A Hierarchical Secure Routing Protocol for Mobile Wireless Sensor Network based on Cryptography

Sathyanarayana S
Department of Computer Science and Engineering
JNNCE, Shimoga, Karnataka, India

Vishwas C.G.M
Department of Information Science and Engineering
JNNCE, Shimoga, Karnataka, India

Abstract - There are quite a few of routing protocols designed for Wireless Sensor Networks (WSNs). These routing protocols can be categorized in accordance with the network organization. But these protocols did not consider the following issues concurrently: mobility of the sensor nodes in addition to the base station, security of network layer and energy. LEACH (Low Energy Adaptive Clustering Hierarchy) and LEACH-Centralize are the routing protocols which follows hierarchical manner. However in both LEACH and LEACH Centralize, the network is split into clusters and all clusters hold an elected sensor node. But LEACH and LEACH-Centralize are not suitable for large WSN which covers large geographic area because of direct communication between Cluster Head and Base Station. They also do not take care of link or node failure. A new secure routing protocol is proposed for wireless sensor networks in which sensor nodes as well as the base station are mobile. The protocol achieves security property through symmetric key cryptography and threshold key cryptography. An analysis of the security strengths of the protocol is presented. Simulation results show the throughput of the proposed protocol and a comparison with LEACH regarding its throughput.

***Keywords* - Wireless Sensor Networks, Secure Routing, Energy Efficiency, Mobility.**

I. INTRODUCTION

A **wireless sensor network (WSN)** consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location. Security in wireless sensor network (WSN) is an extremely important issue and in the recent time it has got significant attention from the research community. There exist various security threats at different layers of the protocol stack of wireless sensor networks and also security threats in routing layer. The various threats at the network layer are tampering of routing information, sinkhole attacks, wormholes, selective forwarding and HELLO flood attacks etc. It is also important to develop secure routing protocol which is well suited for the resource constrained WSNs. The process of routing in wireless sensor network is different from those in other TCP/IP based networks. Any intermediate node in a route from a source node to a destination node may have to open the message/packet in transit and then again to forward the same. Since routing in WSN may be attribute based this phenomenon of accessing packets in the intermediate nodes is very common and that is why end to end security provisioning through secure socket layer (SSL) is not feasible for wireless sensor network routing process. Since the sensor nodes are resource constrained it is also not feasible to deploy asymmetric key cryptographic algorithms which are computation intensive. It is a challenging task to develop secure routing algorithm which can provide good enough security level and also feasible to implement in the resource constrained wireless sensor networks. In this paper we propose a secure routing algorithm for mobile wireless sensor networks in which sensor nodes as well as the sink are mobile. The mobility of the nodes as well as the sink increases the complexity of the system and poses significant challenge in front of the designers of WSN system. We adapt symmetric key cryptography which is feasible to implement in the resource constrained sensor nodes. In the proposed protocol we use some unconventional simple techniques which lead to secrecy of information in the system. Our simulation results show the performance of the proposed protocol in terms of throughput.

The rest of the paper is organized as follows: in section II some related work to the routing in WSN are given followed by section III in which system model adapted in this paper is described. The proposed protocol is described in the section IV and section V analyses the security strength of the proposed protocol. Section VI presents some simulation results regarding the performance of the proposed protocol and finally the paper is concluded in the section VII.

II. RELATED WORK

There are several routing protocols for WSN proposed so far. These routing protocols can be categorized according to the network structure or protocol operation. There are few secure routing protocols which take care of the security issues in the network layer of the protocol stack. For example, SPINS [1], TinySec [2], SIGF [3], FBSR [4] are some examples of secure routing protocols. But none of these protocols consider the following issues simultaneously: *mobility of the sensor nodes as well as the base station*, *network layer security issues* and *energy efficiency*. The proposed protocol can take care of all these three issues and can be classified as hierarchical (network structure) routing protocol.

LEACH (Low Energy Adaptive Clustering Hierarchy) [5] and LEACH-Centralize [6] are some early routing protocol developed for WSNs which are hierarchical so far the network structure is concerned. In both LEACH and LEACH-Centralize the network is divided into some clusters and each cluster contains an elected sensor node which acts as the Cluster Head (CH). The CH nodes manages communication among cluster member nodes, does data aggregation and also relay the aggregated sensory data to the base station directly. LEACH and LEACH-centralize outperform the direct communication protocol (flat network architecture) in terms of network life time. But LEACH and LEACH-Centralize are not suitable for large WSN which covers large geographic area because of direct communication between Cluster Head and Base Station. They also do not take care of link or node failure.

SONS (Self Organizing Network Survivability) [7] are a hierarchical routing protocol for WSN designed to cope with the large area of deployment. It can take care of link or node failure situations. This protocol does not consider mobility of sensor nodes or the base station. SHIVA [8] is an energy efficient hierarchical routing protocol which considers the mobility of sensor nodes as well as the base station. It does not consider the security issues in the network layer. SPINS [1] is a secure routing protocol designed for static wireless sensor networks. It consists of two building block security protocols namely SNEP and μTESLA. SNEP provides confidentiality and authentication between nodes and base station and also freshness of data. μTESLA provides authenticated broadcast mechanism which is an essential component for security of the sensor network.

III. SYSTEM MODEL

The major goal behind the wireless sensor network model considered in this paper is gathering of data through mobile sensor nodes and delivering those at the base station which is again a mobile node and located far away from the sensor field. In this section we enlist some assumptions made in order to simplify the problem of routing under mobile environment. We consider a two-dimensional rectangular sensor field in which some sensor nodes are deployed randomly. The sensor nodes are moderately mobile and this mobility is due to the mobility unit attached to the sensor hardware or the sensor nodes may be attached to some mobile object. We do not consider the energy expenditure due to the mobility circuit. There is only one mobile base station and the base station may be a powerful laptop computer carried by a person in motion. It is assumed that it is not feasible to recharge the battery of the sensor node and that is why sensor nodes are energy constrained. The base station can be recharged and is a resourceful node. It is assumed that the sensor nodes can reveal their location information through GPS free solution. The base station can collect location information from the sensor nodes in the field whenever required. Energy expenditure due to communication i.e., transmission and reception obeys the first order radio model [5]. It is also assumed that the radio power can be controlled, i.e., a sensor node can vary its transmission power depending on the distance to the receiver. This is feasible, for example, Berkley Motes have in total 100 power levels. This helps in energy saving during intra-cluster (i.e., short range) and inter-cluster (i.e., long-range) communications. The sensor nodes are homogenous and have equal energy at the time of deployment.

IV. PROPOSED PROTOCOL

In this section, we present a secure routing protocol for mobile wireless sensor networks. The proposed protocol is hierarchical. One of the key features of the protocol is that it takes care of the link breaks between ordinary node and cluster head nodes and also between two cluster head nodes in any route towards the base station. The protocol selects a cluster head set inside each cluster instead of one cluster head node per cluster. For selecting the members for the cluster head set different attributes of the nodes inside a cluster are considered. Those attributes are average distance to the base station, remaining energy level, closeness of the neighbor nodes, and the number of times cluster headship already taken. The base station selects the members of the cluster head set. The candidate nodes which are above the required threshold value for becoming a member of the cluster head set are selected as the members of the cluster head set. This threshold value may be set initially depending upon the condition of the nodes such as initial energy level of the nodes, mobility level of the nodes and the size of the sensor field along with the position of the base station. The threshold value is a cumulative value of the different attributes considered for selecting the cluster head set members. The protocol may be discussed in terms of five stages namely, Cluster Setup, Route Discovery, Route Establishment and Data Transmission, Route Maintenance, and Security Management.

A. Cluster setup

After deployment of the sensor nodes in the area of interest the clustering process starts. The entire sensor field is logically divided into some clusters by the base station and each cluster is a group of some sensor nodes. Each cluster covers a geographic area in the sensor field. After formation of the clusters the base station selects the members for each cluster head set per cluster. For selecting the members for the cluster head set different attributes of the nodes inside a cluster are considered. Those attributes are: Average distance to the base station, Remaining energy level, Closeness of the neighbor nodes and the number of times cluster headship already taken.

B. Route Discovery

In this phase the routes for data transmission are discovered. The communication is hierarchical and essentially the sensor nodes inside each cluster send data to the respective chief cluster head (CCH). There are two kinds of routes in the system: *intra-cluster route* and *inter-cluster route*.

In case of intra-cluster route the situation is straightforward. Each node knows it's *Cluster-id* and CCH and these are informed by the base station. Therefore each sensor node transmits its data to the CCH. If the CCH is not within the range of any cluster member node then the node may transmit data to any one member of the cluster head set.

Inter-cluster routes are formed by considering the CCH nodes in the sensor field. The base maintains information (*id* and *geographic location*) about CCH nodes of each cluster. The base station discovers the graph, G (V, E), considering only the CCH nodes as the set of vertices V and available links among the CCH nodes as the set of edges E.

C. Route Establishment and Data Transmission

In this stage a particular route is established for data transmission for a particular duration of time. For the *intra-cluster routes*, the CCH distributes TDMA based medium access time slot to its cluster members and the cluster members transmit data to their CCH as per this medium access control information. The routes are valid only during particular time intervals. If the CCH node becomes unavailable the next member in the cluster head set takes over as the CCH and then it distributes a new TDMA based medium access time slot to its cluster members. For *inter-cluster routes* the base station distributes the energy efficient multi-hop / direct routes to each of the CCH nodes. Since multiple routes are available between a CCH and the base station, the base station compels the CCH to switch the multi-hop routes in order to balance energy consumption in the intermediate CCH nodes. The base station keeps on distributing alternate routes in order to optimize the energy consumption in the intermediate nodes. If an intermediate node in an *inter-cluster route* fails, the fault will be resolved automatically during the next time interval when the base station asks the CCH to switch to another alternate route (disjoint). The base station distributes the medium access control information to the CCH nodes. It may be assumed that the CCH nodes use different frequency bands for data transmission as specified by the base station. When the data packets are forwarded (i.e., transmitted) each forwarding node adds its identity ID at the end of the packets. This feature allows the base station to discover the route traveled by the packets. Moreover each data packet is uniquely identified by a *sequence number* that is assigned at the originating node.

D. Route Maintenance

All route information is maintained in the base station. Majority of the route computing burden is shifted to the base station as the sensor nodes are resource starved and mainly energy constrained. The sensor nodes fully devote in data transmission as per the route information distributed by the base station. The sensor nodes including the CCH need to store only the current route as distributed by the base station. Based on the current topology of the wireless sensor network which is determined by the current location of the live nodes, the base station keeps on computing the *intra-cluster* and *inter-cluster routes* as mentioned before. All the computed routes are maintained in the base station and these routes distributed by the base station to the intended parties in right time.

E. Security Management

This phase makes this proposed routing protocol unique. This section describes the security features of the routing protocol. Various security keys are used for making the routing process secure. The protocol uses principles of symmetric key cryptography and threshold key cryptography. The base station generates various security keys and distributes to different nodes. The encryption and decryption processes are carried out using appropriate keys.

Various security keys: There are two major kinds of communication namely *intra-cluster communication* and *inter-cluster communication*. Therefore two sets of security keys i.e., intra-cluster keys and inter-cluster keys are used for secure communication. The base station distributes a unique secret key, $((key)_{CH})_i$, to each of the members of the cluster head set. The base station also distributes a common secret key, $(key)_{SN}$, to all the legitimate cluster members and CCH except the other cluster head set members. This key is unique to a cluster. Thus intra-cluster key set for a cluster k is $\{((key)_{CH})_i, (key)_{SN}\}$. The base station again distributes unique secret keys, $((key)_{CCH})_i$, to each of the CCH nodes in the WSN system. This key is used for inter-cluster communication. Thus inter-cluster key set is $\{((key)_{CCH})_i\}$. The base station refreshes these keys after a regular interval of time and distributes those encrypting with previous appropriate secret keys. It is assumed that each node i comes with a preinstalled embedded unique secret key called *initial key*, $((key)_{ini})_i$, and identification number, ID. The base station uses this *initial key* and *ID* during encryption for distributing various keys to the appropriate nodes. The combination of *initial key* and *ID* is a unique and secret piece of information available with the base station and the node under consideration only.

Various secure communication types: This section describes different types of secure communication types in the WSN system. As already mentioned there are two major types of communication namely intra-cluster and inter-cluster communication.

Intra-cluster communication: The sensor nodes transmit sensory data to the CCH nodes by encrypting through the common secret key, $(key)_{SN}$ and a threshold number of cluster head set members secret key, $((key)_{CH})_i$. The CCH can decrypt the received data only when it acquires a threshold number of unique secret keys of the cluster head set members. The intra-cluster communication is based on the principles of threshold key cryptography [9].

Inter-cluster communication: The CCH nodes throughout the WSN system take part in inter-cluster communication in order to transmit data towards the base station. Each CCH node encrypts data by using a threshold number of unique secret keys of CCH nodes i.e., $((key)_{CCH})_i$, and transmits to the next hop in the route towards the base station. Similarly in order to decrypt the data packets each CCH node has to acquire a threshold number of such secret keys in the system. The value of the threshold number is decided by the base station and it also depends on the application type. Again a sender/receiver entity acquires threshold number of secret keys (for *intra-cluster* as well as *inter-cluster* communication) from other appropriate entities by exchange of messages These messages are encrypted / decrypted by a proper secret key which is distributed by the base station. Only legitimate and needy nodes are given this secret key by the base station. This is an instance of symmetric key cryptography.

Base station-sensor node communication: The base station distributes the route information as well as different secret keys to the sensor nodes. As already mentioned, the base station uses *initial key* and *ID* of the receiver node for encryption of the packets containing secret key information. Similarly the base station uses various keys for encryption of routing information before those are distributed to different intended nodes. Those keys are: *initial key* $[((key)_{ini})_i]$, *ID* and any one of the available secret keys in the receiver node $[((key)_{CH})_i, /(key)_{SN} / ((key)_{CCH})_i]$.

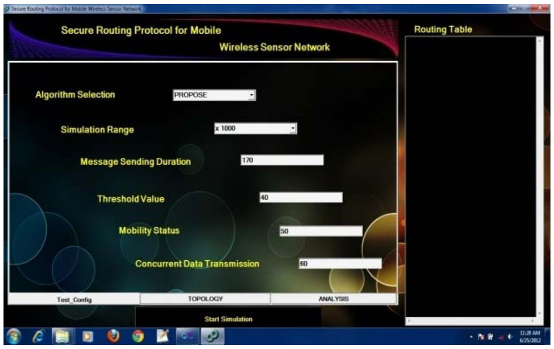
V. SECURITY STRENGTH ANALYSIS

In this section we analyze the security strength of the proposed routing protocol. The security of the proposed protocol comes from the unique way of using various secret keys for different communication types and also from the unique way that the protocol determines the route between a source node and the base station. The routes are determined by the base station instead of the sender nodes. The base station collects different location information of the sensor nodes and then on the basis of the role of a sensor node (i.e., Sensor node or Chief Cluster Head node) and the locations of other nodes the routes are determined by the base station and informed to the concerned sender nodes.

VI. SIMULATION RESULTS

In this section we present some simulation results regarding the performance of the proposed protocol. The simulator program is developed using Microsoft Visual Studio 2010. Microsoft Visual Studio is an integrated development environment (IDE) from Microsoft. It can be used to develop console and graphical user interface applications along with Windows Forms applications, web sites, web applications, and web services in both native code together with managed code for all platforms supported by Microsoft Windows, Windows Mobile, Windows CE, .NET Framework, .NET Compact Framework and Microsoft Silver light. The simulator is consisting of several modules such as deployment module, topology creation module, communication module, energy measurement module, exception handling module.

The performance of the proposed protocol is compared with that of LEACH [5]. We tune LEACH as per the proposal in [10] in order to support mobility in the WSN. We consider LEACH for comparison because it is one of the premier hierarchical and cluster based routing protocol for WSN. Though LEACH was not initially designed keeping mobile sensor nodes into consideration we tune LEACH in order to support mobility in the sensor nodes. The parameter we use for comparison is throughput. Throughput is the ratio of the total number of packets transmitted from within the network towards the base station during a specified period to the actual number of packets delivered at the base station against the same transmissions.



Algorithm Selection: PROPOSE

Simulation Range: x 1000

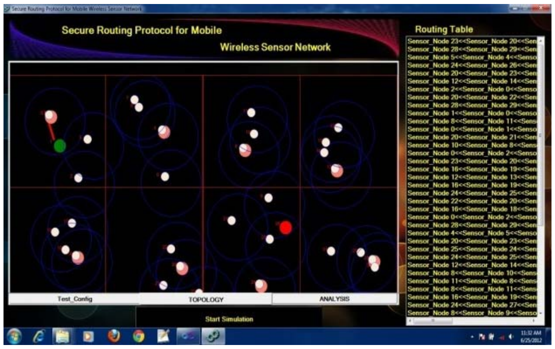
Message Sending Duration: 170

Threshold Value: 40

Mobility Status: 50

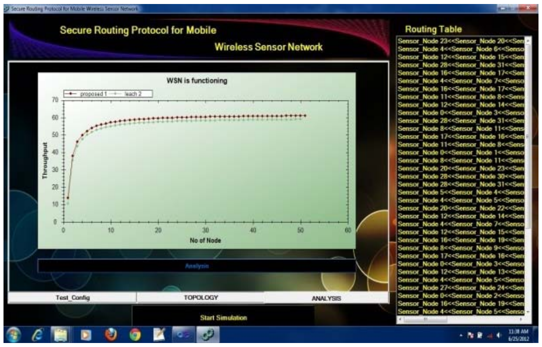
Concurrent Data Transmission: 60

Fig 1 WSN Topology Creation



```
Sensor_Node 23<<Sensor_Node 20<<Sen
Sensor_Node 28<<Sensor_Node 29<<Sen
Sensor_Node 5<<Sensor_Node 4<<Senso
Sensor_Node 24<<Sensor_Node 26<<Sen
Sensor_Node 20<<Sensor_Node 23<<Sen
Sensor_Node 12<<Sensor_Node 14<<Sen
Sensor_Node 2<<Sensor_Node 0<<Senso
Sensor_Node 20<<Sensor_Node 22<<Sen
Sensor_Node 28<<Sensor_Node 29<<Sen
Sensor_Node 1<<Sensor_Node 0<<Senso
Sensor_Node 8<<Sensor_Node 11<<Sens
Sensor_Node 0<<Sensor_Node 1<<Senso
Sensor_Node 20<<Sensor_Node 21<<Sen
Sensor_Node 10<<Sensor_Node 8<<Sens
Sensor_Node 0<<Sensor_Node 2<<Senso
Sensor_Node 23<<Sensor_Node 20<<Sen
Sensor_Node 16<<Sensor_Node 19<<Sen
Sensor_Node 12<<Sensor_Node 13<<Sen
Sensor_Node 16<<Sensor_Node 19<<Sen
Sensor_Node 24<<Sensor_Node 25<<Sen
Sensor_Node 22<<Sensor_Node 20<<Sen
Sensor_Node 16<<Sensor_Node 18<<Sen
Sensor_Node 0<<Sensor_Node 2<<Senso
Sensor_Node 28<<Sensor_Node 29<<Sen
Sensor_Node 4<<Sensor_Node 5<<Senso
Sensor_Node 20<<Sensor_Node 23<<Sen
Sensor_Node 25<<Sensor_Node 24<<Sen
Sensor_Node 24<<Sensor_Node 25<<Sen
Sensor_Node 12<<Sensor_Node 14<<Sen
Sensor_Node 8<<Sensor_Node 10<<Sens
Sensor_Node 11<<Sensor_Node 8<<Sens
Sensor_Node 8<<Sensor_Node 11<<Sens
Sensor_Node 16<<Sensor_Node 19<<Sen
Sensor_Node 24<<Sensor_Node 27<<Sen
Sensor_Node 8<<Sensor_Node 9<<Senso
```

Fig 2 WSN Communications between Nodes



```
Sensor_Node 23<<Sensor_Node 20<<Sen
Sensor_Node 4<<Sensor_Node 6<<Senso
Sensor_Node 12<<Sensor_Node 15<<Sen
Sensor_Node 28<<Sensor_Node 31<<Sen
Sensor_Node 16<<Sensor_Node 17<<Sen
Sensor_Node 4<<Sensor_Node 7<<Senso
Sensor_Node 16<<Sensor_Node 17<<Sen
Sensor_Node 11<<Sensor_Node 8<<Sens
Sensor_Node 12<<Sensor_Node 14<<Sen
Sensor_Node 0<<Sensor_Node 3<<Senso
Sensor_Node 28<<Sensor_Node 31<<Sen
Sensor_Node 8<<Sensor_Node 11<<Sens
Sensor_Node 17<<Sensor_Node 16<<Sen
Sensor_Node 11<<Sensor_Node 8<<Sens
Sensor_Node 0<<Sensor_Node 1<<Senso
Sensor_Node 8<<Sensor_Node 11<<Sens
Sensor_Node 20<<Sensor_Node 23<<Sen
Sensor_Node 28<<Sensor_Node 30<<Sen
Sensor_Node 28<<Sensor_Node 31<<Sen
Sensor_Node 5<<Sensor_Node 4<<Senso
Sensor_Node 4<<Sensor_Node 5<<Senso
Sensor_Node 20<<Sensor_Node 22<<Sen
Sensor_Node 12<<Sensor_Node 14<<Sen
Sensor_Node 4<<Sensor_Node 7<<Senso
Sensor_Node 12<<Sensor_Node 15<<Sen
Sensor_Node 16<<Sensor_Node 19<<Sen
Sensor_Node 8<<Sensor_Node 9<<Senso
Sensor_Node 17<<Sensor_Node 16<<Sen
Sensor_Node 0<<Sensor_Node 3<<Senso
Sensor_Node 12<<Sensor_Node 13<<Sen
Sensor_Node 4<<Sensor_Node 5<<Senso
Sensor_Node 27<<Sensor_Node 24<<Sen
Sensor_Node 0<<Sensor_Node 2<<Senso
Sensor_Node 16<<Sensor_Node 19<<Sen
Sensor_Node 4<<Sensor_Node 5<<Senso
```

Fig 3 Throughput comparison of the proposed protocol with the LEACH

VII. CONCLUSION

In this paper we present a novel secure routing protocol which is feasible to implement in the resource constrained sensor nodes. We consider moderate mobility of the sensor nodes as well as the base station. The proposed protocol is hierarchical and cluster based and it achieves security in the network layer through symmetric key cryptographic technique and principles of threshold key cryptography.

REFERENCES

[1] A.Perrig, R. Szewczyk, V. Wen, D. Culler, and J Tygar, “SPINS:Security protocols for sensor networks”, *Wireless Networks*, vol. 8, no. 5, 2002, pp. 521-534.

[2] Karlof C, Sastry N, Wagner D, “TinySec: A Link Layer Security Architecture for Wireless Sensor Networks”, in *Proc. of the 2nd Int’l Conf. on Embedded Networked Sensor Systems*, Baltimore, MD, USA, November 03-05, 2004, ACM Press, pp 162-175.

[3] A.D. Wood, Lei Fang, J A Stankovic, Tian He, “SIGF: A Family of Configurable, Secure Routing Protocols for Wireless Sensor Networks”, *Proc. of SASN*, October 2006, Virginia, USA.

[4] Zhen Cao, Jianbin Hu, Zhong Chen, Maoxing Xu, Xia Zhou, “FBSR: Feedback based Secure Routing Protocol for Wireless Sensor

Networks", J.*Pervasive Comput. & Comm.* Troubador Publishing Ltd, Vol. 1, No.1, pp 1-8.

[5] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan,"Energy Efficient Communication Protocol for Wireless Microsensor Networks", in *Proc. of the 33rd Annual Hawaii International Conference on System Sciences (HICSS)*, IEEE Computer Society, Maui, Jan. 2000, pp 3005-3014.

[6] W.B.Heinzelman, A.P. Chandrakasan, H.Balakrishnan, An application-specific protocol architecture for wireless microsensor networks, *IEEE Transactions on Wireless Communications*, vol.1, no.4, 2002, pp 660-670.

[7] Mohammad S. Al-Fares, Zhili Sun, Haitham Cruickshank, "A Hierarchical Routing Protocol for Survivability in Wireless Sensor Network (WSN)", in *Proc. of the International Multi Conference of Engineers and Computer Scientists (IMECS) 2009*, vol.1, Hong Kong, March 18-20, 2009.

[8] Hiren Kumar Deva Sarma et. al, "Energy Efficient Communication Protocol for Mobile Wireless Sensor Network System", *IJCSNS*, vol.9, no. 2, 2009, pp 386-394.

[9] William Stallings *Cryptography and Network Security Principles and Practices. Third Edition*, Pearson Education. ISBN 81-7808-902-5.

[10] Lan Tien Nguyen et al.,"An Energy Efficient Routing Scheme for Mobile Wireless Sensor Networks", in *Proc. of IEEE ISWCS 2008*, pp 568-572.