If it is no changed then the status will be true.

The snapshots, communication with nodes is shown in figure. The sender node, receiver node, Router1, Router2 and server are some set of rules. The flow of execution is Server, Sender, Router1, Router2, Receiver, similarly the flow of execution at other send which is shown in below figure Fig: 9.

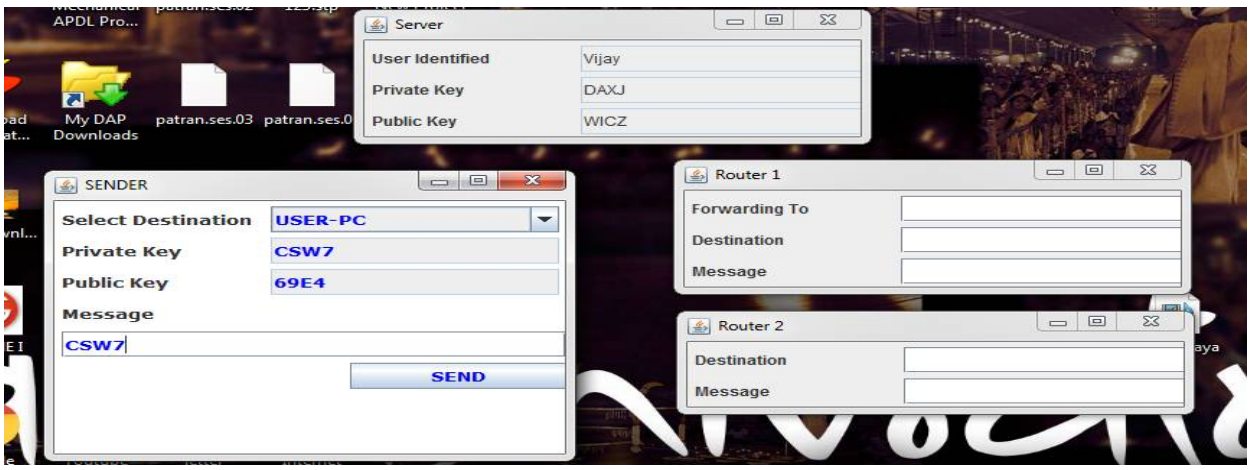

Fig 9: First step output of four modules and Flow of execution with generation of private and public key.

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 6, June 2016

At router1 Vijay and at USER-C. it needs to select the user which are listed in the router2 if router1 is source. On selecting, there is button called continue. On clicking the continue button the information will be sent.

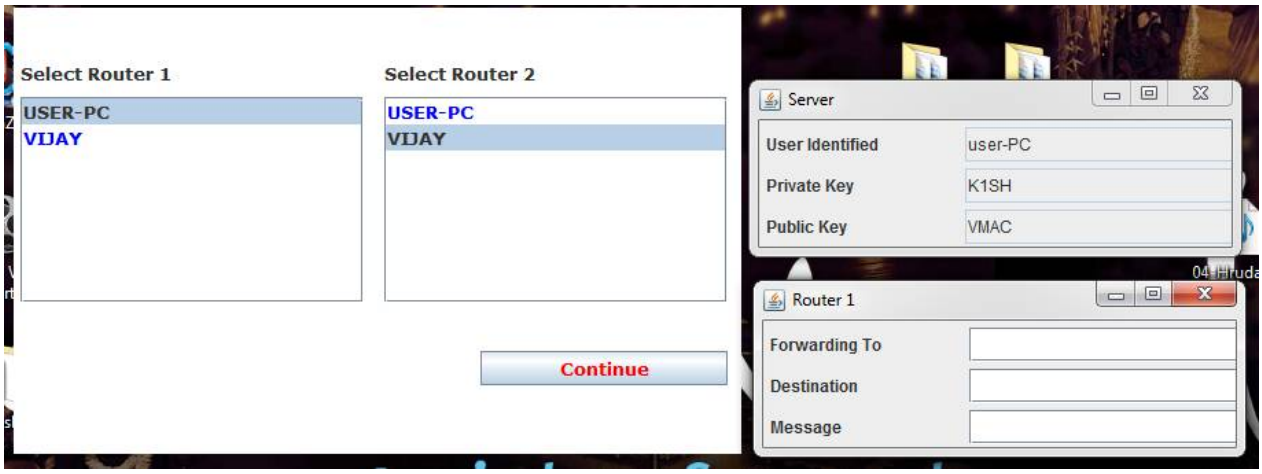

Fig 10: Selection of Router1 and Router2

The wireless network enables or considered to act as Wireless sensor network. The buggy or command information will be sent to next node. It uses public key cryptography for secure communication. The message will be encrypted with private key of sender and public key. This is shown in figure Fig 11.

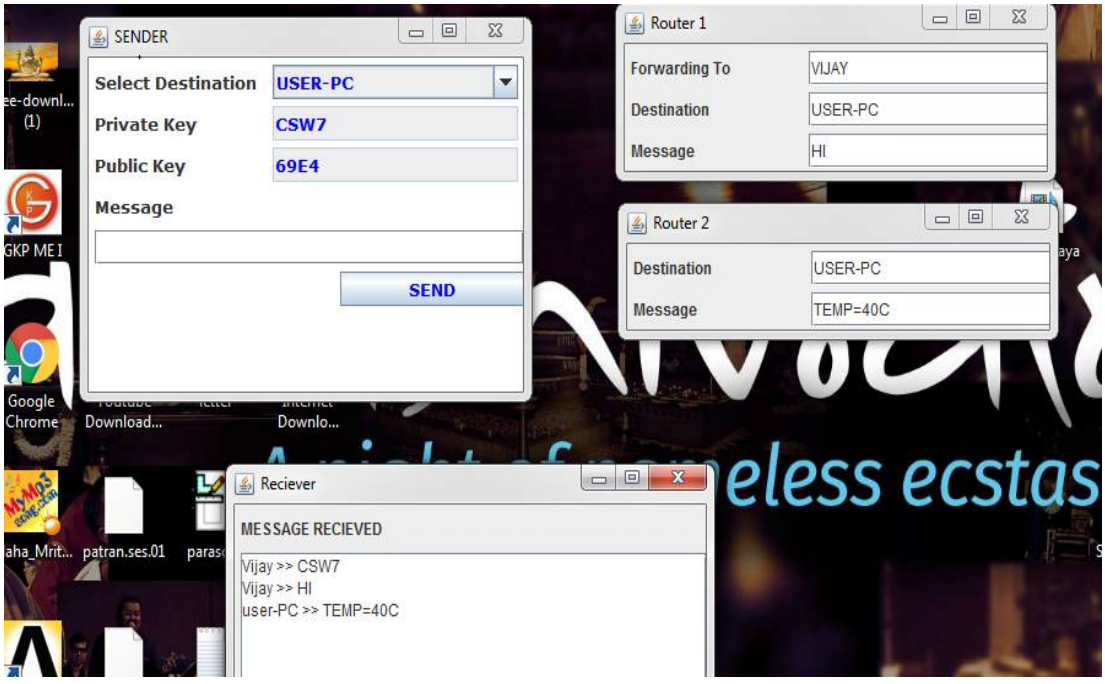

Fig 11: Final message has been sent to USER-C.

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 6, June 2016

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 M.Tech from University BDT college of Engineering, Davangere(Constituent college of VTU, Belagavi) His Interests are Computer networks, Algorithms, Security and Android.

B N Veerappa is working as associate professor in the department of CS & E at University B.D.T college of Engineering, Davangere(Constituent college of VTU, Belagavi). Area of research interest are speech recognition, Pattern recognition, Image Processing, Networking, Data mining etc.