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. 2, Issue 2, February 2014

Data Security in Wireless Sensor Network

P.Uthaya Bhanu[1], J. Saravanan[2]

M.Tech., Student, Department of Electronics and Communication Engineering, PRIST University, Puducherry-605007,India[1]

Assistant Professor, Department of Electronics and Communication Engineering, PRIST University, Puducherry-605007, India[2]

ABSTRACT: In this model the base station has complete monitoring the node. Using color change the behavior of the node is done. If the base station suspect that there is change in behavior of node then encryption is changed .So that once the node is compromised within a time of second using encryption change the key is changed .So the hacker is unable to hack the information even though the node is compromised. Thorough analysis and extensive simulations support our findings. With this Security and Confidentiality solutions are mandatory aspects when developing new pervasive technologies such as wireless sensor networks (WSN). Likewise the each node is monitor by cluster head which the key information is already stored in each cluster. Because of the distribute architecture and cluster type topology, it consume low energy and better security.

KEYWORDS*:* Wireless sensor network, Trust management, Security model, Key management, Encryption model.

I. INTRODUCTION

Many current and envisaged applications for wireless sensor networks (WSNs) involve data collection in remote, inaccessible or hostile environments, such as deserts, mountains, ocean floors, and battlefields. A multitude of sensors might be deployed within a certain area and their activity is usually monitored and managed by a powerful trusted entity, commonly referred to as the sink. Security in WSNs presents several well-known challenges stemming from all kinds of resource constraints of individual sensors. However, the main limitation that complicates sensor security techniques is lack of ubiquitous (inexpensive) tamper-resistant hardware. Lack of secure storage forces sensors to store cryptographic material, such as keys and seeds, in regular memory. Some recent work showed that commodity sensors can be easily compromised, even without physical access. With compromise, the adversary can read the sensor program memory and storage. As a result, no matter which security techniques are in use, sensor compromise reveals all of its secrets to an adversary. From that moment on, any cryptographic protocol ceases to be effective. For example, if the sensor routinely encrypts measurements using a secret key shared with the sink via a symmetric encryption algorithm (e.g., AES), the adversary that subverts the sensor learns the secret key and can decrypt any cipher text produced by its victim. If the key is used for integrity purposes (e.g., via HMAC) the adversary may fabricate arbitrary measurements.

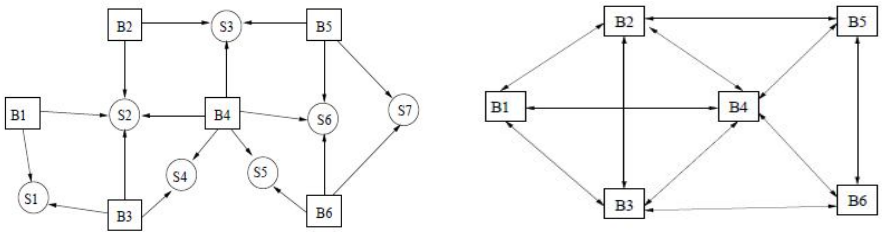
We generalize the model of alert-based approaches and propose an application-independent framework for identifying compromised nodes. The central component of the framework is an abstraction of the monitoring relationship between sensor nodes. Such relationship can be derived from application specific detection mechanisms. The framework further models sensor nodes' sensing and monitoring capabilities, and their impacts on detection accuracy. This framework is built on detection mechanisms provided by applications. It does not require sensor nodes to support additional functionalities. Therefore, no additional communication and computation costs are introduced to the 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. 2, Issue 2, February 2014



(a) (b)

Fig 1: An example for the deployment of nodes in sensor network localization and its corresponding observation graph

Based on the framework, we design alert reasoning algorithms to accurately identify compromised sensor nodes. The algorithm does not rely on any assumptions on how compromised nodes behave and collude. We show that the algorithm is optimal, in the sense that given any set of alerts, our algorithm identifies the largest number of compromised nodes that can generate these alerts, without introducing any false positives. We also study how to tradeoff certain false positives to further eliminate compromised nodes.

We conduct comprehensive experiments to evaluate the proposed algorithm. The results show that it yields high detection rates with bounded false positive rates, and thus is effective in identifying compromised nodes in sensor networks. The rest of the paper is organized as follows. Presents a general framework for identifying compromised nodes, and shows how sensor network application can be modeled by the framework. In section, we propose an optimal algorithm to identify compromised sensor nodes.

II. RELATED WORK

Much work has been done to provide security primitives for wireless sensor networks, including practical key management, broadcast authentication, and data authentication as well as secure in-network processing. The work of this paper is complementary to the above techniques, and can be combined to achieve high information assurance for sensor network applications. Several approaches have been proposed to detect and tolerate false information from compromised sensor nodes through e.g., sampling and redundancy. But they do not provide mechanisms to accurately identify compromised sensor nodes, which is the focus of this paper.

Reputation-based trust management has been studied in different application contexts, including P2P systems, Wireless ad hoc networks, social networks and the Semantic Web .Many trust inference schemes have been proposed .They different greatly in inference methodologies, complexity and accuracy. As discussed early, the Interaction model and assumptions in the above applications are different from sensor networks. Directly applying existing trust inference schemes may not yield satisfactory results in sensor networks.

Ganeriwal et al. , propose to detect abnormal routers in sensor networks through reputation mechanism. Their Decentralized trust inference approach shows the usefulness of reputation in sensor networks. But their approach treats a sensor network the same as a typical P2P system, and thus does not capture the unique properties of sensor networks. Further, their work focuses on avoiding services from potentially compromised sensors instead of identifying and excluding them from sensor networks. Further their work is application specific, and cannot be easily applied to other sensor network applications.

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. 2, Issue 2, February 2014

A. Security Mechanism in unattended wireless sensor network

A constrained optimization algorithm to further improve the above two data distribution schemes .The introduces trust management in UWSNs. A set of efficient and robust trust management schemes for the case of UWSNs. The Advanced Scheme utilizes distributed trust data storage to provide trust data reliability and takes the advantages of both Geographic Hash Table (GHT) and Greedy Perimeter Stateless Routing (GPSR) to find storage nodes and to route trust data to them. As a result a node capture resistance and key refreshing scheme for UWSNs based on the Chinese remainder theorem. The scheme is able to provide forward secrecy, backward secrecy and collusion resistance for diminishing the effects of capture attacks.

B. New Adversary and new threats in sensor network

Some Wireless Sensor Networks (WSNs) preclude constant presence of a centralized data collection point, i.e., a sink. In such a disconnected or unattended setting, nodes must accumulate sensed data until it can be or-loaded to an itinerant sink. Furthermore, if the operating environment is hostile, there is a very real danger of node and data compromise. The unattended nature of the network makes it an attractive target for attacks that aim to learn, erase or modify potentially valuable data collected and held by sensors that adversarial models and defense techniques in prior WSN security literature are unsuitable for the unattended WSN (UWSN) setting.

The result is a new adversarial model by taking into account special features of the UWSN environment. We show that, in the presence of a powerful mobile adversary, securing data stored on unattended sensors presents some interesting challenges and opens up an exciting new line of research

III. SYSTEM ARCHITECTURE AND ASSUMPTION

C. Network Environment

The envisioned UWSN includes N = $\{s_1,s_2,\ldots\ldots,s_n\}$ sensors. Deployment area Consider a network deployed over a sphere of radius S with surface area S. A spherical surface provides uniform coverage of the deployment area with random mobility models. However, the shape of the deployment area is not the focus of our work. Our techniques can be applied to UWSN deployed on any fixed-area surface Uniform coverage only helps our analysis.

D. Time

Time is divided in rounds and all sensors' clocks are loosely synchronized, e.g., via. Round length can be arbitrary; we assume that it reflects a single acquisition of data from the environment, i.e., sensors obtain measurements once per round, that is, at round r sensor S_J obtains data D_J.

E. Initialization

Before deployment, each Sj is initialized with:

1) The sink public key PK.

2) A common cryptographic hash function H(.) used as a pseudo-random number generator (PRNG).

3) A unique secret seed to bootstrap its PRNG. The PRNG is invoked for all random choices made by the sensor and its status is updated at each invocation status at round r for sensor S_J is denoted with $K^{\wedge rj}$.

F. Sink visit and re-initialization

The sink is an itinerant trusted party that visits the network with a certain frequency. Upon each visit, the sink obtains collected measurements from every sensor, erases sensor memory, provides a fresh initial secret seed for the PRNG, and resets the round counter to 1.

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. 2, Issue 2, February 2014

G. Security

Sensor secrets are fundamental to the provisioning of several security services, such as data confidentiality and authentication. The protocol introduced in this paper allows sensors to regain secret status after compromise and is not concerned with usage of sensor secrets. However, to ease exposition we will focus on a concrete example. That is, we assume that secrets are used to generate padding values to achieve public-key randomized encryption.

Sensor behavior model Sensors are not perfect. Even if a node is uncompromised, it may still occasionally report information or behave abnormally. A sensor behavior model includes a parameter r_m(called the *reliability* of sensors) which represents the percentage of normal activities conducted by an uncompromised node. For example, in sensor network localization, if r_m= 0:99, then99% of the time, an uncompromised beacon node provides correct location references.

Observer model similarly, an observer model represent she effectiveness of the detection mechanism of a sensor network, which is captured by its *observability rate* r_b, *positive accuracy* r_p and *negative accuracy* r_n. $r_b$is the probability that an observer $s1$ observes an activity when it is conducted by an observe $s2$. This reflects the fact that in some applications, due to cost and energy concerns, $s1$may not observe every activity of $s2$. The positive accuracy *rp* is the probability that $s1$ raises an alert when $s2$ conducts an abnormal activity observed by $s1$. Similarly, r_n is the probability that $s1$ does not raise an alert when $s2$ conducts a normal activity observed by $s1$. r_p and r_n reflect the intrinsic capability of a detection mechanism. The sensor behavior model and the observer model can usually be obtained from the specification of sensors and application detection mechanisms.

IV. PROPOSED METHOLOGY

A collaborative distributed protocol that leverages sensor cooperation and locomotion to achieve probabilistic key insulation. Sensors take advantage of mobility attains better security. Many current and envisaged applications for wireless sensor networks (WSNs) involve data collection in remote, inaccessible or hostile environments, such as deserts, mountains, ocean floors, and battle fields. A multitude of sensors might be deployed within a certain area and their activity is usually monitored and managed by a powerful trusted entity.

Using both analytical and simulation results, we show that the proposed protocol provides probabilistic key insulation without any trusted third parties or secure hardware and with minimal overhead. A constant storage self-healing protocol for WSNs. Sensor key update uses a polynomial-based secret sharing scheme, performed with the help of the sink. The sink periodically broadcasts information to allow non revoked sensors to update their current session key.

Based on the time of corruption, the security state of a given sensor can be partitioned in three epochs:

1. Time before corruption;
2. Time during corruption; and
3. Time following corruption.

Nothing can be done about security in epoch 2 as the adversary controls the sensor, while enforcing security in epochs 1 and 3 requires forward and backward secrecy, respectively.

Informally, a cryptographic protocol is ***forward secured*** if exposure of secret material at a given time does not lead to compromise of secrets for any time preceding compromise. Whereas, a cryptographic protocol is ***backward secure*** if compromise of secret material at a given time does not lead to compromise of any secret to be used in future.

Starting from round 1, ADV compromises k sensors per round

- Red sensors (Rr): currently controlled by ADV.
- Yellow sensors (Yr): have been compromised in some previous round and their current keys are known to ADV.
- Green sensors (Gr): Either they have never been compromised, or they have recovered through POSH.

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. 2, Issue 2, February 2014

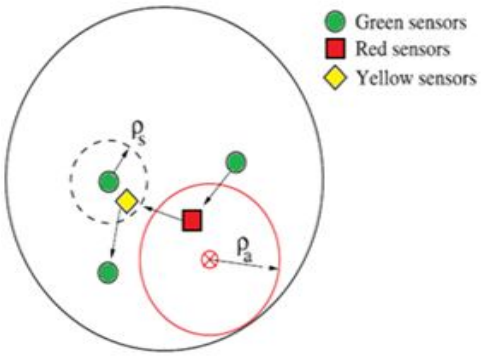


Fig 2a: Reference scenario

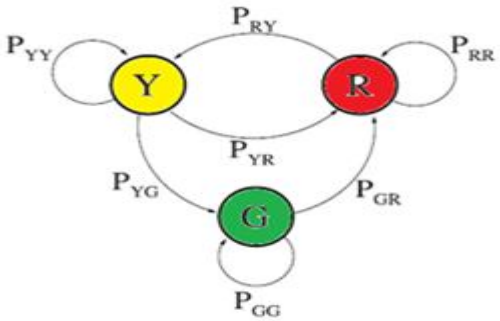


Fig 2b: Transition Diagram

When compared with other schemes, we have the following observations. First, Eigen Trust seems to be inferior to general+mm and Peer Trust. The reason is that Eigen-Trust relies on the existence of pre-trusted peers to identify malicious collectives, which correspond to colluding compromised nodes in our setting. Without pre-trusted peers, it cannot significantly distinguish malicious entities from good ones. That is why we see an upper bound of the detection rate of Eigen Trust even when compromised nodes do not form a strong local majority.

Second, we notice that when the concentration is over20, Peer Trust and voting mechanism actually yield comparable detection rate to that of general+mm with a little bit lower false positive rates. A closer examination of the network reveals that, with 200 nodes in the network, the average number of observers for each node is around 3.

When the concentration is 20, among the neighbors of a compromised node, on the average no more than 1 neighbor is compromised. In other words, when the concentration is over 20, compromised nodes seldom form local majorities .In this case Peer Trust and simple voting, both relying on majority voting mechanisms, are more likely to assign low trust values to compromised nodes or label them as compromised nodes directly. For general+mm, each identified compromised nodes in the second phase will result in the sacrifice of an uncompromised nodes, resulting in higher false positive rates.

Third, when the compromised nodes form strong local majorities (i.e., the concentration is smaller than 20), general+mm yields much higher detection rates and lower false positive rates than Peer Trust. And the simple voting has the poorest detection rate as low as 10%, as it does not do any reasoning on the credibility of the feedback. This is an important advantage of our approach. In sensor networks, it is always cost-effective for attackers to compromised a small portion of the network, and make them collude. Otherwise either they have to compromise a large portion of the 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. 2, Issue 2, February 2014

which is very costly and often not feasible, or they do not collude, in which case any voting-based algorithm can identify most of the compromised nodes, as shown above. So it is important that an identification algorithm performs well even when local majorities are formed by compromised nodes. From the experiment we see when collusion is the strongest, although the false positive rate of our algorithm is close to 50%, it is still the lowest among all solutions, and also achieves the highest detection rate.

A. Advantage of proposed system

- The proposed system is to make a collaborative distributed protocol that leverages sensor cooperation and locomotion to achieve probabilistic key insulation.
- Sensors take advantage of mobility and collaboration with peers to regain secrecy after having been compromised by inadvertently wandering into the area under adversarial control.
- Using both analytical and simulation results, we show that the proposed protocol provides probabilistic key insulation without any trusted third parties or secure hardware and with minimal overhead.

B. Security assumption in proposed model

Each sensor node is assigned a unique id before deployment and it can authenticate the messages sent or received with appropriate shared keys established through a key management protocol. More specifically, to secure the exchanged messages, the message sent between sensors should be protected by the pair wise key shared between them; and the local broadcast packets can be protected by a cluster key as in the LEAP scheme.

C. Attacker model

An attacker can obtain the sensors physically in several ways. For example, the attacker can capture the sensors from the sensing field in person. They can also collect sensors from the deployed area using unmanned vehicles. For the purpose of placing the sensors back to the original locations after compromising, the attackers might record the sensors' original locations. After obtaining the sensors, the attackers tamper the sensors and obtain the critical information (such as the cryptographic keys, the collected sensitive data, etc.) in the sensors.

The attacker can even add malicious code which can be used to attack the sensor network after rejoining the network into the sensors. The adversary then redeploys the compromised nodes back into the network. To minimize the chance of being detected, the attacker tries to put the compromised sensors back to the original locations based on the recorded location information before. In the following, we refer to this activity as node redeployment attack (or simply node redeployment). An attack similar to what we are addressing here is called node clone attack, in which the replicas of compromised sensors are inserted at strategic locations to launch attacks. This attack can be addressed effectively by discovering the existence of duplicate node ids in the network. However, the redeployment attack cannot be detected by the countermeasures for clone attack, since the compromised, original sensors are used for attacking.

D. Neighbor ship-based detection

In this scheme, each node has a set of monitoring nodes. For ease of presentation, we refer to the node being monitored as monitor and the nodes that monitor it's in the rest of the paper. The basis of the neighbors-based scheme is that different transmission power levels correspond to different transmission ranges. Thus, a certain neighbor can hear from the monitor only when the monitor transmits packets with a transmission power higher than a certain level. By having the monitor transmitting with all possible transmission power levels, each of its neighbors can record the power level from which the packets sent from the monitor start to be heard (note that any message sent using a power level higher than that can also be heard). If later a neighbor can overhear a packet from the monitor with a lower power level or only with a higher power level, it can suspect that the monitor is redeployed.

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. 2, Issue 2, February 2014

V. RESULT

Ns-2 is a discrete event simulator targeted at networking research. It provides substantial support for simulation of TCP, routing and multicast protocols over wired and wire-less networks. It consists of two simulation tools. The net-work simulator (ns) contains all commonly used IP proto-cols. The network animator (nam) is use to visualize the simulations.Ns-2 fully simulates a layered network from the physical radio transmission channel to high-level applications. Version 2 is the most recent version of ns(ns-2). The simulator was originally developed by the University of Cal-farina at Berkeley and VINT project the simulator was recently extended to provide simulation support for ad hoc network by Carnegie Mellon University (CMU Monarch Project homepage, 1999). The ns-2 simulator has several features that make it suitable for our simulations. A network environment for ad-hoc networks, Wireless channel modules (e.g.802.11), Routing along multiple paths, Mo-bile hosts for wireless cellular networks. Ns-2 is an object-oriented simulator written in C++ and OTcl. The simulator supports a class hierarchy in C++ and a similar class hierarchy within the OTcl interpreter. There is a one-to-one correspondence between a class in the interpreted hierarchy and one in the compile hierarchy. The reason to use two different programming languages is that OTcl is suitable for the pro-grams and configurations that demand frequent and fast change while C++ is suitable for the programs that have high demand in speed. Ns-2 is highly extensible. It not only sup-ports most commonly used IP protocols but also allows the users to extend or implement their own protocols. It also provides powerful trace functionalities, which are very important in our project since various information need to be logged for analysis.

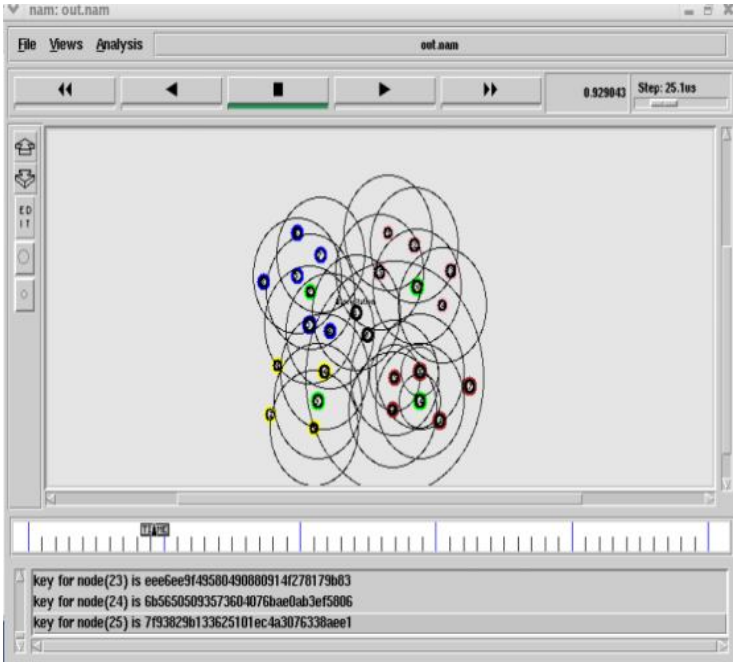


Fig 3: Output - Node, cluster head and base station is created

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. 2, Issue 2, February 2014

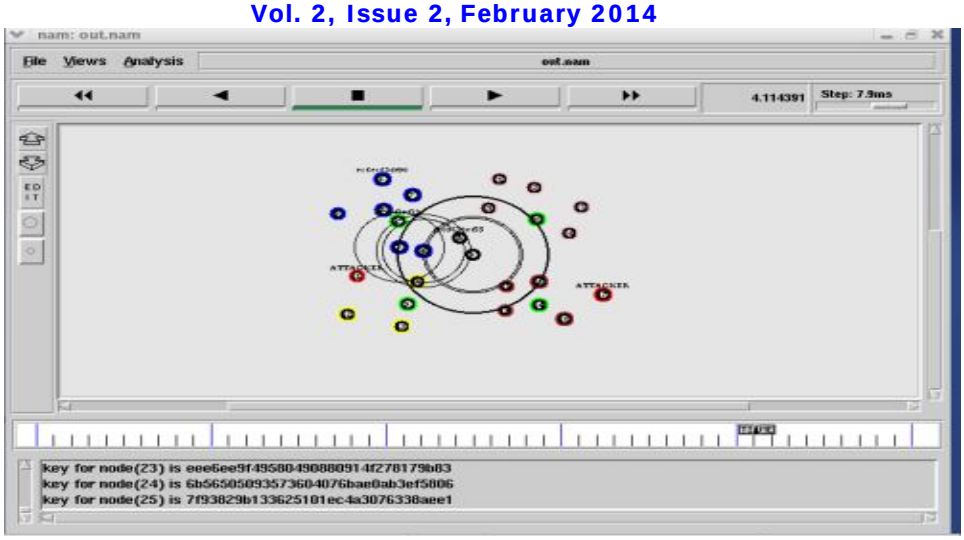


Fig 4: Output- Hacker is denoted in red color

Fig 3 denotes the creation of node, cluster and base station. Each are separated in each color. Node in each cluster has yellow, blue and pink this state node member in each cluster. Cluster is identifying in green color. Base station is noted as 0 nodes. Network is created and communication of packet is send between each. It uses LEAP Protocol so that it consumes low power and better coverage area.

Fig 4 state that new adversary node is denoted as hacker. Because use symmetric key and shifting the key is done by the base station for every particular time. So the even a node is compromised the hacker is unable to Identify the node. The behavior of the node is monitor by the base station by the behavior color change as mentioned above as related in transition diagram.

VI. CONCLUSIONS

To sum up, the above scheme meets such high safety requirements as safely reserving the master keys, safe generation and distribution of private key, secure communication between cluster heads ,safe updating of keys between the communication links. We introduced a mechanism of trust management in cluster head election. Trust management mechanism, as an important complement for password-based system, has significant advantages for the WSN in the settlement of internal attack, identifying malicious nodes, system security and reliability improvement, and so on.

REFERENCES

1) Roberto Di Petro, Gabriele Logier, Claudio Oriented, and Gene Tsudik, “United We Stand: Intrusion Resilience in Mobile Unattended WSNs”, IEEE Transactions on Mobile Computing, Vol. 12, NO. 7, July 2013.
2) A. Falchion, "Sensor networks: Performance measurements with motes technology ", in Dept. of Information Engineering, vol. Master’s thesis: University of Pisa, 2004.
3) A. Bharathidasan and V. A. S. Ponder, "Sensor Networks: An Overview", Technical Report, " Dept. of Computer Science, University of California at Davis 2002.
4) M. Tubaishat and S. Maria, "Sensor networks: an overview", IEEE Potentials, vol. 22, pp. 20-23, 2003. [4] I. F. Akyildiz, Y. S. W. Su and E. Cerci, " Wireless Sensor Networks: a Survey", Computer Networks, vol. 38, pp. 393-422, 2002.
5) V. Rajaravivarma, Y. Yang and T. Yang, "An Overview of Wireless Sensor Network and Applications ", in The 35th Southeastern Symposium on System Theory, 2003.
6) G.Werner-Allen, K. Lorenz, M. Ruiz, O. Marcello, J. Johnson, J. Lees and M. Welsh,
7) "Deploying a Wireless Sensor Network on an Active Volcano", IEEE Internet Computing, 2005.

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. 2, Issue 2, February 2014

8) G. Werner-Allen, J. Johnson, M. Ruiz, J. Lees and M. Welsh, "Monitoring Volcanic Eruptions with a Wireless Sensor Network", in Second European Workshop on Wireless Sensor Networks (EWSN05), Istanbul, Turkey, 2005.
9) D. Culler, D. Estrin and M.Srivastava, "Overview of Sensor Networks", IEEE Computer Journal, vol. 37, pp. 41-49, 2004.

BIOGRAPHY

Mrs. P.UTHAYA BHANU presently pursuing final year M.Tech in Electronics and Communication Engineering, In PRIST University, Puducherry campus, Puducherry, India.

Mr. J. SARAVANAN Received the M.E., In. Presently he is a Working Assistant Professor in Electronics and Communication Engineering at PRIST University, Puducherry Campus, Puducherry, India