# Designing Optimal Path for Wireless Sensor Networks by Combining Energy and Security Components.

**Girish.R.Deshpande, V.S.Rajpurohit, S.S.Sannakki, Sudhindra .K. Madi**

***Abstract*: The data transferring using multi-directional in remote sensor systems (WSNs) offers little security against malicious attacks through proper acknowledgement. An enemy can use confidential information to attack events, also deteriorate proper functioning of routing protocols. This situation is also expands to mobile and hostile network conditions. In this novel, I would like to propose trustworthy and operational location based routing instructions which provides security and also helpful to extends this works for large wireless sensor networks. The proposed idea has been clearly provide the mechanism to finds out malicious attacks as well as to provide security. As per the statistics, There are constraints on storage, processing of data, battery resources and variation in frequency ranges deeply effects for implementation, in addition to this data propagation ,improper links between network components, requires extra care while choosing different routing paths.***

***Keywords: Routing paths, Routing schemes, hostile conditions.***

## I. INTRODUCTION

Remote Sensor Systems (WSN) offer proficient, low-cost arrangements for an incredible variety of applications like military areas, healthcare, homeland security, industry control, and event control in building smart architecture. In spite of the fact that organizing and deploying security measures is difficult, due to the constrained sensor assets in terms of memory space, control and vitality accessibility, oblige the complexity of the security components, for these reasons the need for more advanced routing schemes. Due to their dispersed nature, WSNs are helpless to different assaults [2], most threats focusing on injecting false data into routing paths which is arranged in a multi-directional mode. Whereas the conventional (or the so called “hard”)

Security measures (e.g. encryption, verification) are very productive in Protecting against few sorts of assaults; there are a few particular sorts of assaults that can be way better taken care of by applying a efficient and trust-based techniques. In other words, security and trust parameters are most helpful in protecting routing information (trust-factors of neighbors) which is present in topology. It recognizes such interlopers that mislead recognizable network security disruption by knowing trust factors of other nodes and routing table information and which causes to deteriorates throughput of entire network.

Remote sensor systems (WSNs) [2] are perfect candidates for applications to report recognized events, such as battle field and fire detection in forests. A WSN comprises battery-powered senor nodes with greatly restricted execution capabilities. With a limited radio communication band, a sensor hub wirelessly sends messages to a base station through a multi-mode way. But the multi-mode technique of WSNs regularly gets to be the target of sever assaults. A malicious user may alter hubs physically, create collision with apparently substantial transmission, drop or mislead messages in a period, or create collision in communication channel by disrupting radio bandwidth [3]. This paper mainly addresses the kind of threats in which enemies mislead the entire network by hacking nodes identity through replying routing information. Based on fake identity, the enemy is able to create very sever and very tricky to identify attacks towards data transmission, such as selective route information, wormhole threats, sink hole threats, and Sybil threats.

## II. LITERATURE REVIEW

Theodore Zahariadis et.al., proposed that Ad-hoc and wireless networks identified problems on the security issues of security components which is more requires because they are deployed in very sensitive applications like monitoring environmental conditions. To protect against data security and to maintain confidentiality, the design of a trust based framework is recommended. Jaydip Sen addressed that public keying mechanisms are still very difficult to implement in sensor networks. It is more complicated and minimizes the execution speed of the network. Using private key mechanisms are more compatible for maintaining stable operations in sensor architectures.

***2.1 Secure routing rules for wsn***: Due to mobility of sensor hubs includes an incredible impact on building stable network model and thus on the routing methods. Mobility can be at the base station, sensor nodes, or both. Current protocols assume the sensor network is stationary. A current security mechanism assumes that sensor network is dynamic in nature.

**Revised Manuscript Received on December 12, 2019.**

***** Correspondence Author

**Girish.R.Deshpande***, Computer science, or University/Industry, City, Country. Email: grdeshpande@git.edu

**V.S.Rajpurohit,** Computer science, or University/Industry, City, Country. Email: grdeshpande@git.edu

**S.S.Sannakki,** Computer science, or University/Industry, City, Country. Email: grdeshpande@git.edu

**Sudhindra .K. Madi,** Computer science, or University/Industry, City, Country. Email: grdeshpande@git.edu

So there is need for developing most efficient security frameworks, Theodore Zahariadis suggest that there is strong need of designing security tools. After finding security problems, Trust-based frame work is built and also deployed in various applications it proves its non-functional and functional requirements are successfully meet its needs. After conducting different test in different scenarios it proves that trust metrics are successfully implemented. In real time applications it is very feasible to deploy a trust frame work. The overall security depends on protocols the way how they handled and fulfill security requirements.

### 3. Nth-degree truncated polynomial ring unit algorithm

Basically NTRU is public key crypto mechanism. It is very difficult to break. All procedural steps are based on the object based system which is present in polynomial ring with multiplication. All polynomial have the coefficients in the range of 1 to N-1.

#### *3.1 Steps involved in NTRU Key Generation*

1. Select the value of p and q.
2. Compute the inverse polynomial of the secret key modulo p, Fp.
3. Compute the inverse polynomial of the secret key modulo q, F.
4. Finally we got the public key,

$$h = p * ((F * q) * g \,\%\, q$$

#### *3.2 NTRU Encryption:*

*1.* Assume 'A' is a sender and 'B' is receiver. 'A 'puts the message in 'B's incoming buffer.

2. Message in m is in the form of polynomial its coefficients values lies in between $-\frac{q}{2}\ to\ \frac{q}{2}$
3. Next source node A randomly chooses the value of r.
4. By using parameters m, r and B's public key we are computing

$$e = r * h + m \,\%\, q$$

#### *3.3 NTRU Decryption:*

1. Perform polynomial multiplication of

$$a = f * e \,\%\, q$$

2. Rearrange the value of a into the range $-\frac{q}{2}\ to\ \frac{q}{2}$

3. Finally we compute $d = a * F * p \,\%\, p$

## III. SYSTEM DESIGN

The entire security design is characterized by several parameters like building architecture, placing entities in the system also defining constraints.

### *4.1 UML Diagrams*

UML is the best way of representing the roles, and behavior of the phenomenon. It was proposed by Object management group.

### *4.2 Use Case Diagrams*

The best way of understanding functionalities and entities that are responsible for conducting those functions is modeled by use case diagrams. These diagrams can clearly shows different types of actors of a system and the various interactions by user to it.

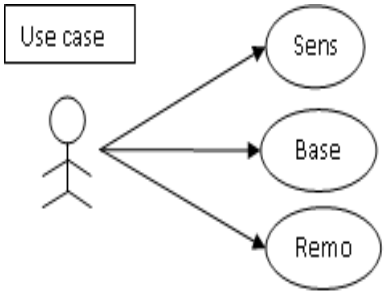



**Fig4.1. Use-case diagram.**

### *4.3Data Flow Diagram*

Data flow representation is the way of showing information transfer in between various components in framework, designing its process aspects. DFDs can moreover be utilized for the visualization of information handling (organized plan).

It could be a basic graphical representation that can be utilized to visualize framework in terms of the input information to the framework.

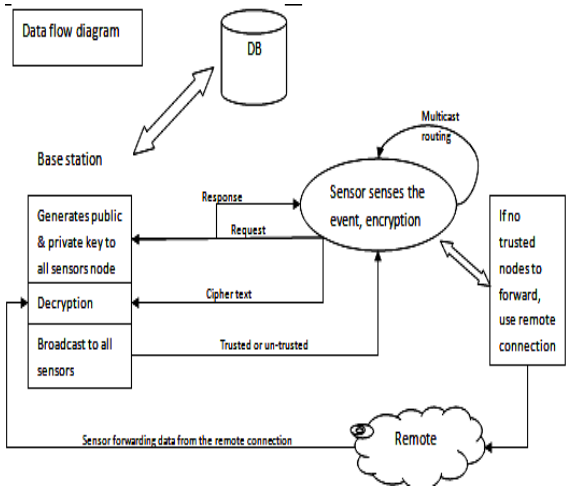



**Fig. 4.2. Dataflow diagram**

## IV. IMPLEMENTATION

### *5.1Network Model*

In this framework, a mote organizes composed of a security manager which could be a trusted entity, an expansive number of sensor hubs, and numerous clients are considered. In this work security controller is used with 'S' notation. Clients are represented by 'U' Sensor hubs are denoted by 'N'. All clients and motes are assigned by unique identity numbers. Client id & mote-id is defined as 'Ui' and 'Ni' respectively. Trust party 'S' can switch its state to online and off-line. It comes online only on demand. e.g In case of malicious attacks, each network has high-capacity sensor node as i-mote2 which is different from other nodes and its execution speed and memory is high. Information can be stored in its own memory area or at some other remote locations in

network using data storage schemes.

### *5.2 Adversary Model*

In this model we are taking account of hackers their main goal is to steal data but actually they don't have access permissions. The attacker may be exist internally or remote place. Due to less protection, sensor motes are much subjected to sever attacks. We have to identify enemies with all aspects, which can

- Passively observing all the communication channels.
- Compromise and tries to control clusters.
- Attacker can create wrong encrypted messages.

### *5.3 System architecture and implementation steps*

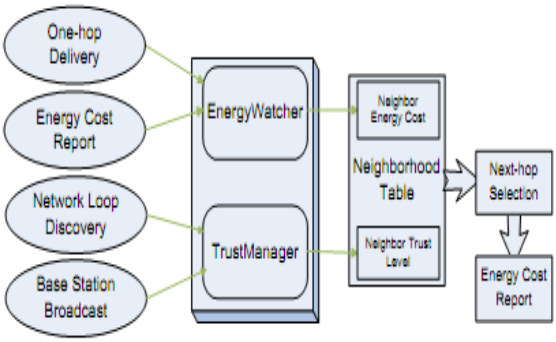



**Fig5.1 Energy Watcher and Trust Manager**.

In the above architecture, it shows n number of sensor nodes. Each sensor node has

- Unique id is randomly generated and unique in entire network.
- Every node has Energy tracking system, for every event its value will be updated. And also it contains battery level of other sensor nodes.
- Every node has security-manager, it has trust values of other motes, and it's updated for every operation. Every time it updates and ensures its security level to the all nodes.

### *5.4 Routing Procedure:*

The routing procedures deployed in this security frame-work functioning on demand basis. They switch on or off depend on requirements. The following steps are required to select optimal paths:

- FIRST WE NEED TO COMPUTE LIFE-SPAN OF EVERY EVENT, IT DEPENDS ON NUMBER OF CONTROL INFORMATION IS COMMUNICATED AMONG SOURCE AND DESTINATION.
- Base station is responsible for replying acknowledgements to the intended node. Acknowledgement field contains number of bits are received and pending.
- After completion of every event sink node broadcast battery consumption report and trust level to all nodes. The Start-End interval is defined for every node and it calculates energy consumption and trust factor within that interval.
- While sensor node choosing transmission path it considers according to the updated values in its table.

### *5.5 Implementation of Energy module*

The following steps will be taken by Energy module

- We assume Node 'X' want to transmit data, it has two possible next immediate nodes are named as 'Y' & 'Z'.
- Then it computes the energy values of 'EnY' & 'EnZ ' from the values which are stored in its table. if the value of EnY>EnZ then it selects EnY.
- Once bits are handover to the node 'Y' it is responsible for selecting the remaining path. Same calculation is repeated up-to it reaches maximum threshold level.
- After completion of transmission process, energy manager computes total amount of battery consumed to transmit data from source 'X' to the sink node. Sink node confirms data delivery by acknowledging to 'X'.

### *5.6 Implementation of Security module*

- A node 'X' s Security manager is responsible for deciding security level of its immediate neighbor nodes 'Y '&'Z'.
- The security level of all the nodes depend on two factors: Identifying deadlock occurred & acknowledgement message from sink.
- For Every node the value of 'S' is assigned by security manager. The value of 'S' will be stored in its own table. Initially the value of 'S' is 0.5, after every event the value of 'S' will be updated.

### *5.7 Combining Energy component and Security manager in Frame work:*

The main advantage of our proposed framework incorporates both energy component and security manager. The following steps are taken by both components:

- ANY NODE 'X' EVALUATES ENERGY COST AND SECURITY LEVEL OF ITS OTHER NODES WHILE CHOOSING EFFICIENT PATH.
- Every node after completion of event, they will receive energy-cost report from other nodes. Some time adversaries will try to inject wrong values in that report. The main target of enemies spoofing information rather than avoiding efficient path.
- Whenever the nodes are failed to get valid energy values, Security manager will support because it work independently. Security manager in one node will not reveal its information to others.
- Security manager in one node observes multiple failure messages from base station to other node, immediately it

decreases the security level of that

node and it selects most and secured prominent node which is present in the network.

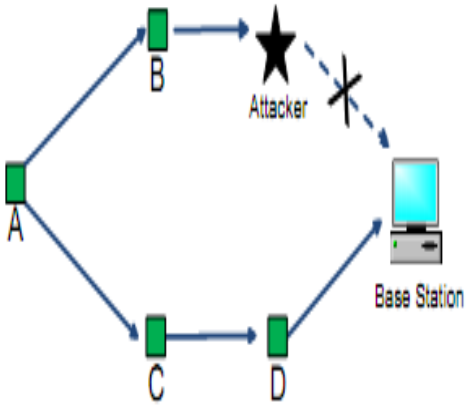
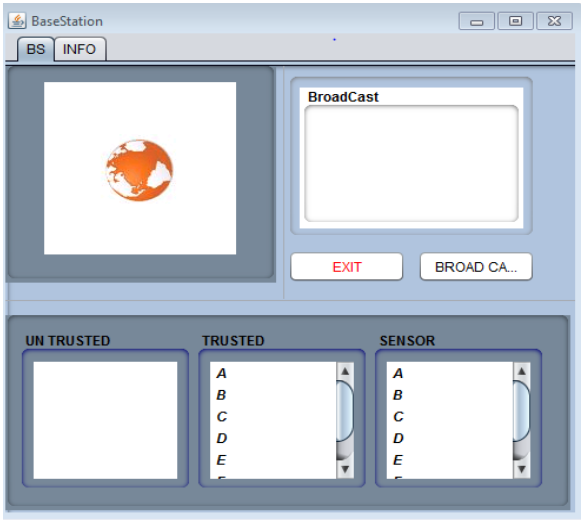


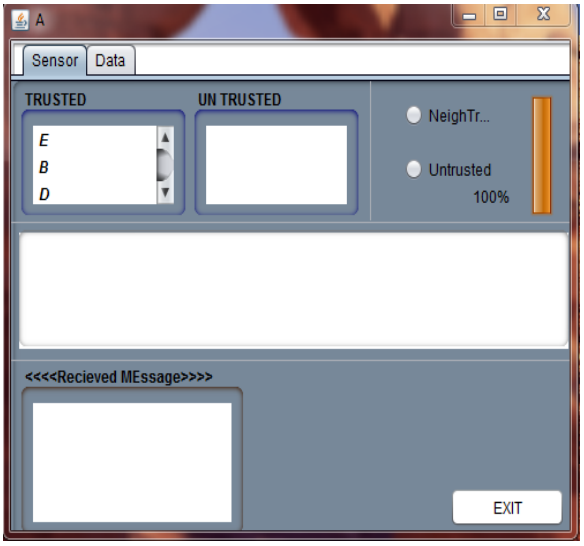

**Fig.5.2 working of security manager**

## V. RESULTS AND ANALYSIS

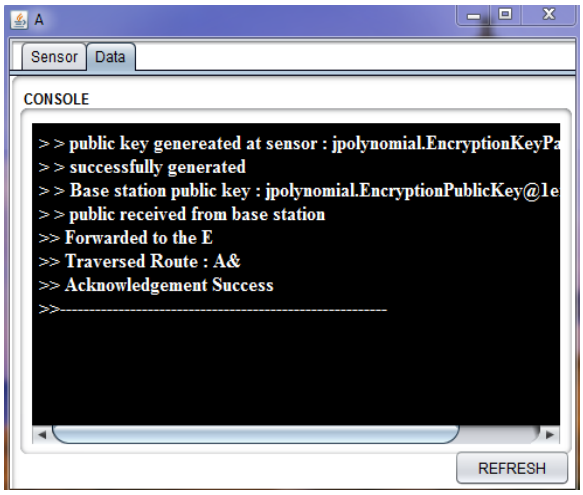
### *6.1 Sink node*



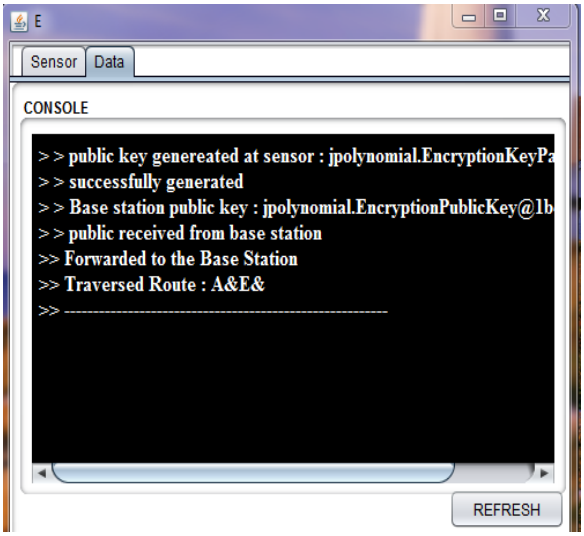

### *6.2 Event Generator node*



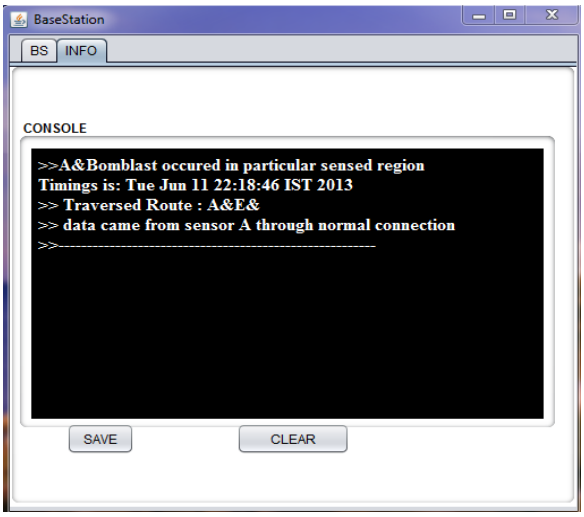

### *6.3. Routing information stored in Source node*



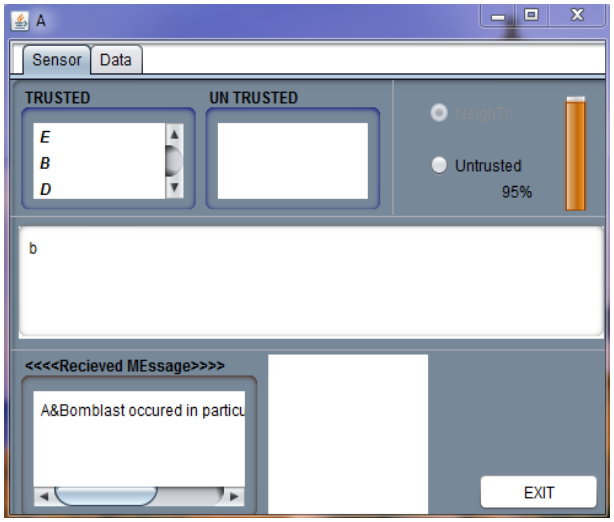

### *6.4 Information stored in intermediate node*



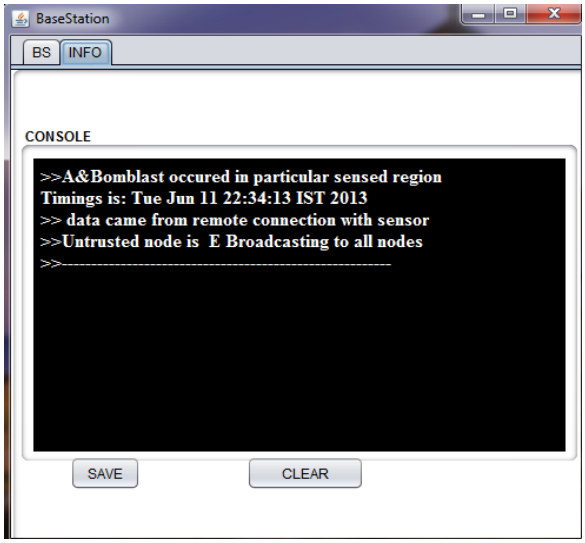

### *6.5. Information stored in Sink*



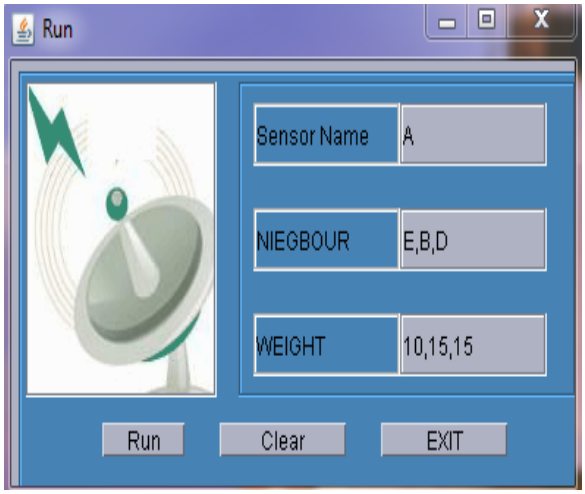

### *6.6. Battery-consumption Report from node A*




*6.7 Broadcasting Trust factors E to all nodes*



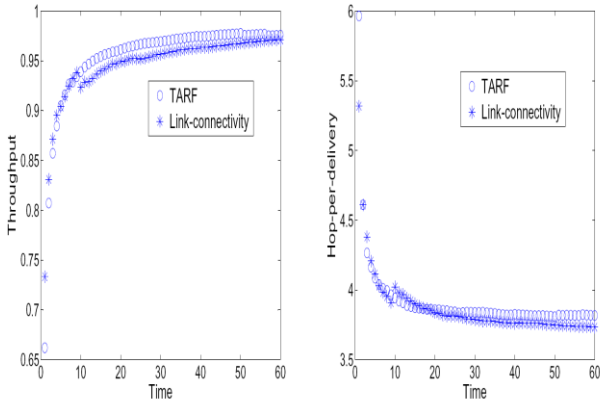

*6.8 Registration process*




## VI. ANALYSIS OF FRAMEWORK UNDER DIFFERENT SCENARIOS

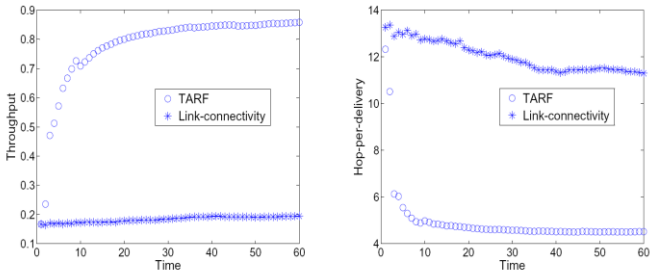
The feasibility of proposed frame work is evaluated and tested under different scenarios.

### *7.1 Performance evaluation under misbehavior nature of nodes*



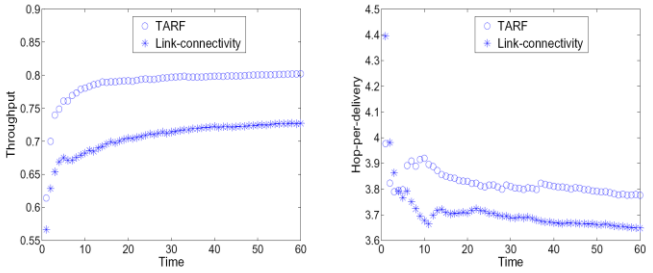

(a) (b)

### *7.2 Forging node identity and acts like fake server*




(a) (b)

### *7.3 Packet drop and Recovery*




(a) (b)

- Under scenario 1, we are comparing two routing schemes and their impacts under different situations. Due to assigned security levels for every node, it can easily differentiate in between valid node and invalid.

- Under scnario2, some nodes act like fake server by forging other nodes. They forge the identity of other nodes involve in stealing messages. But there is strong security associations are in between valid nodes and server. Server can easily differentiate them by using unique id as well as recent security level's of respective nodes.

- Under scenario3, sometimes there is chance of data loss due to interference and collision occurs in channels. By using secure frame work we can avoid data loss without effecting data rate.

## VII. CONCLUSION

Our proposed framework aims to prevent wireless network from sever attack's. The main aim of our proposed work concentrates on energy and security of entire network. But the existing protocols cannot focuses on both parameters. The entire framework is implemented and tested under various scenarios. Our main contributions in this work are listed as follows:

1. Unlike existing protocols better in providing secure environment for wsn's, our framework secures wireless network from several major threats by building proper acknowledgements.

2. We are adding both energy and security components in a single framework. They are incorporated and ensure reliability and robustness.

## REFERENCES


1. G. Zhan, W. Shi, and J. Deng, "Tarf: A trust-aware routing framework for wireless sensor networks," in Proceeding of the 7th European Conference on Wireless Sensor Networks (EWSN'10), 2010.
2. A. Wood and J. Stankovic, "Denial of service in sensor networks," Computer, vol. 35, no. 10, Oct 2002. PP. 54–62.
3. A. Perrig, R. Szewczyk, W. Wen, D. Culler, and J. Tygar, "SPINS: Security protocols for sensor networks," Wireless Networks Journal (WINET), vol. 8, no. 5, Sep. 2002, pp. 521–534.
4. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Communications Magazine, vol. 40, no. 8, Aug. 2002, pp. 102–114.
5. C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, 2003.


## AUTHORS PROFILE

**Girish.R.Deshpande is** working as Assistant professor in the department of computer science and Engg at Gogte institute of technology, Belgaum. He pursued his B.E in Information science and engg & M.tech in Digital Communication and Networking from V.T.U, Belgavi. His research interest areas include Image Cloud computing, and Network Security.

**Dr.Vijay.S.Rajpurohit** is working as professor in the department of computer science and Engg at Gogte institute of technology, Belgaum, He pursued his B.E in computer science and engg from Karnataka university Dharwad, Mtech from N.I.T.K Surtahkal, and phd from M.I.T, Manipal in 2009. His research interest areas include Image processing, Cloud computing, and Data analytics. He has published a good number of papers in journals, International, and conferences. He is the associate editor for two international journals and a Senior Member of International association of CS and IT. He is also the life time member of SSI ,ISC, and ISTE associations.

**Dr. Sanjeev S Sannakki,** has completed his Ph.D.degree in Image processing & Data Mining from VTU Belagavi.. His career spans over a period of two decades is in the field of teaching, research and other diversified in-depth experience in academics. He is currently working as a Professor in the Department of CSE, Gogte Institute of Technology, and Belgaum. He has published several papers in reputed national/international conferences and journals. He is also guiding the research scholars & UG/PG students of VTU.

**Prof. Sudhindra K. Madi,** has completed His B.E & M.Tech from VTU, Belgavi. His career spans over a period of two decades is in the field of teaching, research and other diversified in-depth experience in academics. He is currently working as a Professor in the Department of ISE, Gogte Institute of Technology, and Belgaum. He has published several papers in reputed national/international conferences and journals. He is also guiding the research & UG/PG students of VTU.