Secure routing protocol using cross-layer design and energy harvesting in wireless sensor networks

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 374796, 11 pages
http://dx.doi.org/10.1155/2013/374796

Research Article

Secure Routing Protocol Using Cross-Layer Design and Energy Harvesting in Wireless Sensor Networks

Nabil Ali Alrajeh,[1] Shafiullah Khan,[2] Jaime Lloret,[3] and Jonathan Loo[4]

[1] *Biomedical Technology Department, College of Applied Medical Sciences, King Saud University, Riyadh 11633, Saudi Arabia*
[2] *Institute of Information Technology, Kohat University of Science and Technology (KUST), Kohat City 26000, Pakistan*
[3] *Department of Communications, Universidad Politecnica de Valencia, Camino de Vera 46022, Valencia, Spain*
[4] *School of Engineering and Information Sciences, Middlesex University, London NW4 4BT, UK*

Correspondence should be addressed to Nabil Ali Alrajeh; nabil@ksu.edu.sa

Received 28 November 2012; Accepted 23 December 2012

Academic Editor: Shuai Li

Energy efficiency is the main concern of research community while designing routing protocols for wireless sensor networks (WSNs). This concern can be addressed by using energy-harvesting scheme in routing protocols. In this paper, we propose a secure routing protocol that is based on cross layer design and energy-harvesting mechanism. It uses a distributed cluster-based security mechanism. In the cross-layer design, parameters are exchanged between different layers to ensure efficient use of energy. Energy-harvesting system is used to extract and store energy, which is used to take decisions for the node state and thus for the routing issues. Simulation results show that our routing protocol can perform better in many scenarios and in hostile attack-prone environment.

1. Introduction

WSN is typically used to monitor environmental or geographical location for some specific purpose. WSN consists of sensor nodes that have the capability of self-configuration and its deployment in target area is so easy. WSNs have some limitations in terms of battery power, data rates, memory, and processing.

Energy efficiency is one of the most important factors in designing a WSN. As WSN is deployed in many hostile and extreme environments, it is not possible to supply energy source or recharging facility. The entire network has to perform its task on the embedded batteries. If some nodes died due to low battery power, it may result in the breakdown of entire network termed as network partitioning [1], so one of the main purposes is to enlarge the WSN lifetime [2]. Built-in power technologies such as batteries are consistently improving [3], and there are many power saving and energy saving techniques for WSNs [4]. However, most of WSNs are deployed in harsh environments in which there is a need of environmental energy harvesting. Energy harvesting is a mechanism in which sensor nodes have the ability to extract energy from environment, store it, and then use it whenever needed. In WSN more energy is used in data transmission from source to multihop away destination. This is the reason; energy-efficient routing is always desirable in such kind of networks [5]. Energy efficiency can be achieved by utilizing clustering mechanism in WSN. Clustering is a technique in which many sensor nodes are grouped together to perform a task. Cluster head is responsible for monitoring all the nodes in its own cluster. In cluster-based WSN, routing mechanism is more simple and easy as compared to noncluster WSN. Cluster head facilitates the routing protocol to reliably send data from source to destination. On the other hand, routing protocol is responsible for finding optimal route from source to destination. In classical OSI model, all the layers operate independently. In such case, routing protocol would select a path regardless of physical layer (battery power) and MAC layer (data rates) requirements. Networks having energy or bandwidth limitations must interact with upper layers

for selecting energy-efficient path. This kind of interaction between different layers is only possible using cross-layer technique.

The idea behind cross-layer information exchange [6, 7] is to optimize network usage and resources by communicating different layers. Cross-layer optimization technique can be used to make intelligent decisions about power saving, QoS routing, enhanced scheduling, and bandwidth allocation algorithms in multihop networks. The important fact of using cross-layer design is to exchange multiple parameters across the protocol stack to increase network performance and efficiency of network resources. Network resources in WSN can be threatened by many security attacks such as sleep deprivation attack, packet dropping attack, or collecting sensitive information [1, 8–10]. The attacker conducts sleep deprivation attack at physical layer while packet dropping attack at network layer. Such kind of multilayered security attacks cannot be prevented by using a security mechanism at single layer. To counter multilayer security attacks, again cross-layer security mechanism is highly desirable for detecting and responding to different attacks at different layers. One possible solution can be cross-layer secure routing.

Secure routing is highly desirable for multihop wireless networks such as WSN. Multihop wireless networks are more vulnerable to security attacks as compared to single-hop wireless networks. The reason is that most of multihop wireless networks are distributed having no centralized body. Designing an appropriate secure routing protocol for WSN is a challenging task. In WSN the ideal routing protocol should be secure and efficient in terms of energy consumption.

In this paper, we present a secure routing protocol which is based on cross-layer information exchange and energy-harvesting technique.

Our proposal is capable to consistently monitor the energy consumption and select secure and energy-efficient path from source to destination.

The rest of the paper is organized as follows. Section 2 discusses related work. Protocol design considerations and parameters are covered in Section 3. Section 4 describes the evaluation and simulation results. Section 5 concludes the paper and provides our future work.

2. Related Work

WSN has many applications such as wide area surveillance for borders security, monitoring heat, sound, and pressure in a given area [11]. Routing packets from source to destination is one of the important operations in WSN. Many Routing protocols have been proposed in the literature [12–16]. Most of these protocols are either application specific or lacking security mechanism. Research community is paying special attention to propose various security mechanisms for WSN [17–20]. Most of these security mechanisms operate and counter specific security threat. Many secure routing protocols are developed for WSN as mentioned in [21–24], which are used to address particular security concern. Furthermore, most of these proposed routing protocols are based on key management schemes to encrypt the data. Although key management scheme is efficient to protect data confidentiality, it cannot prevent data dropping or packet misdirecting kind of attacks [8]. It is also important to mention that most of these existing secure routing protocols operate without taking energy into consideration. Some researchers proposed energy-aware routing protocols for WSN [25–27]. However, most of these energy-aware routing protocols lack security mechanism. Furthermore, these proposed mechanisms have no concept of energy-harvesting mechanism in WSN.

It is important to consider energy limitations while designing any mechanism for WSN. Majority of current energy-aware routing protocols determine efficient use of energy. Such mechanisms may increase the life time of WSN, but do not offer harvesting of environmental energy to provide durable solution.

Research community is now seriously considering such mechanisms for WSN, in which environmental energy is harvested and stored so that to provide a durable source of more energy to sensor nodes especially for those sensor networks which are deployed for long-term activities. Many routing protocols have been proposed so far which are based on the concept of energy harvesting in WSN. Low latency geographic routing using energy harvesting is proposed for WSN [28]. This proposal estimates the energy consumption and the expected energy from harvesting device. The authors made a claim about reliable data delivery with low latency. However, this scheme cannot ensure reliable data delivery in case of security attack or malicious activity in WSN.

Another beaconless geographic routing based on energy-harvesting technique is proposed for WSN [29]. The main idea of this proposal is same as presented in [28] except that its nodes send data packets first instead of control packet and the nodes have no prior information of neighbors. This proposal also harvests energy from harvesting device. However, the performance is yet not known in case of mobility, multimedia traffic, and large network size. Furthermore, security concerns are not addressed in this proposal.

Adaptive opportunistic routing based on energy harvesting technique is proposed in [30]. This proposal considers grouping of nodes and estimating distance of nodes from sink. In this work, the authors assume that all the nodes have energy harvesting capability.

In [31], a routing protocol is proposed on the basis of energy transfer mechanism using electromagnetic waves. Another routing protocol based on the concept of energy harvesting is proposed in [32] for environmental monitoring of sustainable WSN. In this work, the authors equipped WSN networks with two types of node, that is, battery-power-driven nodes and energy-harvesting-driven nodes. Two types of routing are proposed for these two categories of nodes. Authors in [33] proposed a novel mechanism for transmission power control based on energy level and harvesting technique. The authors claim that the problem of unbalanced energy consumption is solved by using unbalanced energy capability. Routing protocol with hybrid energy storage system is proposed [34] to extend the network lifetime with a new cost metric. Another harvesting-aware mechanism [35] is designed for sustainable mobile sensor nodes. In this mechanism, mobile sensor nodes move to energy station

for recharging if the energy is found below threshold value. However, this mechanism is not suitable for static WSN. A detailed work is done on opportunistic routing based on ambient energy harvesting [36]. In this proposal, nodes are grouped together to improve throughput and minimize delay.

3. Proposed Routing Scheme

Data transmission from source to destination node requires some sort of routing mechanism. Typical WSN nodes sense information and forward to sink node over multi-hop intermediate nodes using routing protocol. The objective behind this work is to transmit packets along such path, which is reliable and energy efficient. We assume that each WSN node is equipped with energy harvesting system. It is capable to harvest environmental energy and convert it into electrical energy. The proposed mechanism consists of four important modules as given in Figure 1.

(i) The proposed mechanism is cluster based in which when WSN is deployed for any application, nodes form two-hop cluster for coordination. In cluster-based WSN, the optimal cluster size is two hop as presented in [37].

(ii) Energy consumption can be reduced when nodes only communicate with cluster head. So our energy model is cluster-based WSN.

(iii) Proposed mechanism is cross-layer in nature so that it can get energy parameters at network layer using cross-layer interface.

(iv) The mechanism is secure in nature especially against variety of active and passive attacks.

3.1. Cluster Formation. The first step consists of cluster formations. There are many clustering schemes [38], but we have used the following one. In the start of the network deployment, all the nodes are assumed to have equal battery power. Initially, each node broadcasts a neighbor-discovery message. All nodes in their coverage area will reply with a neighbor-discovery ack message. Thus, network links and topology are built. Then, interested cluster head nodes send a *cluster-invitation* message to all one-hop and two-hop neighbors in order to become its cluster members. One- and two-hop neighbors respond back with cluster-joining message. In cluster-joining message, the node enables hop-count field, so that when cluster head receives cluster-joining message, it can confirm that the distance of the joining member is not more than two hops. Interested cluster head nodes may be defined in advance or selected randomly by the system based on their position. Described message flow system is shown in Figure 2.

We assume that cluster head is aware of its position with respect to sink node. Such location information can be obtained using global positioning system or using built-in configuration.

3.2. Energy Model. WSN is deployed in such areas where wired network is not feasible to maintain and configure. WSN

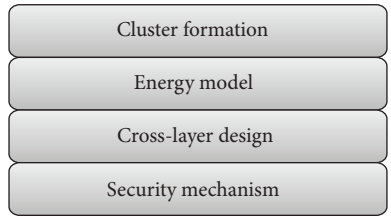

Figure 1: Modules of proposed routing mechanism.

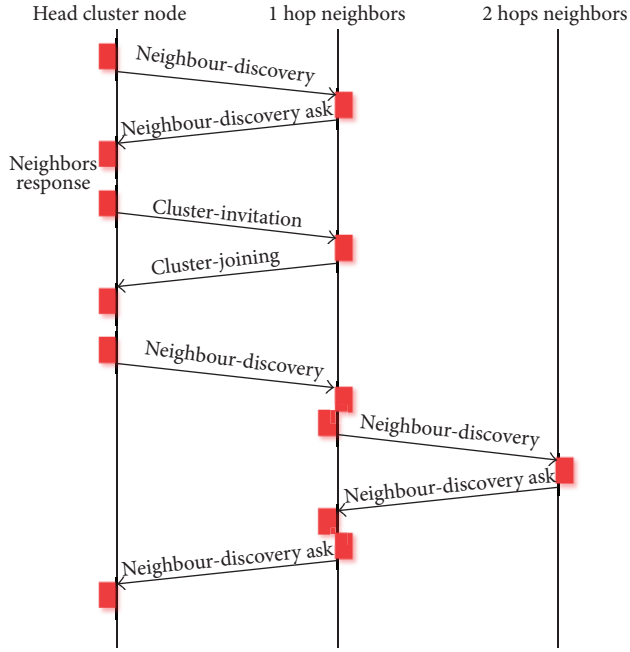

Figure 2: Message flow for cluster formation.

is used to sense information, analyzes them, and transmits to base station. WSN nodes have built-in batteries which determine the network lifetime. The battery life of nodes in WSN depends on the location and other environmental factors. A node that is located in the center of WSN has less battery life as compared to those nodes which are located at edges, because the centre nodes not only collect information around its own field but also forward data for others as well towards the base station. It is not possible to replace or recharge batteries of dying nodes. There is a need for a constant power source for WSN nodes especially for sustainable WSN. Energy harvesting is a promising technique in which sensor nodes are empowered to extract energy from environment, store it, and later on use it for performing different tasks.

Some important sources of energy harvesting are mentioned in [39–41], which are summarized below.

(i) Mechanical vibration is used to create movement which is later on converted to electrical energy using piezoelectric, electrostatic or electromagnetic schemes.

(ii) Photovoltaic cells are used to convert sun light energy into electric energy.

Some other sources of energy are radio frequency (RF) radiation and thermal energy [42]. In RF scheme, high power electromagnetic waves are directed towards sensor nodes from nearby source. In thermal energy-harvesting schemes, sensor nodes have the capability to convert heat energy to electric energy. More investigation is needed to explore all possible merits and demerits of these energy sources especially factors like environmental pollution. Furthermore, some energy harvesting schemes may perform well in one scenario but may not in other. For example, usage of photo cells to harvest solar energy may perform well in those WSN applications where nodes have more exposure to sunlight. Some other challenges are mentioned in [43] such as energy harvesting hardware and software overheads. Enabling energy harvesting in sensor nodes demands specialized hardware to harvest and store energy. Furthermore, specific software is needed to control and manage harvested energy. Such specialized demand of software and hardware will definitely increase the overall cost of WSN deployment. From the literature survey, it is observed that less attention is given to security mechanisms in WSN having energy-harvesting mechanism. Any new mechanism for WSN must consider that as WSNs are deployed in harsh areas, so only battery power may not be sufficient for medium and long-term monitoring. It is indeed necessary to harvest environmental energy so that to provide constant and durable source of energy to all nodes.

In the proposed mechanism, the energy model is considered in next step. We are considering sunlight as the source for harvesting in WSN. For perpetual operation, a duty cycle and energy harvesting mechanism using a mathematical model is present in [44]. Using this equation, we can get the power output from energy source and energy harvested. The proposed equations in [44] also estimate power consumption of a node during specific interval of time. We defined three energy ranges for every sensor node. These three energy ranges define three states of sensor node. The three states are *active state, semiactive state,* and *idle state*. The three states and their characteristics are listed in Table 1.

In active state, WSN node is actively participating in WSN operations, that is, as soon as it sense, or receives any packet, it is immediately routed to cluster head. In active state, node does not harvest environmental energy. A node remains in active state as far as its energy is greater than X. In semiactive state, node starts harvesting environmental energy. A node remains in semiactive state as far as its energy (Y) is in between X and Z.

In semiactive state, a node does not actively participate in WSN operation. It collects and stores packets and later on sends to cluster head. In semiactive state, when node is in the process of harvesting energy, it collects and stores packets. After some time, it stops harvesting process and sends a bulk of packets to cluster head and again starts harvesting energy. It is a kind of sleep and wake state. In sleep state, it only harvests energy and collects packets. When in wake state, it forwards packets to cluster head and stop energy-harvesting process.

Table 1: The energy related states of WSN node.

State	Energy range	Energy harvesting
Active	Above X	No
Semi active	Y	Yes
Idle	Below Z	Yes

In idle state, a node does not perform any operation, only harvest environmental energy. A node remains in idle state as far as its energy is below Z.

In idle state, node calculates its harvested energy after interval of time. If the energy value is greater than "X," then it switches to active state. If the harvested energy is still below "Z," it remains in idle state or otherwise switchs to semiactive state.

Given $E(\mathrm{AR})$ as the energy in active range and $E(\mathrm{SAR})$ as energy in semiactive range, the algorithm for the three states of sensor node is given in Figure 3.

Along a node lifetime, it will be in any of these three states. Now we can define t_a as the amount of time that has been in active mode, t_s as the amount of time that has been in semiactive mode, and t_i as the amount of time that has been in idle range. The node lifetime T can be expressed by

$$T = t_a + t_s + t_i. \tag{1}$$

Now, we can estimate the energy consumed along the node lifetime. It is given by the following expression:

$$E(t) = E(\mathrm{AR}) \cdot t_a + E(\mathrm{SAR}) \cdot t_s + E(\mathrm{IR}) \cdot t_i. \tag{2}$$

$E(\mathrm{AR})$ varies according the number of packets to transmit, packets to receive, acknowledgements to transmit, acknowledgements to receive, and the number of retransmissions during t_a time. Bearing in mind that in a wireless link there is a packet retransmission probability (P_s), because there can be lost or error packets, $E(\mathrm{AR})$ can be given by the following expression:

$$E(\mathrm{AR}) = \left(1 + P_s\right) \cdot \left(E_{\mathrm{TX}} + E_{\mathrm{RX}} + E_{\mathrm{TX\_ACK}} + E_{\mathrm{RX\_ACK}}\right), \tag{3}$$

where E_{TX} is the energy consumed because of the transmitted packets, E_{RX} is the energy consumed because of the received packets, $E_{\mathrm{TX\_ACK}}$ is the energy consumed because of the transmitted acknowledgement packets, and $E_{\mathrm{RX\_ACK}}$ is the energy consumed because of the received acknowledgement packets. If we take into account the following parameters and the energy model for wireless sensor nodes provided in [45], we obtain (4) to estimate $E(\mathrm{AR})$ in free space:

(i) number of packets to be transmitted (n_t),

(ii) average number of bits of each transmitted packet (x_t),

(iii) average number of acknowledgements transmitted for a packet (n_{at}),

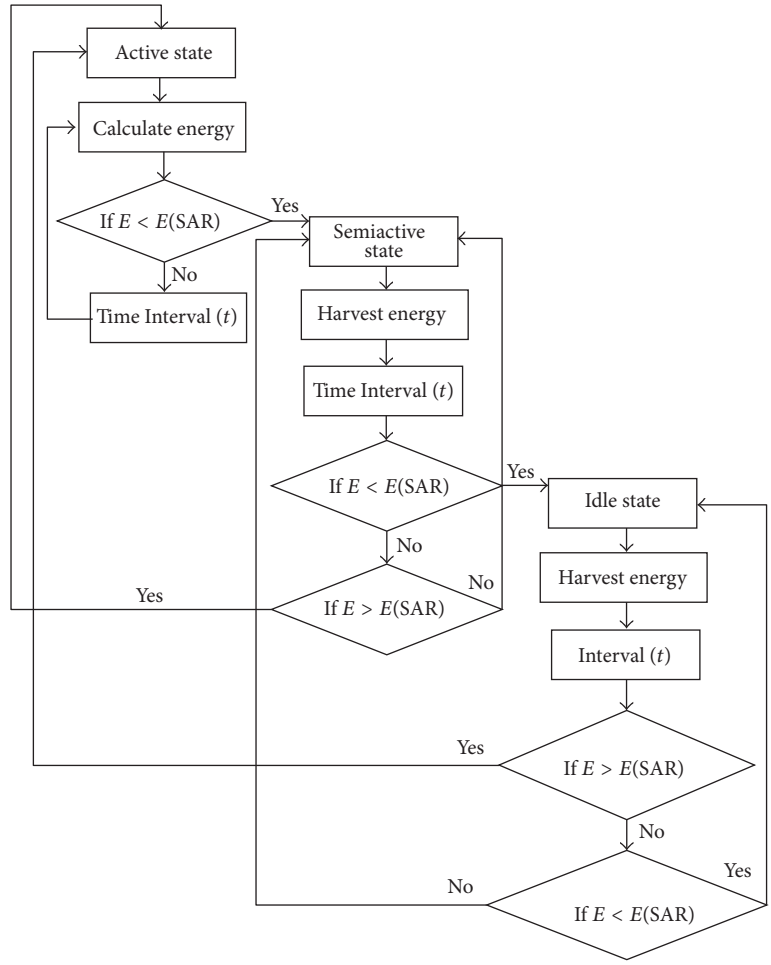

Figure 3: Algorithm for the three states of sensor node.

(iv) average number of bits of each transmitted acknowledgement packet (x_{at}),

(v) number of packets to be received (n_r),

(vi) average number of bits of each received packet (x_r),

(vii) average number of acknowledgements received for a packet (n_{ar}),

(viii) average number of bits of each received acknowledgement packet (x_{ar})

$$E(\text{AR}) = \left(1 + P_s\right) \cdot \left(E_{\text{elec}} \cdot \left(n_t \cdot x_{tr} + n_r \cdot x_{tr} + n_{\text{atr}} \cdot x_{\text{atr}} + n_{\text{atr}} \cdot x_{\text{atr}}\right) + \varepsilon_{\text{amp}} \cdot d^2 \cdot \left(n_t \cdot x_{tr} + n_{\text{atr}} \cdot x_{\text{atr}}\right)\right). \quad (4)$$

We have assumed that generally $x_t = x_r$ (we will call it x_{tr}), $x_{\text{at}} = x_{\text{ar}}$ (we will call it x_{atr}), and $n_{\text{at}} = n_{\text{ar}}$ (we will call it n_{atr}).

When any node switches to idle state, it informs its neighbors. In return, neighbor nodes start routing packets through another route.

For energy-efficient routing, all the member nodes of cluster periodically exchange route energy packets (REP). In REP, nodes communicate energy value. A node always selects that path in which the neighbors have more energy. For example, node A has three one-hop neighbors K, L, and M. Now A will select that neighbor which has more energy.

3.3. Cross-Layer Design. Interaction amongst parameters across the protocol stack is performed using methodology of cross-layer design. In proposed mechanism, the interaction between physical layer and network layer is possible due to this methodology.

REP is generated using cross-layer design. Energy is physical layer scheme, while routing is the mechanism of network layer. To bring current energy value of a node in routing packet is only possible using cross-layer design. In cross-layer design, energy value is first captured at application layer and then inserted to network packet using cross-layer interface [9]. This selection of energy efficient route helps semiactive nodes to harvest more energy and to participate less in WSN operations so that they become active soon. This kind of intelligent routing is possible with cross-layer design.

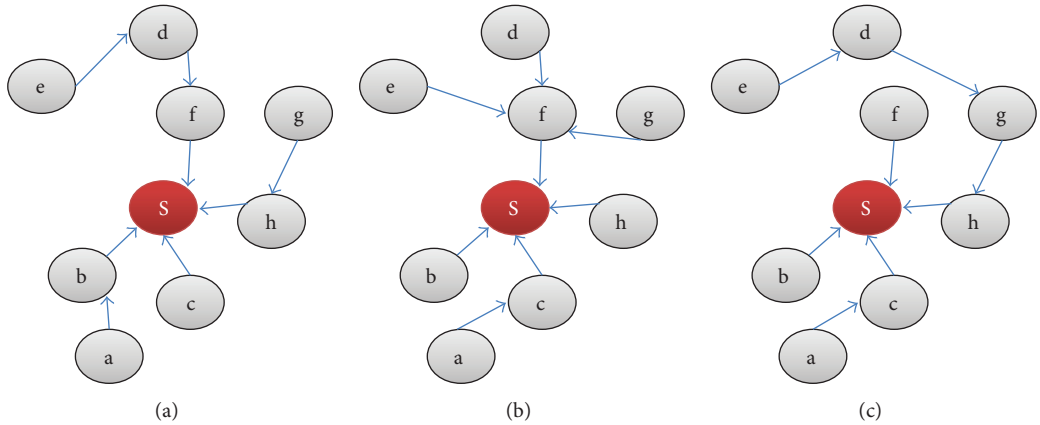

Figure 4: Energy-efficient route selection.

The energy-efficient route selection process is given in Figure 4.

In Figure 4(a), "S" is a cluster head forming a two-hop cluster of many nodes. Initially all the nodes are in active state and as soon as any node gathers some information, it transfers that information immediately to cluster head for further processing. As in active state, environmental energy is not harvested so that all the nodes are using battery power. In WSN, those nodes which are in center or having many neighbors are supposed to consume more energy as they not only gather information and transmit to cluster head but also relay data for all other neighbors. In Figure 4(a), node "b" is not only forwarding its own data to "S," but also relaying data for "a" as well. So "b" energy consumption is more as compared to "a." Here "b" cannot remain in active state for long time. When "b" energy falls in semiactive range, it will switch to semiactive state. Here "a" has an alternate path to start routing data through node "c" as shown in Figure 4(b).

Node "b" will start energy harvesting and will remain in semiactive state. Let suppose node "c" is not there and node "a" has no alternate path. In such case, node "a" will still forward data to node "b" and node "b" will relay data for node "a" after some interval of time. As in semiactive state, node "b" will harvest environmental energy for some time and will forward collected data to cluster head for some time. Let suppose node "b" is in idle state and node "a" has no alternate route to cluster head. In that case, node "a" will collect information and has to wait till it receives a control packet from node "b" about its active or semiactive state.

From Figure 4(a), suppose node "b," "h," and "d" are under heavy traffic load. After some time, these three nodes switch to semiactive state. Their neighbors will start data relaying through other alternate routes as given in Figure 4(b). In this figure, node "a" is now routing data through node "c," node "e" is communicating with cluster head through node "f", while node "g" is relaying data through "f." However, now node "f" is relaying packets for many nodes. Suppose, node "f" switches to semiactive state, then the nodes will reorganize themselves to alternate paths as shown in Figure 4(c).

As nodes periodically communicate REP packet, so all the nodes are informed of neighbors current state. When a neighbor receives REP packet and the energy value in REP packet is in semiactive or idle range, the corresponding neighbors start searching for alternate routes. This kind of mechanism ensures energy-efficient routing in cluster-based sustainable WSN. However, there is a need of some kind of security scheme to ensure reliable data forwarding,

3.4. Security Mechanism. Most of WSNs are used to sense, collect, and process sensitive information. Data confidentiality and integrity is one of the important objectives in such cases. This kind of objective can be achieved by designing some sort of security mechanism especially enabling security mechanism in routing protocol. Important requirement of any network is to ensure confidentiality, integrity, and availability [1, 8, 10]. Confidentiality ensures the secrecy of data sent from source to destination. Integrity makes sure that the destination received data in correct format and sequence without any alteration. Availability means that all the nodes and network devices are operating in harmonious mode and the network resources are available all the time. The attacker uses active or passive attacks to violate either confidentiality of sensitive data or integrity of transmitted data by altering the real information

Different kinds of active and passive attacks can bring serious disruption in overall performance of WSN. Passive attacks [10] do not harm the network or network resources; however, these attacks collect, analyze, and decode sensitive information. Active attacks [1] have the capability to drop or misdirect routing packets. To counter passive attacks and to ensure secrecy and confidentiality of data, we are using similar kind of mechanism as used in [46]. To counter packet dropping or misdirecting kinds of active attacks, we modified a bit the security mechanism proposed in [9]. The security mechanism proposed in [9] sends passive acknowledgement for every successful delivery of packet. For example, if a source node sends 100 packets to destination node through intermediate node(s), the destination node sends back 100

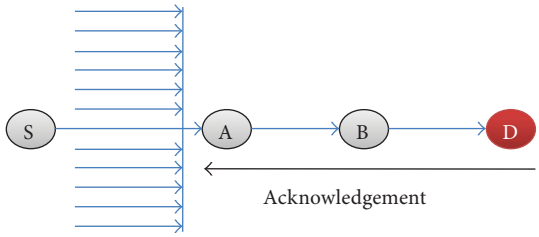

Figure 5: Proposed security mechanism.

passive acknowledgements to source node for every packet arrived. Keeping in view the limited resources and bandwidth, in WSN we cannot use this kind of heavy mechanism. The reason is that, such mechanism will greatly increase routing overheads and could create congestion. In our case, a packet counter is introduced at every node including cluster head. Suppose in Figure 4(a), node "e" forwards 300 packets to cluster head. When cluster head will not receive any further packets from node "e" till fixed interval of time, it will assume that node "e" has no more packets to send. The cluster head will send a packet count of 300 to node "e," which means that cluster head successfully received 300 packets. When node "e" receives packet count from cluster head which matches to its own packet count, it means node "d" is not malicious and all the packets are successfully relayed through node "d." Our mechanism is per session basis contrary to the per packet bases mechanism proposed in [9].

The proposed security model can counter many kinds of active attacks such as blackhole, greyhole, and wormhole [1, 8, 9]. Blackhole is a compromised node and if it is located as intermediate node between source and destination, it is used to drop all the packets passing through it. Greyhole is a less harsh version of blackhole attack. Greyhole is such a malicious node, which is used to selectively drop packets passing through it. Wormhole is basically packet misdirecting attack, in which the attacker establishes a wormhole link between two malicious nodes. The wormhole link is established using fast medium such as fiber optic. One malicious node captures packets at one end and tunnel them through wormhole link to other malicious node. The objective of this attack is to create routing overheads and congestion in network. Our security mechanism is further explained in Figure 5

In Figure 5, "S" is a source node, while "D" is cluster head acting as destination node. Node "A" and "B" are intermediate nodes which relay packets for "S" towards "D." Let us suppose, node "A" is malicious and acting as greyhole. Node "S" sent 12 packets to "A." Node "A" dropped 4 packets. Node "D" received only 8 packets. At the end of the transmission, node "D" sent an acknowledgement to "S" that 8 packets are received successfully. At this stage, node "S" assumes that the next node is malicious and dropping the packets. Now, node "S" starts searching an alternate route to node "D."

Similarly, if node "A" is acting as blackhole or greyhole, the acknowledgement at the end of the session can easily detect such packet dropping or packet misdirecting kind of malicious activities.

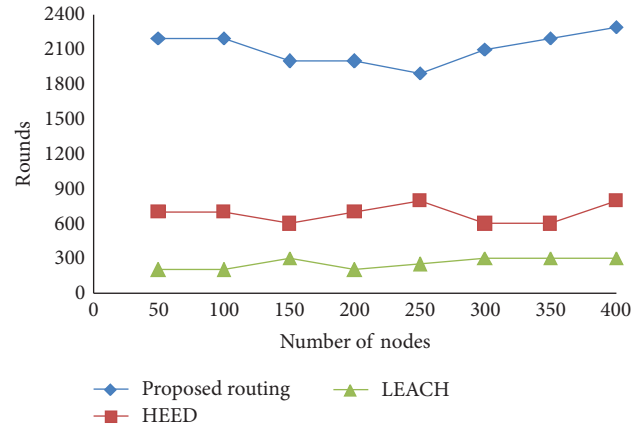

Figure 6: Network life time based on number of rounds.

On the other hand, the mechanism proposed in [9] uses every next hop passive acknowledgement. For example, node "B" sends passive acknowledgment to node "S" for every packet received. Similarly node "D" sends passive acknowledgement to node "A" for every packet received.

4. Performance Evaluation

The performance of secure routing protocol based on cross-layer design and energy harvesting technique is simulated using realistic scenarios. We simulated a WSN having 200 nodes capable of harvesting environmental energy using NS-2. These nodes are randomly deployed at 100 m × 100 m. Each data packet is of 200 bytes, while PER packet size is 40 bytes. We compared our routing mechanism with low energy adaptive clustering hierarchy (LEACH) and hybrid energy-efficient distributed (HEED) cluster-based routing protocol. Figure 6 shows the network lifetime comparison of three routing protocols based on number of rounds.

The performance of the proposed protocol is better as compared to LEACH and HEED.

The reason is that the proposed routing scheme selects energy efficient path to cluster head; furthermore, environmental energy-harvesting mechanism can create great difference in network lifetime.

In Figure 7, the remaining network energy is presented with respect to number of rounds. The total number of nodes is 400 and the network remaining energy is computed for 80 rounds. It is observed that the proposed routing mechanism is better than the rest of two. This difference is again created by the usage of energy harvesting mechanism. The proposed routing scheme is capable to balance the energy usage and harvesting. HEED performance is also satisfactory till the end of 40 rounds. The reason is that HEED is also energy-efficient routing mechanism. However, after 40 rounds, HEED gradually decreases energy value as it has no support of energy harvesting. On the other hand, LEACH performance shows gradual degradation as soon as the number of rounds increases. The reason is that LEACH is not energy efficient in nature.

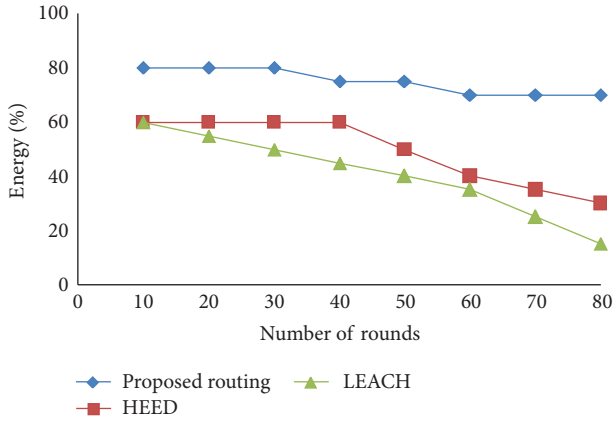

Figure 7: Remaining network energy.

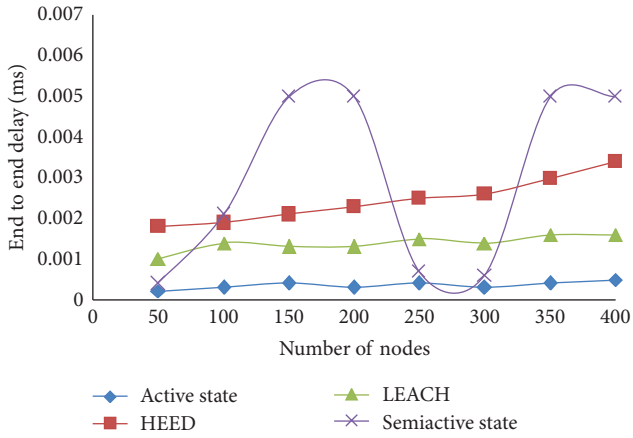

Figure 8: End to end delay.

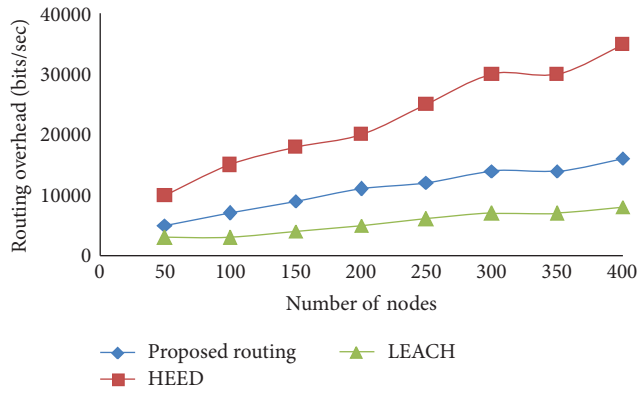

Figure 9: Routing overhead comparison.

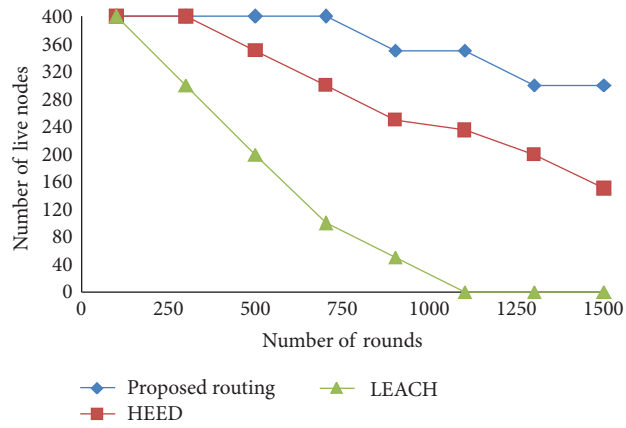

Figure 10: Number of live nodes in increased traffic scenario.

In Figure 8, end to end delay is presented, which shows some interesting results. When the proposed mechanism is in active states, it shows lowest end to end delay from source to cluster head. This is because, the proposed mechanism follows such a path which is rich in energy. However, the proposed scheme shows more end to end delay if some of its nodes are in semi-active state. The reason is that, if a node(s) is in semiactive state, it harvests energy for some time. During energy harvesting period, nodes do not forward packets or take part in communication. In this case, a neighbor has only one route to cluster head through the node in semiactive state. The node has to wait for its neighbor to harvest energy for some time and then forwards its packets through it to cluster head.

Figure 9, compares routing overheads of all three routing protocols with 400 nodes. The proposed routing scheme has more routing overheads as compared to LEACH. It is due to periodic exchange of REP packets to inform the neighbors about energy value.

Figure 10 shows a number of live nodes with respect to rounds in a network of 400 nodes. This simulation result is obtained with increased traffic from sensor nodes to destination. It is observed, that even after 1500 rounds, the number of live nodes in proposed mechanism is more than 300, whereas great performance degradation is seen in LEACH just after 200 rounds.

In Figure 11, a malicious node is introduced to observe the packet loss ratio of all the routing protocols. The malicious node is acting as a greyhole [8]. Greyhole node selectively drops packets which it receives from neighbors. We selected greyhole attack as it represents an entire class of packet dropping and packet misdirecting attacks such as blackhole, sinkhole, jellyfish, and wormhole attacks [1, 9]. This simulation is setup in many sessions. Every session is used to forward 150 packets toward cluster head. Greyhole node is introduced from second session onward (i.e., in sessions 3, 4, 5, and 6). In first two sessions, all the routing protocols successfully forward all the packets without any loss. However, when greyhole malicious node is introduced, almost half of the packets are dropped by all the routing schemes. However, our proposed mechanism adapted a new route from session 4 and onward.

Our proposed mechanism also dropped almost half of the packets in session 3. At the end of session 3, our mechanism waits for response of cluster head to receive a packet counter in which the cluster head will mention the number of packets

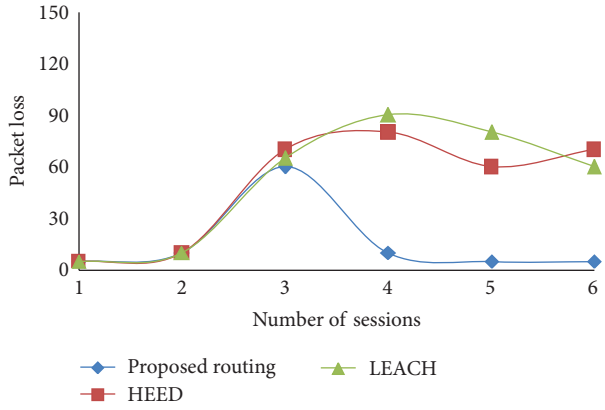

Figure 11: Packet loss in presence of malicious node.

successfully arrived. Cluster head sends packets to nodes by enabling packet counter in it. The node sees that the total number of packets sent to cluster head were 150 while only 70 packets are successfully transferred. At this stage, our routing scheme assumes that the neighbor is malicious and it is dropping packets. That is why in session 4 and onward, packet loss in our routing mechanism is negligible due to selection of alternate path. On the other hand, HEED and LEACH cannot distinguish malicious node in their way.

5. Conclusion

Research community is trying to explore different possibilities to enable energy harvesting in WSN. In this way, the lifetime of sustainable WSN can be increased to a great extent to achieve all goals of sensors deployment. In this paper, we presented in detail a secure routing protocol for WSN, which is based on cross-layer design and energy-harvesting technique. We use a cluster-based approach to group together nodes of two-hop neighbors. Initially all the nodes are in active state, in which nodes actively participate in WSN operations. However, as long as the energy value of sensor node decreases, it switches to semiactive state. In semiactive state, nodes are in wake and sleep conditions. In wake position, nodes take part in network operations, while in sleep position, nodes only harvest environmental energy. In idle state, nodes only harvest energy till it switches back either to active or semiactive states. When compared to other cluster-based routing protocols such as HEED and LEACH, our proposed routing scheme shows better performance in terms of network lifetime, number of live nodes, remaining network energy, and the presence of malicious node.

Some packet loss is observed in our mechanism especially in session 3 as shown in Figure 11. We cannot use per packet acknowledgement as it may result in high routing overheads. We are planning to devise a mechanism in which such packet loss could be reduced. Our future work is to design such distributed algorithm, which is capable of operating in both cluster and non-cluster-based WSN. Furthermore, such mechanism is also desirable since it enables sensor nodes to harvest environmental energy as well as participate in network operations simultaneously. Security mechanism can be improved by using lightweight hash function mechanism or advanced cryptographic scheme to handle active and passive attacks. An interesting technique of artificial neural network (ANN) can be considered to locate those nodes having less remaining energy.

Acknowledgments

The authors extend their appreciation to the Research Centre, College of Applied Medical Sciences, and the Deanship of Scientific Research at King Saud University for funding this research.

References

[1] S. Khan, N. Mast, and J. Loo, "Denial of service attacks and mitigation techniques in IEEE 802.11 Wireless mesh networks," *Information*, vol. 12, pp. 1–8, 2009.

[2] M. Segal, "Improving lifetime of wireless sensor networks," *Network Protocols and Algorithms*, vol. 1, no. 2, pp. 48–60, 2009.

[3] J. M. Gilbert and F. Balouchi, "Comparison of energy harvesting systems for wireless sensor networks," *International Journal of Automation and Computing*, vol. 5, no. 4, pp. 334–347, 2008.

[4] S. Sendra, J. Lloret, M. Garcia, and J. F. Toledo, "Power saving and energy optimization techniques for Wireless Sensor Networks," *Journal of Communications*, vol. 6, no. 6, pp. 439–459, 2011.

[5] A. H. Mohsin, K. Abu Bakar, A. Adekiigbe, and K. Z. Ghafoor, "A survey of energy-aware routing protocols in Mobile Adhoc networks: trends and challenges," *Network Protocols and Algorithms*, vol. 4, no. 2, pp. 82–107, 2012.

[6] S. Shakkottai, T. S. Rappaport, and P. C. Karlsson, "Cross-layer design for wireless networks," *IEEE Communications Magazine*, vol. 41, no. 10, pp. 74–80, 2003.

[7] V. Srivastava and M. Motani, "Cross-layer design: a survey and the road ahead," *IEEE Communications Magazine*, vol. 43, no. 12, pp. 112–119, 2005.

[8] S. Khan, K. K. Loo, N. Mast, and T. Naeem, "SRPM: secure routing protocol for IEEE 802.11 infrastructure based wireless mesh networks," *Journal of Network and Systems Management*, vol. 18, no. 2, pp. 190–209, 2010.

[9] S. Khan and J. Loo, "Cross layer secure and resource-aware on-demand routing protocol for hybrid wireless mesh networks," *Wireless Personal Communications*, vol. 62, pp. 201–214, 2010.

[10] S. Khan, N. Mast, J. Loo, and A. Silahuddin, "Passive security threats and consequences in IEEE 802. 11 wireless mesh networks," *International Journal of Digital Content Technology and Its Applications (JDCTA)*, vol. 2, pp. 4–8, 2008.

[11] M. Frederickson, A publication of the National Electronics Manufacturing Center of Excellence, 2005.

[12] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," *Ad Hoc Networks*, vol. 3, no. 3, pp. 325–349, 2005.

[13] S. Singh, M. Singh, and D. Singh, "Routing protocols in wireless sensor networks, A survey," *International Journal of Computer Science & Engineering Survey (IJCSES)*, vol. 1, pp. 25–34, 2010.

[14] A. Popescu, G. Tudorache, B. Peng, and A. Kemp, "Surveying position based routing protocols for wireless sensor and Ad-hoc networks," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 4, no. 7, pp. 41–67, 2012.

[15] O. Fdili, Y. Fakhri, and D. Aboutajdine, "Impact of queue buffer size awareness on single and multi service real-time routing protocols for WSNs," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 4, no. 2, pp. 104–111, 2012.

[16] M. Hussaini, H. Bello-Salau, A. Salami, F. Anwar, A. Abdalla, and M. Islam, "Enhanced clustering routing protocol for power-efficient gathering in wireless sensor network," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 4, no. 12, pp. 18–28, 2012.

[17] A. Kellner, O. Alfandi, and D. Hogrefe, "A survey on measures for secure routing in wireless sensor networks," *International Journal of Sensor Networks and Data Communications*, vol. 1, Article ID 235548, pp. 1–17, 2012.

[18] J. Sen, "A survey on wireless sensor network security," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 1, pp. 55–78, 2009.

[19] K. Xing, "Attacks and countermeasures in sensor networks, a survey," *Springer Network Security*, vol. 7, pp. 534–548, 2005.

[20] V. Kesavan and S. Radhakrishnan, "Multiple secret keys based security for wireless sensor networks," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 4, no. 1, pp. 68–76, 2012.

[21] M. Azeem, K. Khan, and A. Pramod, "Security architecture framework and secure routing protocols in wireless sensor networks-survey," *International Journal of Computer Science & Engineering Survey (IJCSES)*, vol. 2, pp. 189–204, 2011.

[22] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2-3, pp. 293–315, 2003.

[23] B. Kur, *Secure routing protocols for wireless sensor networks [M.S. thesis]*, Masaryk University Faculty of Informatics, Brno, Czech Republic, 2008.

[24] P. Samundiswary, D. Sathian, and P. Dananjayan, "Secured greedy perimeter stateless routing for wireless sensor networks," *International Journal of Ad Hoc, Sensor & Ubiquitous Computing (IJASUC)*, vol. 1, pp. 9–20, 2010.

[25] M. Liu, J. Cao, G. Chen, and X. Wang, "An energy-aware routing protocol in wireless sensor networks," *Sensors*, vol. 9, no. 1, pp. 445–462, 2009.

[26] M. Younus, A. A. Minhas, M. Y. Javed, and A. Naseer, "EEAR: efficient energy aware routing in wireless sensor networks," in *Proceedings of the 7th International Conference on ICT and Knowledge Engineering (ICTKE '09)*, pp. 57–62, December 2009.

[27] S. Singh, M. Singh, and D. Singh, "A survey of energy-efficient hierarchical cluster-based routing in wireless sensor networks," *International Journal of Advanced Networking and Applications*, vol. 2, pp. 570–580, 2010.

[28] D. Noh, I. Yoon, and H. Shin, "Low-latency geographic routing for asynchronous energy-harvesting WSNs," *Journal of Networks*, vol. 3, no. 1, pp. 78–85, 2008.

[29] O. Jumira, R. Wolhuter, and S. Zeadally, "Energy-efficient beaconless geographic routing in energy harvested wireless sensor networks," *Concurrency and Computation*, vol. 25, no. 1, pp. 58–84, 2013.

[30] Z. Eu and H. Tan, "Adaptive opportunistic routing protocol for energy harvesting wireless sensor networks," in *Proceedings of the IEEE International Conference on Communications (ICC '12)*, pp. 318–322, June 2012.

[31] R. Doost, K. R. Chowdhury, and M. Di Felice, "Routing and link layer protocol design for sensor networks with wireless energy transfer," in *Proceedings of the 53rd IEEE Global Communications Conference (GLOBECOM '10)*, December 2010.

[32] K. Takahashi, M. Bandai, H. Tan, W. Seah, and T. Watanabe, Least Impact Routing towards Sustainable Sensor Networks Enhanced by Energy Harvesting. White Paper published by Victoria University of Wellington, 2010.

[33] G. Dai, J. Qiu, P. Liu, B. Lin, and S. Zhang, "Remaining energy-level-based transmission power control for energy-harvesting WSNs," *International Journal of Distributed Sensor Networks*, vol. 2012, Article ID 934240, 12 pages, 2012.

[34] N. Pais, "Cost-benefit aware routing protocol for wireless sensor networks with hybrid energy storage system," *Journal of Green Engineering*, vol. 11, pp. 189–208, 2011.

[35] S. Kim, C. Won, J. Lee, S. Kwon, and Y. Park, "Harvesting aware system for sustainable mobile sensor networks," *International Journal of Hybrid Information Technology*, vol. 5, pp. 199–206, 2012.

[36] Z. A. Eu, H. P. Tan, and W. K. G. Seah, "Opportunistic routing in wireless sensor networks powered by ambient energy harvesting," *Computer Networks*, vol. 54, no. 17, pp. 2943–2966, 2010.

[37] A. Förster, A. Förster, and A. L. Murphy, "Optimal cluster sizes for wireless sensor networks: an experimental analysis," in *Ad Hoc Networks*, vol. 28 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pp. 49–63, 2010.

[38] A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Computer Communications*, vol. 30, no. 14-15, pp. 2826–2841, 2007.

[39] S. Chalasani and J. M. Conrad, "A survey of energy harvesting sources for embedded systems," in *Proceedings of the IEEE Conference of Southeastcon*, pp. 442–447, April 2008.

[40] B. Atwood, B. Warneke, and K. S. J. Pister, "Smart dust mote forerunners," in *Proceedings of the 14th IEEE International Conference on Micro Electro Mechanical Systems (MEMS '01)*, pp. 357–360, January 2001.

[41] G. Park, T. Rosing, M. D. Todd, C. R. Farrar, and W. Hodgkiss, "Energy harvesting for structural health monitoring sensor networks," *Journal of Infrastructure Systems*, vol. 14, no. 1, pp. 64–79, 2008.

[42] L. Mateu and F. Moll, "Review of energy harvesting techniques and applications for microelectronics," in *Proceedings of the SPIE Microtechnologies for the New Millennium*, pp. 359–373, May 2005.

[43] C. Moser, *Power management in energy harvesting embedded systems. Doctor of Sciences dissertation [Ph.D. thesis]*, Swiss Federal Institute of Technology Zurich, Zurich, Switzerland, 2009.

[44] A. Kansal, J. Hsu, S. Zahedi, and M. B. Srivastava, "Power management in energy harvesting sensor networks," *ACM Transactions on Embedded Computing Systems*, vol. 6, no. 1, pp. 1–35, 2007.

[45] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the 33rd Annual*

Hawaii International Conference on System Siences (HICSS-33), p. 223, Maui, Hawaii, USA, January 2000.

[46] M. Ba, I. Niang, B. Gueye, and T. Noel, "A deterministic key management scheme for securing cluster-based sensors networks," in *Proceedings of the IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing (EUC '10)*, pp. 422–427, December 2010.