ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2019.0286

AUTONOMOUS GREEDY ROUTING IN WIRELESS SENSOR NETWORKS

N.V. Kousik[1], M. Sivaram[2] and S.Kalidass[3]
[1, 3]Department of Computing Science and Engineering, Galgotias University, India
[2]Department of Information Technology, Lebanese French University, Iraq

Abstract

Routing is challenging issue in WSN: Cryptography and key management schemes seem good, but they are too expensive in WSN. Prevention-based and detection based are the two approaches that are used in MANET. In prevention-based approaches a centralized key management is required, These applications require a good Quality of Service (QoS) from sensor networks, such as, minimum percentage of sensor coverage in the required area, continuous service during required time slot with minimum (or limited) resources (like sensor energy and channel bandwidth) and minimum outside intervention. The whole network may be affected if the infrastructure is destroyed. So this approach is used to prevent misbehavior, but not detect malicious based routes Detection based approaches are used to detect selfish node along with route that helps to identify malicious misbehavior route. Detection based approaches are based on trust in MANETs. Hence this approach is used to calculate the trust value in trust management schemes. The proposed scheme differentiates, routes, data packets and control packets, and also excludes the other causes that results in dropping packets, such as unreliable wireless connections and buffer overflows. The proposed scheme in a MANET routing protocol, evaluation of the AODV (Adhoc on demand on distance vector) and Low Energy Adaptive Clustering Hierarchy (LEACH) protocol with the NS2 simulator.

Keywords:

MANET, WSN, Routing, Quality of Service, AODV

1. INTRODUCTION

Most WSN trust based detection approaches cannot use both direct and indirect observations (neighboring node or a third party node information). No direct observation could evaluate the differentiation between the data, information and control packages. It is important that routes along with nodes which are credible to other nodes are identified without using centralized authorities to create a trust to enhance authentication. Not only does this mechanism help track detect, it will also enhance network performance. We use direct and indirect observations to evaluate the trust value. In this study, the calculation of the trust value means a credo which is a node that does what is anticipated.

Enriched trust management systems for the security of multi - hop wireline sensor networks are therefore used to improve the security [1] [3]. It is suggested that the route extension in WSN should be improved by means of a unified trust administration system. The efficient model of the autonomous confidence path has two elements in this scheme: confidence from direct observation and also indirect observation. The trust value is derived by a change in inference of Bayesian inference, a sort of uncertain reasoning, in which a complete probability model can be defined, by direct observation in observation in observer node.

The trust value is derived in indirect observation from neighboring nodes of the observer node, using Dempster - Shafer theory, another type of uncertain thinking where a proposal of interest may be derived in an indirect way [7].

In order to cover an area large numbers of sensor nodes are usually required. Nodes must therefore be cheap in order to make economic use of the network. Wireless sensors are designed for this purpose in small sizes, powered by a battery and limited memory. You can communicate in a small area because your radio range is small. WSNs are vulnerable to many security threats, as with any other broadcast - oriented wireless technology.

Moreover, they are frequently used in unattended, unreliable environments, where there is no physical safety. These restrictions have made it difficult to route safely in WSNs. Various attacks on the various layers of WSNs are applicable. The physical layer operation can be perturbed by hardware based attacks such as eavesdropping, interference, and jamming. Attacks to MAC layers cause selfish node misconduct and unfair bandwidth.

The attacks target network layer and routing protocols like selective forwarding, Sinkhole attack, Sybil attack, etc. Attacks like the SYN flooding, the hijacking of sessions, etc. lead to transport layer malfunctioning. Lastly, some of the possible attacks on application layers are viruses, worms, spywares etc. Both operating systems and user applications can be attacked. Numerous routing protocols for the continuous and emerging technology of wireless sensor networks were designed and implemented.

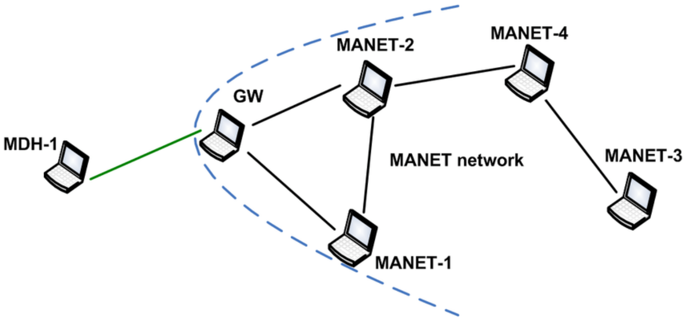

Fig.1. MANET Architecture

The main purpose of the proposed work is to overcome sensor node limitations and extend the network life. For large - scale and highly dynamic sensor networks, geographic routing based on the geographic location of the sensors is proposed. Lastly, some of the possible attacks on application layers are viruses, worms, spywares etc. Security not considered in the GPSR protocol design, therefore it is vulnerable to attacks like Sybil, Sinkhole, selective forwarding and many others. The proposed scheme in a MANET (Fig.1) routing protocol is evaluated against AODV and LEACH protocol in a NS-2 simulator.

2. RELATED WORKS

In [1] the cluster is organized and the heads of clusters are chosen. Each node decides whether it becomes a CH or not, regardless of other nodes. The basis of this decision is when the node last served as the cluster head; the node that is long time unchecked is likely to be chosen. In advertising phases the head sends the advertising packet to tell its vicinity that it is the head of the cluster. The advertising packet is selected based on received signal strength from non-cluster head nodes.

Anisur [1] developed a study on AODV routing, apply a route request (RREQ) message if a node wants to communicate with a non - neighbor node, this includes various key information such as the source, the target, the Sequence Number (Unique ID), etc.

In [6], the most difficult problem to date is the extension of the lifetime of the network to small battery capacity and autonomous operation is discussed. Attempts have been made to save energy at different frontiers from hardware improvements to medium access and routing protocols to networking and strategies that change roles. Furthermore, some authors have studied communication failures considered error detection.

In [3] enforces nodes to cooperate by using virtual currencies. The use of a tamper - resistant devices is unattractive despite its efficiency. Sprite also uses incentives to encourage co – operation between egoistic nodes. Sprite is generic because it relies on a central incentive authority and also does not address malicious nodes. The authors collect and combine the reputation of recommenders for the recommended node and path extension. The main disadvantage of the model is that the malicious nodes, regardless of their misbehaviors, are truly recommended. The Dempster Shafer Theory (DST) is a useful mechanism in uncertain thinking and is used extensively in expert systems and multifunctional systems.

In [2], the Dempster-Shafer theory is used in sensor fusion. The Dempster - Shafer theory applies to intrusion detection systems to evaluate non - reliable IDS sensor information. In this paper, we use uncertain artificial intelligence theory of reasoning to evaluate the confidence of the WSN nodes. Uncertainty is an ancient issue from the world of players. The probability theory can address this problem. Another significant behavior in daily life is reasoning. Uncertainty - based reasons for the development of the probability theory and symbolic logic were prosperous in the artificial intelligence community. The DST is a useful mechanism in uncertain thinking and is used extensively in expert systems and multifunctional systems. Intelligence systems that are used to deal with exceptions in the automatic reasoning have probabilistic reasoning introduced. In order to overcome the inconveniences of traditional rules based on tables of truth without exception, it is proposed to provide probabilistic reasoning which regards and describes the unsure knowledge as a subset of' potential worlds. Probabilistic thinking can be used in various fields, ranging from artificial intelligence to philosophy, cognitive psychological science and management. In the field of safety at WSN [10], we found that this theory is very appropriate for an assessment of trust based on the trust interpretation contained in this document. In uncertain reasons two approaches are Bayesian and the DST of evidence. The proposed system differentiates and excludes other causes that result in dropping packets such as non - reliable wireless links and buffer overflows, routes, data packets and control packets.

3. PROBLEM DEFINITION

First, sensor networks were motivated mainly by military applications but subsequently were considered in civil applications like environmental surveillance, health monitoring, etc [2]. Many factors, including tolerance to fault, scalability, costs of production, operating environment, sensor network topology, hardware constraints, transmission media, and electricity consumption, influence the design of a sensor network. To meet the performance, following design issues [5] [6] [7] of the sensor networks have to be measured.

3.1 SCALABILITY

A system that, when adding hardware, improve performance, is said to be a scalable system, proportional to its added capacity. This network can vary in hundreds, thousands or more of sensor nodes. This number of nodes must be used for the new schemes.

3.2 ROUTE DESIGN

In view of the original system routes and extension coverage routes proposed a route failure may be reinforced. The deployment is either deterministic or autonomous. The sensor knots are manually placed in deterministic situations and the transmission of data is carried out by default. The sensor nodes are randomly dispersed, creating an infrastructure in a wireless fashion in self-organizing conditions. Here, in terms of energy and performance, the position of sinks is also crucial.

4. ROUTING IN WSN

The definition and characteristics of WSN trust are described in this section. This explains, and sets out a framework for this proposed schemes, the trust model that is used to formulate an efficient autonomous route.

4.1 DEFINITION AND PROPERTIES OF ROUTE PATH

Confidence in the road has different meanings from psychology to business [9] in various disciplines. The WSN trust definition resembles the sociological explanation, in which trust is seen as grades in the belief that a node in a network (or an agent in a distributed system) performs tasks it should perform [9]. Because of the specific characteristics of WSN, WSN confidence has six fundamental characteristics: subjectivity, dynamics, non - transitivity, asymmetry, context dependence and extensibility [9]. Subjectivity means that the node is entitled to determine the confidence of an observed node. Different nodes in observers may have the same node's different trust values. Dynamicity means that, depending on your conduct, the confidence of a node must be changed. Non transitivity means that node A does not necessarily have the trust of node B and node B of node C of node C. In asymmetry, node B does not necessarily trust node A when trusts node B. Context dependence is defined as a confidence evaluation based on a node's behaviour. Various aspects of the actions can be assessed with a different confidence. For example, a node may not be able to send messages to its neighbors if it has less power. In this situation, power confidence in this node decreases, but because of its state, security confidence in this node will not be changed. Another important concept is reputation in the assessment of trust. The reputation reflects members of the community's public views [3]. In WSN, reputation can be a collection of confidence from network nodes. Extendibility means to discover a new route from the perspective of the whole network [3], reputation is more global than trust.

4.2 ROUTE EXTENSION MODEL

We evaluate trust for the proposed scheme by a real number between 0 and 1, based on the definition and properties of trust in WSNs. Although route reply acknowledgement may be found, then trust and confidence in contexts where trustees must take risk into account [5] can be different, trust and confidence worthiness is considered to be identical for simplicity in the scheme proposed. Trust consists of two components: a trust for direct observation and an indirect trust for observation. These are similar components to those of described in [6]. In a directional observation, an observer estimates his one-hop neighbor's confidence based on his own view. The trustee value is therefore the expectation that a trustee will use a subjective probability to decide whether a trustee is reliable or not. It is similar to the information defined in first hand [5].

5. PROPOSED SYSTEM

The AGR protocol is a routing protocol to discover the route when a data transfer between nodes is requested. Only with source nodes will the AGR search a new route. If a node asks for a route to a destination node, it starts a route discovery process and invades routes across network nodes. In comparison with AODV and LEACH among source and destination with track information for all the nodes, the protocol can greatly reduce the number of radio transmissions requested for routing search processes.

5.1 FRAMEWORK OF THE PROPOSED SCHEME

The context of the proposed scheme is developed on the basis of the Route Trust Model. The confidence assessment and update module can use two approaches: route mechanisms and update, for calculating and updating route values, in the trust system part of modules for direct and indirect observations [4]. The path be saved in the trust repository module. Networking components for routing schemes can set secure pathways between sources and destinations based on the trust repository module. Data can been sent via secure routing paths via the application element.

The confidence in this trust system can be established through a direct observation between an observer Node *A* and an observed Node *B*. Node 1 is an observer node and node 3 is an observation node in this example. Node 1 transmits node 5 data messages to node 3. Node 1 can overhear it when node 3 receives data messages and transfers it to node 5. Node 1. Then, based on data messages, can calculate the Node 3 route value. The same idea applies to the situation of the control message [7]. In the meantime, node 1, which has interactions with node 3 to assess the trust value of node 3, can collect Node 2 and Node 4. This data gathered from nodes of third parties is called indirect observation. Node 7 sends data messages, which is the target node, to node 3 in another situation. Node 1 in this situation cannot overhear information transmitted to node 3.

5.2 ROUTE PATH EVALUATION WITH DIRECT OBSERVATION

We evaluate route extension values based on the model presented in the last section, with direct observation on two malicious behaviours: packets dropping and packet modifying. In direct observation, each observer can overhear the packs forwarded by an observed node so that the observer can determine the malicious behavior of the observed node and compare them to the original packs.

$$E_n\left(\theta\right)=\frac{\alpha_n}{\alpha_n+\gamma\beta_n}+R_i \tag{1}$$

The factor of route path makes the trust evaluation more realistic. The route factor in the formula of trust evaluation in Eq.(1) are described as follows: where $\gamma \geq 1$. As the value of γ becomes larger, the Route path value declines more. This is because the punishment factor gives more weight to misbehavior. R_i and R_j are ideal path of route mechanism Based on this deduction, is defined as:

$$T^s = E_n\left(\Theta\right)+R_j \tag{2}$$

5.3 ROUTE PATH EVALUATION WITH INDIRECT OBSERVATION

A situation where a node is good for one node, but malicious for others may be alleviated. The Dempster-Shafer methodology, which is a mathematical theory of evidence, is applied in order to implement this method [8] because it is well developed to cope with insecurity or ignorance and provides a numerical measurement of degrees of belief about a proposal from multiple sources. The central theory is the belief function based on two essential ideas: a conviction of a proposition can be obtained from the subjective probabilities of a related question, which can be combined on condition that they are evidence of independence. In indirect remarks we assume that when the trust evaluation is performed using the route mechanism, there are more than one neighboring nodes between an observer and an observed node. Further, it is assumed that the proof is independent between different neighbors.

5.4 ROUTE EXTENSION CALCULATION WITH DIRECT OBSERVATION ALGORITHM

```
If the sensor node A is observer,
    Finds its route path
    The sensor node B receives the transmitting packet
Else
    The packets transmitted and received is increased by 1
    Case 1: Sensor node A finds that the sensor node B forwards
            the data packet.
            The total packets forwarded is increased by 1
Else if
    Case 2: If packet TTL = zero or buffer overflow in sensor node
            B
```

The total packets received are reduced by 1.

End

5.5 ROUTE CALCULATION WITH INDIRECT OBSERVATION WITH NODAL ALGORITHM

To find a route to a destination node, a source node floods a RREQ packet to the network. When neighbor nodes receive the RREQ packet, they update the Min-RE value and the TRE value and rebroadcast the packet to the next nodes until the packet arrives at a destination node. If the intermediate node receives a RREQ message, it increases the hop count by one and replaces the value of the Min-RE field with the minimum energy value of the route.

```
If sensor node A (observer) has more routing path than sensor node B then
    Calculate the optimal value of routes,
Else
    Set to original path
    Set to extension path
End if
```

5.6 ANALYSIS OF ROUTING PROTOCOLS WITH ALGORITHM

We consider three different routing protocols for operational comparison to understand the work of the proposed protocol:

Case 1: Select a minimum hop count route (AODV routing protocol) between source and destination, in comparison with AGR.

Case 2: Compare the LEACH routing protocol to the Autonomous Greedy routing route with a minimum residual route

Case 3: Select a route with the longest minimum route and lower hop count that is to say with the longest lifetime network (proposed protocol).

5.7 SPECIFYING AND EXECUTING

During the path construction phase our protocol is supposed to be executed. The following criteria are considered when the protocol is designed:

Step 1: The WSN is flat in structure and no nodes, except the base station that acts as the gateway, take on special roles.

Step 2: Node authentication steps should not be taken by the base station.

Step 3: Mobile sensor nodes and re-authentication may be necessary when the node's neighbors change.

Step 4: No information on keys in nodes, e.g. key indices must be revealed in the protocol.

Step 5: The in-network data processing of intermediate nodes should not be prevented from the protocol.

5.8 AUTHENTICATED ROUTING FOR GPSR WSN NETWORKS

- Authentication protocol analysis is not an easy task, and various methods for verification have been suggested. As for sensors, when we think about implementing authentication, a number of challenges arise.

  These are listed below.
- The speed and storage capacities of computing are limited and exclude the use of certain algorithms [12], for example asymmetrical, computationally intense cryptography which needs large keys to be stored.
- • There is no trusted server available, provided that the basic station is physically secured, for this role. This is a communication bottleneck in large sensor networks, in particular since the base station is already concerned about gathering data from the network.
- A WSN has no fixed infrastructure that can assign different roles to different nodes. WSNs look like Mobile Ad - hoc Networks (MANETs). In this sense.
- Nodes could fail, and the network might be replaced by new nodes. This function affects key administration. We must ensure, in other words, that new nodes can authenticate to old nodes.
- After initial deployment, the nodes' location can change (or new nodes can be added). In such cases, a node may need to authenticate itself in its transmission range repeatedly to new nodes.

A protocol of authentication is executed so that nodes can have "trust" in the identities of others. A trusted node can use its authorized resources in the network. In addition, if two nodes authenticate each other, they can agree on a fresh key *K* for future communication encryption. The key can also be used to calculate Message Codes (MACs) [11]. A MAC ensures a specific node, namely the node known to *K* has been created with a message m. It is also used to detect if during communication m has been manipulated.

6. SIMULATION PARAMETERS

The simulation set-up is as follows for evaluation. There are 6 permanent nodes in all simulations that represent the nodes of the commanders, 18 nodes as watchmen, and 2 patrol nodes that move along a predefined patrol path. In the area of responsibility there are 50-200 free movement nodes which represent regular soldiers. This range refers to the rate of penetration of communications technology, i.e. only part of the elements have communication equipment. The simulation takes the following cases into consideration:

- A single UDP application running on battalion nodes (source and destination).
- Multiple UDP applications running on commander nodes (two and three source and destination applications).
- A single 512-byte packet is sent to the head of the battalion every second by a commanding node. It takes 6000 seconds when the simulation ends. The simulation lasts. We then

note the performance in the following metrics of the routing protocol:

Delay: The time between packets from a source to their final destination. Delay: For completeness, this metric is to refer to timings for physical layer (i.e. not including processing times for MAC layers). The timekeeper starts when the packet is transmitted at the source by the transceiver and ends when the packet is received at its destination successfully.

Number of Hops: the length of the path to be passed by the packet. The simulation runs IO times for a specific number of free movement nodes and records the performance of the above-mentioned metrics. Since there is limited network traffic, a network segmentation or poor forwarding choices are expected to cause packet loss by routing protocol.

7. PERFORMANCE EVALUATION

Simulative evaluations evaluate the performance of the localization-based detection discussed in this paper, the location-based detections are presented for comparison with the original AODV and LEACH. It implements a location attack and performs a series of experiments to assess its efficacy in a network simulator. The Network Simulator NS-2 wireless network simulation software is finally used with small OS. The following parameters are compared and the delay is completed in this paper.

7.1 THROUGHPUT

The performance gives the ratio of transmitted number of packets to the number of received packets. Since our approach adds the data in the parent node and then sends it to the base station for some time, there is a higher output compared to the previous system, but no packet reached the sink. The Fig.2 showed AGR, LEACH and AODV as comparison performance. The result shows that the proposed method achieves higher throughput performance than other methods.

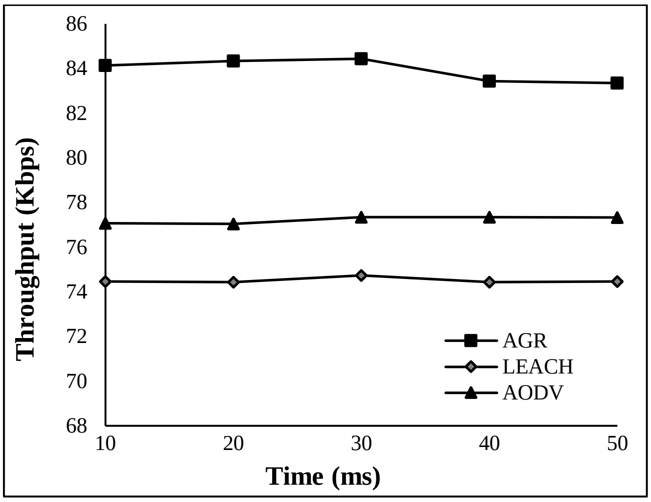

Fig.2. Comparison Throughput of AGR, LAR and AODV

7.2 END TO END DELAY

End-to-end delay is the average time that data packets are delivered to the destination node from the source node. If *n* nodes are in the network, the average delay is calculated by taking all packets as average. The end-to-end is also known as latency. The Comparison between AGR, LEACH and AODV is shown in Fig.3. The result shows that the proposed method achieves reduced delay than other methods.

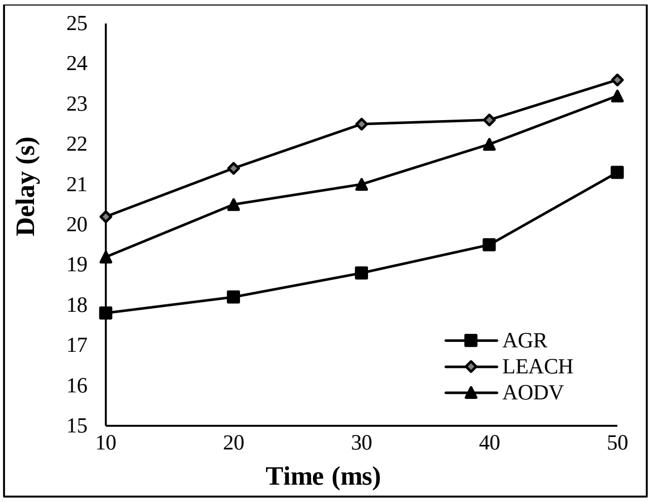

Fig.3. Comparison End to End delay of AGR, LEACH and AODV

8. CONCLUSIONS

Scalability is taken into account in performance measurement. The various inputs from autonomous greedy routing are analyzed. Efficient autonomous route (AGR) algorithm is proposed and improved and compared to AODV and LEACH. It states that new packet designs are considered for performance analysis that do not cover attacks and scalability advantages. For analysis the performance and end to end time are taken into account. In addition to maintaining routine abnormalities, route finds and projection range, AGR provided attack preservation and monitoring for malicious nodes. AGR is considering improving the scalability advantages of the simulation results. The AGR packet drop is compared with the AODV and LEACH.

REFERENCES

[1] M.A. Rahman, M.S. Islam and A. Talevski, “Performance Measurement of Various Routing Protocols in Ad-Hoc Network”, *Proceedings of International Multi Conference of Engineers and Computer Scientists*, pp. 18-20, 2009.

[2] R.P. Gupta, D.V.K. Sharma and V.M. Shrimal, “Investigation of Different Parameters of Dynamic Source Routing with varied Terrain Areas and Pause Time for Wireless Sensor Network”, *International Journal of Modern Engineering Research*, Vol. 1, No. 2, pp. 626-631, 2011.

[3] J.N. Al-Karaki and A.E. Kamal, “Routing Techniques in Wireless Sensor Networks: A Survey”, *IEEE Wireless Communications*, Vol. 11, No. 6, pp. 6-28, 2004.

[4] T. Van Dam and K. Langendoen, “An Adaptive Energy-Efficient MAC Protocol for Wireless Sensor Networks”, *Proceedings of 1st International Conference on Embedded Networked Sensor Systems*, pp. 171-180, 2003.

[5] Vijay Mohan Shrimal, Ravindra Prakash Gupta and Virendra Kumar Sharma, “Investigation of Adhoc Topology AODV for Wireless Sensor Networks for Varying Terrain

Areas for Different Speed (Node Speed)", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 2, No. 1, pp. 12-18, 2012.

[6] L. Breslau, D. Estrin, K. Fall, S. Floyd, J. Heidemann, A. Helmy and H. Yu, "Advances in network simulation", *Computer*, Vol. 33, No. 5, pp. 59-67, 2000.

[7] K. Fall and K. Varadhan, "The ns Manual (formerly ns Notes and Documentation)", Available at: https://www.isi.edu/nsnam/ns/doc/ns_doc.pdf.

[8] Imad Aad, Mohammad Hossein Manshaei and Jean Pierre Hubaux, "ns2 for the Impatient", Available at: http://www.manshaei.org/files/HoE-ns2-Mobnet09.pdf.

[9] A. Aziz, S. Rahayu, N.A. Endut, S. Abdullah, M. Daud and M. Norazman, "Performance Evaluation of AODV, DSR and DYMO Routing Protocol in MANET", *Scientific Research Journal*, Vol. 5, No. 2, pp. 49-65, 2008.

[10] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "Wireless Sensor Networks: A Survey", *Computer Networks*, Vol. 38, No. 4, pp. 393-422, 2002.