JEAS | Journal of Economics and Administrative Sciences
E-ISSN: 2148-1792 P- ISSN: 1302-2024
Volume 4, Supplement Issue 1
www.jeasweb.org

A Trust Management-Based Security Mechanism in Wireless Sensor Networks

Samira Tabandeh
Master of Computer Software Orientation, Islamic Azad University, Kerman, Iran.

Farokh Koroupi
Head of computer department, Ph.D from Birmingham university of England, Birmingham, England.
Assistant Professor, Azad university of Baft, Baft, Iran.

Masoud Zamani, Ph.D.
Assistant Professor, Department of Public and International Law, Shiraz University, Shiraz, Iran.

ABSTRACT

This research has examined the trust-based routing protocols for sensor networks and tried to present a trust-based solution for the protocols that are consistent with the proposed protocol. Regarding that the previous security methods to were not suitable to resist against attacks such as encryption, key management and using IDS due to the high computation overhead and their high costs, and also the weakness of these methods after disclosing the password mechanism, a trust-based method was suggested to solve these problems. The salient feature of this method is its negligible computation overhead and energy loss, in one hand, and counteracting the attacks and repairing the defects in the sensor network, on the other hand. The proposed protocol and mechanism were simulated by using NS2 simulator software and the feedback of the proposed method in counteracting the number of malicious nodes has been evaluated. The results of comparisons indicate the proper performance of the proposed protocol and mechanism in detecting and countering the attack. The suitability of the results reveals that using the trust method is a useful solution to achieve a secure and safe network and to solve the problems of sensor networks' security.
Keywords: wireless sensor networks, trust method, routing, neighbor, sensor network attacks

Introduction

Wireless sensor networks have gained more interest in recent years due to their widespread applications in the military and civilian operations. Many ad-hoc networks have critical tasks, therefore, it is clear that the security should be considered during design. Trust-based routing in wireless sensor networks is a new phenomenon and unexplored activity (1).

One of the tools used to solve the security problems of sensor networks is the trust mechanism that is taken from human and social relationships. This trust can be related to each object in the network, such that the trust threshold can be estimated for one node relative the neighbor node, routing node, connection ling, sink, and base station. Then, the node can evaluate the trust metric based on some approaches and select the best action (2). In recent years, wireless sensor systems have gained much interest due to their

widespread use in military and civilian operations. Many ad-hoc networks have critical duties; therefore, it is clear that security should be considered during design. Trust-based routing in wireless sensor networks is a new phenomenon and unexplored activity.

Wireless sensor networks are vulnerable to security attacks due to their wireless function. This condition becomes worse because they work in an environment without infrastructure. This causes all network tasks including routing are done by the contribution of nodes. This means that all nodes act as a router and sent all packets produced by their neighbors in their route to the sink node. As a result, malicious nodes (instead of their function) influence the network operation. Security in the classic network is generally provided through authentication and encryption. These techniques can be considered as the first defense line because they are preventive and cannot develop a complete security framework for sensor networks (3). In fact, using these techniques cannot prevent an endangered node that is an authenticated component in the network and can do any wrong action. In sensor networks that lack infrastructure, the nodes rely on their cooperation for routing and sending their packets to the base station. Many attacks, in particular, target the routing processes; for example, in a black hole attack, a node shows selfish behavior and avoids sending traffic to its neighbors. This condition can become worse when this node propagates its routes to attract network traffic, in addition to non-sending traffic data. Another set of attacks is based on changing packets (even routing packets or data packets) that can ruin the routing process and lead to the wrong routing of traffic by nodes, or even they can manipulate and destroy the packet that reaches the sink. Another attack is a Sybil attack in which a node pretends that it has the properties that lack them; wormhole attack is another type of attack in which more than one node cooperates to attract the passing data by disturbing the routing process. A humanistic approach has been proposed to resist these attacks in which nodes supervise the behavior of their neighbors to evaluate their trust by considering certain behavioral aspects that are called trust metrics (4). Based on this, nodes develop trust relationships among themselves and take routing decisions not only based on the geographical data or other weak routing data but also based on their prediction of honest participation of their neighbors (or their trust to them). In other words, a trust management system is implemented (5). Although key-based methods can be used to preserve the accuracy of data and authentication methods and encryption are robust tools to preserve the accuracy of packets and trust of nodes, they are not able to detect a large set of routing attacks, like selfish behaviors, selective delivery, backhoe, and eavesdropping attack. A trust model is used for the decisions of higher layers like routing, data aggregation, selecting cluster head or even key distribution.

The trust management method is a robust tool to detect an unexpected behavior of nodes (even malicious or failed nodes). When malicious nodes were identified, their neighbors can use their information to prevent their participation in data delivery, data aggregation, and other participatory activities. Currently, trust is a hot topic in the discussion about different networks like peer-to-peer and ad-hoc networks. Trust method is more robust than traditional encryption methods and can solve the problems that they cannot solve, for example, the judgment about the behavior of sensor nodes. Trust management is necessary to develop secure and reliable applications in sensor networks (6). Since sensor networks have unique challenges, the existing trust models cannot be used for them (7). Therefore, a new approach is needed to protect against security attacks. This research tries to present a preventive security method in the routing protocol by identifying and applying security mechanisms in ad-hoc networks.

This study aims to provide a trust-based protocol and algorithm to show this capability. The use of the trust method should consider the conditions and constraints of these networks. The purpose of routing is presenting a protocol that, in addition to security, increases the tolerance of attacks and the life-span of the sensor network. In this protocol, a suitable path is selected by using the trust method to meet the goal of reducing the lost packets. In terms of tolerance, we aim to provide a protocol that can send the right information which is its main task. To achieve this goal, the malicious nodes are detected in this protocol by using the trust method and nodes with high reliability, send the information. In this protocol, the trust method in each node is responsible to select the node and proper delivery path.

Materials and Methods

1. Proposed OLSTR protocol

In this algorithm, the paths will be considered both according to their shortness as well as other security features. Only the nodes with the determined security requirement can participate in algorithm routing and forwarding the packets. The major goals of the proposed protocol are:

1. Implementing a trust management protocol that has inherently developed for routing protocol.
2. Delivering the packets to the known nodes with the highest trust level.
3. Achieving high efficiency in routing by limiting the irregular exchange of packets along the path.
4. Reducing the number of dropped packets that only create overhead in the routing.
5. Optimizing the use of resources.
6. Obtaining good performance of the network.
7. Adapting ti changes of the network including topology, density, etc.

How the proposed trust management algorithm works

The designed trust management algorithm works as follows: after the formation of a graph in the network, if a node intends to send data, first it sends a Hello message to the destination node. This message contains a scheduler and a random number that is produced by the source. The destination node should receive the packet and add a unit to the random number at the scheduled time; then, it should send the packet to the source. If it did not return the packet at the scheduled time, 30% will reduce its trust and if it sends a packet with an improper response, 30% of its trust will also reduce. If it sends no packet, another 30% of its trust will reduce. In the trust of a node becomes less than 75%, this node will be blocked. The blocked node cannot receive or send a message. This process will continue until the source node has no neighbor except this node. In this step, the source node would test this node again. If the node acts properly, the source node will add 30% to its trust and the node will be released from blockade but it remains as the nodes with low trust.

The implementation phase of the proposed protocol

To select the proper path for data delivery, MPR compares all the tables received from subset nodes so that by using column analysis, it can determine how many steps a node is away from other nodes. Because each node has the information of its neighbors in these analyses, if a malicious node enters the set, the proposed trust metric can show whether it is reliable or unreliable. If there is a doubt about the reliability or unreliability of two nodes, both nodes should be evaluated. After the required evaluation and detection of the malicious node, that node becomes unreliable and quarantined such that we receive no message from it and send no message to it.

Now, if a node intends to deliver data to the other node, the metric to select the proper path is as follows and we add a trust metric to it. Our ideal metrics are:

- The smallest sequence number: because this node was currently active and participated in routings and it has updated data.

-it has the minimum distance (using Dijkstra algorithm)

-it has the highest trust;

W=SNmin+Xmin+Trust

Now we can consider another assumption. We allocate a trust threshold to each node in the network and each node in the network can tell lie only two times because the node may be valuable and we want to consider a punishment threshold for it (8).

It is worthy to mention that when the trust is given to the node that has told lie once or twice that we have no path to deliver data to the destination and we are forced to use them. If this node does its task properly, we will increase its trust each time (9).

Simulation of protocols

Network simulator software provides the ability to simulate the connection networks without using coding through graphic interfaces. In these cases, the presence of simulated elements that correspond to the real elements (router, switch, etc.) increases the precision, ease, and speed in the simulation process.

Therefore, it is suitable for those users who are not familiar with programming. The aim of this simulation is the study of the effect of one or several parameters (for example the length of packets or buffers capacity) on the network efficiency; therefore, repeatability is a necessary condition for this software.
In sum, we should note that the development of a precise and reliable network simulator requires using the simulation technology along with the network knowledge and its protocols.

NS2 Simulator

NS Simulator has developed before the VINT project. NS simulator was developed in 1989 by the NRG network research group in LBNL lab and it is designed based on another network simulator called REAL that its development continued up to now and accelerated after selecting it as a VINT project simulator [10].
NS2 is a discrete event simulator and conducts simulation by tracking events as discrete times. This simulator is designed in an object-oriented form in C++ and OTCL programming language (fig. 1).
Network simulators have consisted mainly of two parts with different intentions:
1. A group of building blocks that simulate the elements like nodes, links, queues, traffic generators, and protocols.
2. An interface that is called Simulation Description Language (SDL) and its task is to connect the building blocks in the simulation process.

Designers of network simulators face an essential problem in these two parts. Although the efficiency and the speed of implementation are the major goals for building blocks, SDL needs flexibility and ease of changing the configuration. Achieving these two goals with the same programing language is difficult. Therefore, the VuSystem model proposed by David Wetherall at MIT University suggests that the solution to this problem is using two separate programming languages for each of them. According to this model, a compiler language (C++) is used for building blocks and an interpretive setting (like OTCL) is used for their interface.

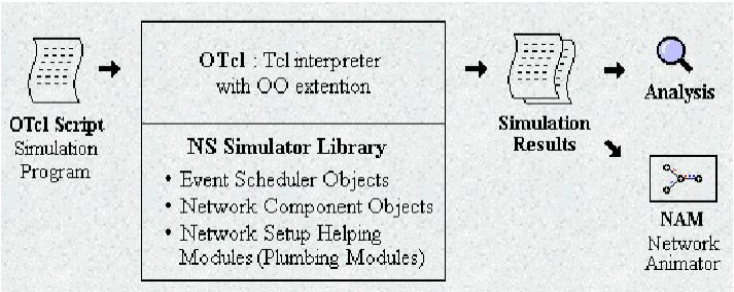

Fig. 1: NS2 schematic from the user's view

NS2 designers, using a set of objects called two-pieces objects, succeeded in applying VuSystem to their simulator. According to this model, NS2 consists of a set of objects that communicate with each other in binary compiler/interpretive environments by calling other methods (fig 2).

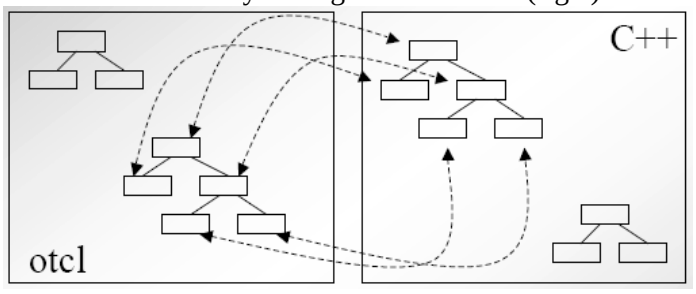

Fig. 2: Calling C++ and OTCL methods by each other

Results and Findings

The simulation evaluation and comparison of the proposed OLSTR protocol with OLSR is done. In trust-based routing, we can consider several modes: Node to node trust, node to link trust, node to cluster head trust, node to sink trust, and vice versa. Besides, each of these methods can be implemented indirectly such that a node evaluates its trust to the neighbor node through network events and receiving neighbors' reports. Therefore, there are various solutions to implement a network trust mechanism.

Table 1: Simulation parameters

Effective parameters	First scenario	Second scenario	Third scenario
Physical layer	Phywireless-Mica2	Phywireless-Mica2	Phywireless-Mica2
Type of antenna	OmniAntenna	OmniAntenna	OmniAntenna
Qeue type	DropTail/preQ	DropTail/preQ	DropTail/preQ
Qeue length	50	50	50
Energy sourse	Battery model	Battery model	Battery model
Network size	1000*1000m	1000*1000m	1000*1000m
Number of AP	1	1	1
Network distribution	Random	Random	Random
Simulation time	500s	500s	500s
AP location	Network center	Network center	Network center
AP initial energy	100J	100J	100J
AP communication range	200m	200m	200m
Number of nodes in sensor network	50	50	50
Nodes communication range	50m	50m	50m
Sensing interval	5s	5s	5s
Nodes initial energy	10J	10J	10J
Number of malicious node	3	6	9

Tests of two protocols

First test: 50 nodes and 3 malicious nodes

Second test: 50 nodes and 6 malicious nodes

Third test: 50 nodes and 9 malicious nodes

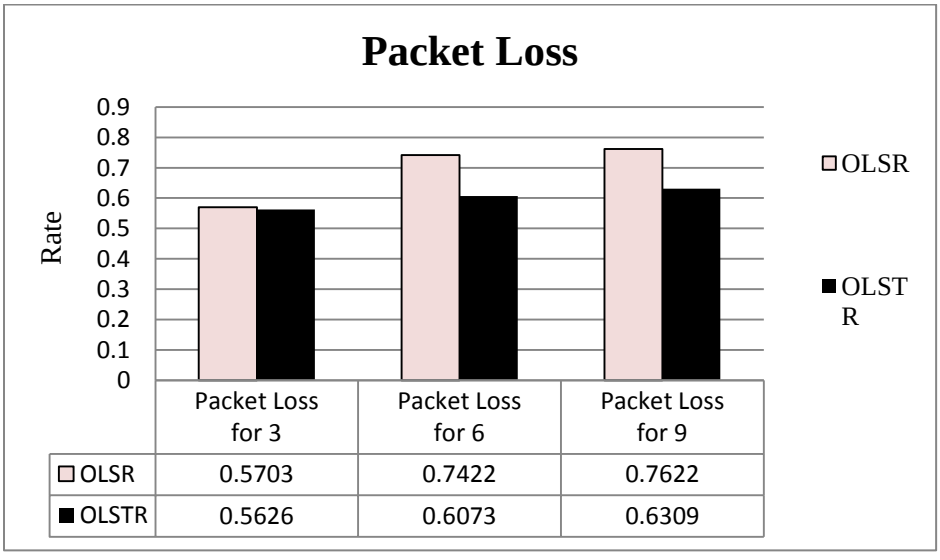

Fig. 3: Number of lost packets

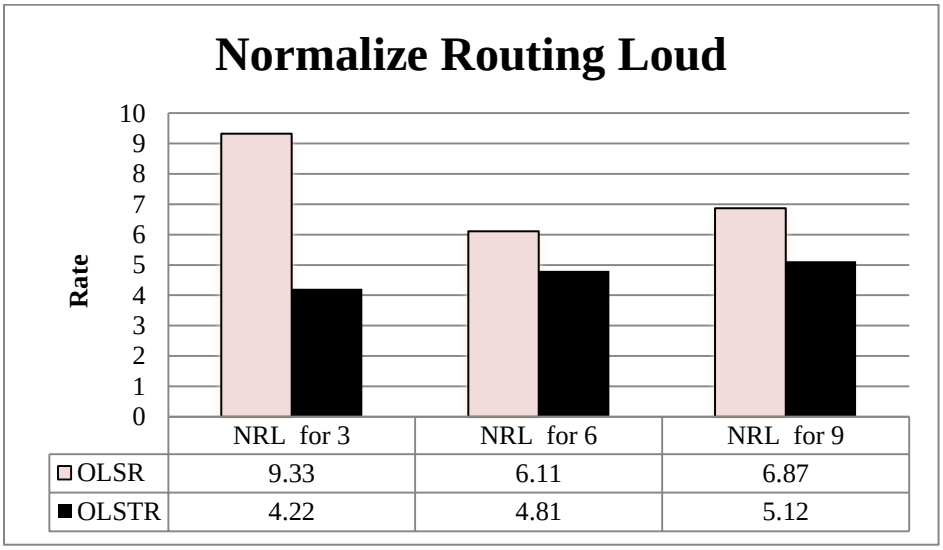

Fig. 4: Normal routing rate

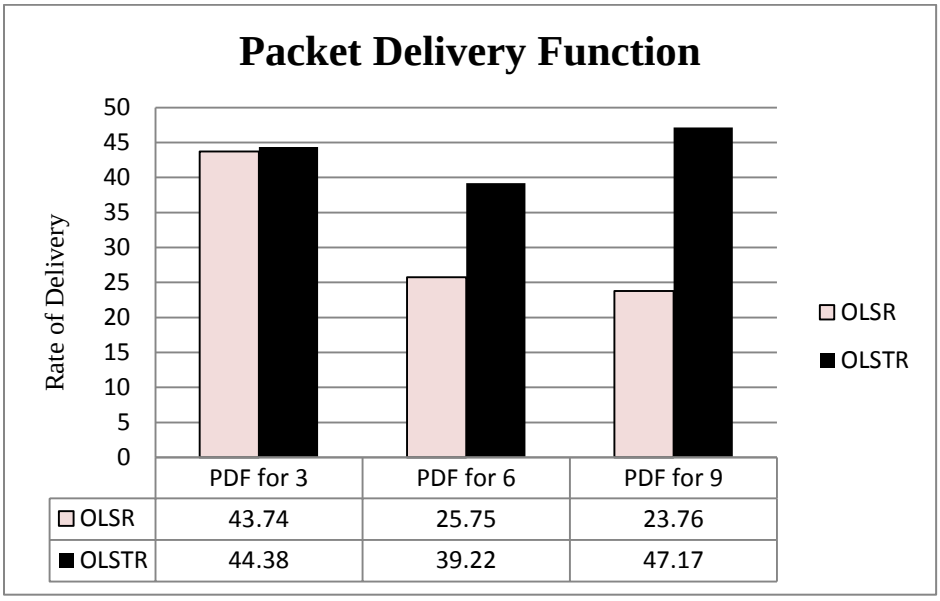

Fig 5: Rate of packet delivery

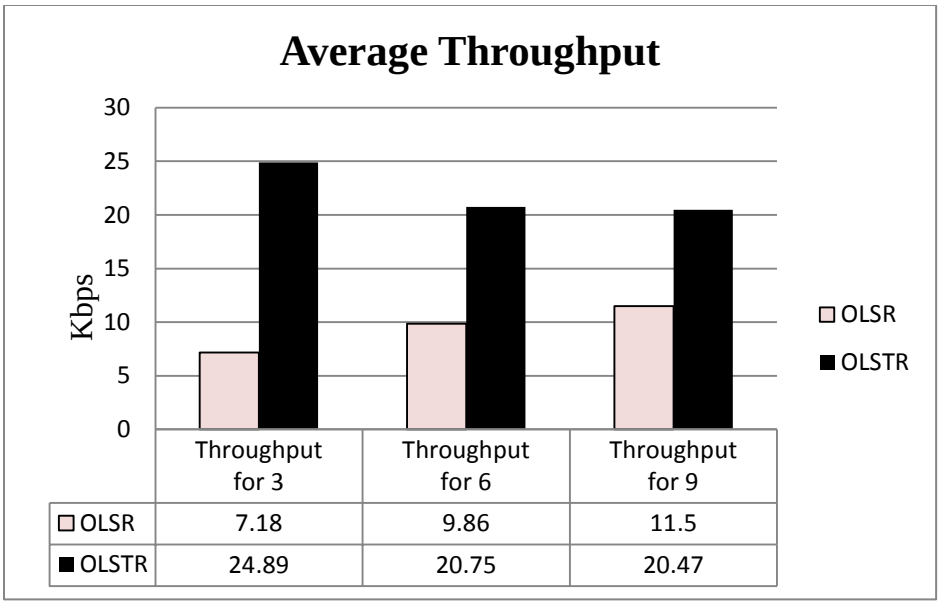

Fig 6: Mean throughput rate

Results of Simulation

To evaluate the OLSR protocol for which the proposed trust mechanism is used (OLSTR) and OLSR protocol that lacks security mechanisms were simulated by using NS2 simulator software (Palmieri et.al, 2011) and the results were compared. 50 sensor nodes scattered in 1000*1000m2 area for simulations. Sink node is randomly placed among these 50 nodes. The nodes receive the temperature of the environment and inform their changes to the sink node. The efficiency of OLSR and OLSTR was tested for a different number of malicious nodes. These tests aim to obtain the rate of lost packets by increasing the number of malicious nodes, the rate of delivered packets, normal routing rate, and throughput rate of the proposed protocol. Some measures are provided for this purpose in the proposed protocol.

Conclusion

There are various problems in the sensor networks and different algorithms and protocols have been presented to solve them up to now. One of these problems is the security and trust-based routing.

Recently, trust is a hot topic in discussions about the different networks including peer-to-peer and ad-hoc networks. The robustness of the trust method is higher than traditional encryption methods and it can solve the problems that other methods cannot. Since sensor networks have unique challenges, the existing trust models for other networks cannot be used for them. Therefore, we need a new approach to counter security attacks. The trust method is, in fact, the confidence of node Si that node Sj acts according to prediction in cooperation between node I and node j. The proposed algorithms and protocols for solving these problems should consider various issues like low energy consumption, low delay, limited bandwidth, longevity, minimum interruption, and security-related issues (11). The features of the trust method show that this method can solve the security and confidence issues in the sensor networks. Among salient features of the trust method, we can refer to the effectiveness of this method in the distributed and multi-factor setting with limited communication, incomplete data, and simplicity of the structure. Since the application of wireless sensor systems increases day by day, the qualitative issues in these networks have gained high importance (12). Cases like uninterrupted network connection, service quality based routing and covering, the accuracy and health of sensed data, data security, and such are among these uses. Recently, we observe that the research direction is toward ensuring the quality of the network depending on its function. One of these cases is trust-based routing in wireless sensor networks (13).

This study proposed a trust-based routing protocol that uses trust metrics and network parameters simultaneously. OLSTR protocol was compared to OLSR's basic protocol for the evaluation in the same conditions and NS2 simulation methods and the obtained results were compared. The results indicate the proposed protocol has outperformed OLSR protocol in the effective network parameters including lost packets rate, normal routing rate, packet delivery rate, and mean throughput rate of the network and showed better efficiency. The proposed method has low overhead and network cost and contrary to various security measures, no disruption occurs in the network in the case of disclosing keys and encryption methods because the malicious node immediately becomes isolated and receives or delivers no packet. Regarding what has been said in this research, the trust method can be used to provide security for proactive protocols in different types of sensor networks. The trust mechanism can be implemented by using inherent topological data of these protocols, directly or indirectly. In this section, we used direct trust metric but these protocols can implement trust including node to node, node to MPR, MPR to MPR, MPR to sink and vice-versa.

References

[1] Momani, Mohammad, and S. Challa. 2010. Survey of trust models in different network domains. ArXiv preprint arXiv: 1010.0168.

[2] Wang, G., W. Zhou and L.T. Yang. 2013. Trust, security and privacy for pervasive applications. The Journal of Supercomputing: 1-3.

[3] Li, X., M.R. Lyu, L. Jiangchuan. 2004. A Trust Model Based Routing Protocol for Secure Ad hoc Networks. IEEE Proceedings on Aerospace Conference, vol. 2.

[4] Kumar, G., I. Titus and S.I. Thekkekara. 2012. A Comprehensive Overview on Application of Trust and Reputation in Wireless Sensor Network. Procedia Engineering 38: 2903-2912.

[5] Prathapani, Anoosha, L. Santhanam and D.P. Agrawal. 2013. Detection of blackhole attack in a Wireless Mesh Network using intelligent honeypot agents. The Journal of Supercomputing: 1-28.

[6] Shaikh, R. Ahmed and (et al). 2009. Group-based trust management scheme for clustered wireless sensor networks. Parallel and Distributed Systems, IEEE Transactions on 20.11: 1698-1712.

[7] Dhulipala, V. Sarma, N. Karthik and R.M. Chandrasekaran. 2013. A Novel Heuristic Approach Based Trust worthy Architecture for Wireless Sensor Networks. Wireless Personal Communications: 1-17.

[8] Denko, K., Mieso, Tao Sun and I. Woungang. 2011. Trust management in ubiquitous computing: A Bayesian approach. Computer Communications 34.3: 398-406.

[9] Samundiswary, P. 2012. Trust based Energy aware Reactive Routing Protocol for Wireless Sensor Networks. International Journal of Computer Applications (0975 – 8887) Volume 43– No.21

[10] Boukerch, A., L. Xu, and K. El-Khatib. 2007. Trust-based Security for Wireless Ad-Hoc and Sensor Networks. Computer Communications, 30:24132427.

[11] http://www.pmel.noaa.gov/vents/acoustics/sosus.html. 2013.

[12] Chen, Chin-Ling, Yu-Ting Tsai, and Tzay-Farn Shih. 2012. A novel key management of two-tier dissemination for wireless sensor network. Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), Sixth International Conference on. IEEE.

[13] Babu, S.S., A. Raha, M.K. Naskar. 2011. Trustworthy Route formation Algorithm for WSNs. International Journal of Computer Applications (0975 – 8887) Volume 27– No.5.