Design Principles of Routing Protocols in Wireless Sensor Networks

Gergely Ács, Levente Buttyán
Laboratory of Cryptography and Systems Security (CrySyS)
Department of Telecommunications
Budapest University of Technology and Economics, Hungary
{acs, buttyan}@crysys.hu

October 28, 2010

Abstract

There have been proposed multiple surveys on wireless sensor network routing in the past. However, they use rough operational and network models to classify routing protocols as well as disregard works which are not routing protocols but rather function as separate routing modules. Moreover, dependability concepts of sensor network routing have not been addressed by them. In this work, we attempt to factor out the main design principles for sensor network routing, as well as to identify the most important dependability concepts in this context. We propose a modular approach to design a routing protocol for sensor network applications. We gather the mainstream implementations of each module to aid this development process.

1 Introduction

There is a vast literature of wireless sensor network routing protocols. The variety of routing protocols is caused by the diverse application requirements and network assumptions. Routing surveys [1, 2] that have been proposed so far attempt to make an exhaustive list of existing routing protocols and/or classify them based on some rough network and operational characteristics. However, this approach has several problems which are detailed as follows.

- First, this hardly supports the development of sensor network applications due to the rough operational and network models. In particular, using these classifications, it is difficult to identify a routing protocol which perfectly fits specific application requirements. In practice, there have been two extremes

of designing routing protocols so far. First, an application designer selects a routing protocol which partially satisfies application requirements and provides a "good enough but not perfect" solution. For instance, AODV [46] and TinyOS beaconing [79] seems to be workable routing solutions for most sensor applications, however, they are far from being efficient for resource constrained devices. Second, a novel protocol is developed using a clean-slate design. Although this new protocol is tailored to a specific application, it may lack for exhaustive analyses because its constrained application domain.

- Second, current routing surveys have a rough picture of routing protocols, they often disregard such proposals which are not routing protocols indeed but are *components* of that. Prior works on sensor network routing are diverse which means that the proposed routing components are often independent and can be jointly used. For instance, some works focus on path selection [16], while others deal with different cost metrics and their calculation [27, 40].

- Third, current surveys do not consider the dependability attributes of sensor network routing protocols. For instance, there are separate security surveys of networking protocols, and routing surveys hardly contain secure routing protocols. Dependability is a part of routing objectives, and as such, it should be considered from the grounds as a basic design principle. For instance, multipath routing increases the reliability of the routing service inevitably. However, one may reach the same reliability improvement with lower overall network overhead by using cluster-based or cooperative forwarding. Moreover, these low-layer modules often fall behind the scope as they reside between the routing and data-link layer belonging to neither of them. Finally, dependability also includes reliability and maintenance attributes besides security which are not considered by any routing surveys.

- Fourth, multiple routing techniques have been proposed for wireless sensor networks since the creation of the latest survey. To the best of our knowledge, they have not been covered by any survey so far. Our work is aimed to fill this gap and we consider all major routing techniques which have been developed meantime.

Instead of creating yet another survey of routing protocols, here we attempt to factor out the main design principles for sensor network routing, as well as to identify the most important dependability concepts in this context.

We imagine that a routing protocol is a combination of different routing modules. Each module may have one or more routing objectives (like real-time or de-

pendable packet delivery) and multiple implementations in different works, where each implementation may have different routing model (i.e., network and operation assumptions). First, we select the required routing modules based on the routing objectives of the application. Afterwards, we select an implementation of these modules having the identified routing model. As every implementation is analysed in its routing model, the performance of their combination should also be easily computable. We believe that this approach is more beneficial for an application designer than the exhaustive list of different routing techniques.

In order to aid this development process, we identify the mainstream implementations of different modules, and give their routing model. We emphasize that this list of implementations is not intended to be exhaustive, it rather serves as a starting point as well as a demonstration purpose for our method. In addition, in contrast to prior works, we also classify all modules (and indirectly routing protocols) according to their dependability attributes (like availability, reliability, security and maintainability) that enables designers to consider dependability objectives as a basic design principle.

2 The routing model

Our model builds upon the *network and operational model*, a set of *routing modules*, and the *routing objectives*. Instead of selecting a specific protocol, an application designer should identify routing modules which try to achieve the desired routing objectives. The routing objectives define the goals of all routing modules like the guarantees of packet delivery with real-time constraints and dependable requirements. Afterwards, an implementation of the module can be chosen which matches the network and operational model of the application. All modules are categorized into four different components.

The *low-layer component* includes all modules which directly invokes the data-link layer in order to conserve energy as well as to increase reliability and network throughput. In particular, these modules can measure link reliability to aid routing decisions, use network coding or error-correction to reduce retransmissions, or implement reliable broadcasts by exploiting node overhearing. These modules provide different link-layer measurements and/or topological information to upper-layer modules.

The *cost calculation component* encompasses all routing cost calculation modules. These modules may need some input from the low-layer modules such as reliability or power transmission measurements and assign a cost value to a node in the network. This cost value may incorporate energy-based, distance-based, link-reliability based, time-based, or maintenance cost based metrics. This is a

core component which means that a routing protocol must include at least one cost calculation module.

The *path selection component* selects a path towards a destination based on the available routing information delivered by low-layer and cost-calculation modules. This component includes modules which implement a mean of path selection like centralized selection when a single node computes the routing tables of all other nodes in the network, multi-path selection, probabilistic selection, or route selection towards multiple base stations. This is also a core component (i.e., a routing protocol must include at least one path selection module).

Finally, the *security component* gathers all modules with specific security goals like data authentication and confidentiality, or misbehaving detection. These security functionalities may be invoked by all modules in all components.

The relation of all modules and components are depicted in Figure 1.

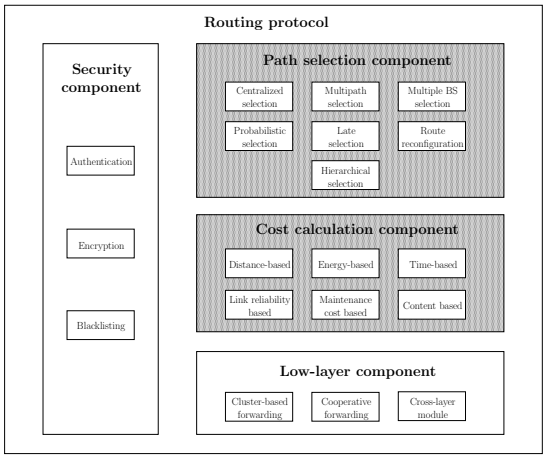

Figure 1: Routing components. Darker boxes denote core components.

3 Network and operational model

3.1 Network model

Base station It is commonly agreed that the base station is a powerful device with unconstrained energy supply and computational capacity. However, the following characteristics of a base station may severely influence the operation of a routing protocol.

Number: In most practical applications, the increased number of base stations

provides more robust data gathering, and may also decrease the network delay. However, the typical number of base stations is one. If only one base station is presented (and there is no need for explicit communication between sensor nodes), the destination node for all messages is identical, while in case of multiple base stations, the destination node may vary.

Mobility: In some applications, where the number of base stations is too small to ensure acceptable network delay and robustness, the base station supports mobility during data gathering. This property of the base station severely affects routing, since some nodes in the network field cannot follow the movement of the base station and are not aware of its current position. Hence, the routing mechanism needs to find the mobile base station in the field. Moreover, the routing topology may heavily vary in time that causes extra overhead in the network layer. A few routing modules support mobile base stations, while others tolerate limited mobility.

Presence: The base station can be either continuously or partially presented during the routing process. In the latter case, the routing protocol must support the temporary lack of a base station (e.g., the base station is switched off for a certain amount of time due to maintenance reasons), since a missing base station cannot definitely mean a failure. Thus, the messages should not be dropped or rerouted rather their delivery should be delayed.

Sensor nodes In most sensor networks, sensor nodes are homogeneous tiny devices with constrained energy supply and computational capabilities. In addition, we assume that all sensor nodes are stationary. The following characteristics of sensor nodes may differ for some networks, and they can influence the protocol operation.

Deployment: Sensor nodes can be deployed in either a deterministic or a random fashion. When nodes are deployed along a road-side, or in a metro-station, the deployment is rather deterministic than random. In these cases, the protocol should adapt to the fixed network topology. However, numerous routing protocols proposed so far rely on the more general random deployment (e.g., nodes are scattered from a helicopter).

Addressing: The task of routing in sensor networks is to deliver the queries to the sensor nodes which have the requested data (in case of query-driven routing protocols, see later), and to return the requested data to the querier node. Accordingly, we can distinguish the addressing method of queries and responses:

- *Query-addressing:* All routing protocols which use query dissemination in the networks employ data-based (What is the average temperature?), or location-based addressing (What is the average temperature in location (x, y)?). Here, the location can also be a virtual location which means that they are calculated based on the connectivity graph of the network instead of exact geographic positions (e.g., all nodes in the network can determine their distances measured in hop-counts from the same pre-defined landmark nodes. Then, these distances for each node constitute a vector that is further used to address the node.)
- *Response-addressing:* The response is either returned on the reversed path which the query traversed, or it is routed back purely based on location information. In the former case, neighboring nodes use locally (or globally) unique identifiers to identify the neighbor from which they received the query, and which is further used to forward the reply towards the destination.

3.2 Operational model

Communication pattern: A routing protocol can support the communication from sensor nodes to sensor nodes, from base stations to sensor nodes, as well as from sensor nodes to base stations.

- *Node-to-Node:* Generally, there is no need for this kind of communication in sensor networks. However, in some special applications where it is needed, a few routing modules supports this pattern, or alternatively, ad hoc network routing protocols can be employed.
- *Node-to-Base station:* This pattern is usually supported in order to route responses back to the base station. This is typically reverse-multicast (many-to-one), a.k.a. convergecast, which means that every sensor node is able to send a message to any base station. If there are multiple base stations or only one node is responsible for gathering and transmitting the sensed data to the base station, this pattern can also be unicast.
- *Base station-to-Node:* This is the pattern of routing requests originated from the base station to sensor nodes. This is typically anycast (one-to-many), which means that any sensor node which has the requested data can respond to the query. If some nodes are uniquely identified in the network (by their IDs, locations, etc.), then multicast (one-to-many) and unicast (one-to-one) patterns can also be supported. The base station(s) must be capable of sending messages to any sensor nodes.

Reporting model: The reporting model describes *what* initiates data reporting. In this sense, we distinguish time-driven, query-driven, and event-driven protocols.

- *Time-driven:* Employing a time-driven routing protocol, a sensor node is triggered in specific moments, when it should perform its measurement task, and forwards the measurement to its next-hop neighbor. These activations can be periodic or one-shot in time. Short periods may cause more traffic in the network, and the quality of routing in terms of energy efficiency becomes a crucial concern. Time-driven sensors may be pre-programmed, or the reporting schedule may come with explicit queries. Furthermore, a time-driven routing protocol can support in-network processing (like data aggregation) on intermediate nodes.
- *Query-driven:* The task of a query-driven protocol is to route the queries to the measurement area, and to route back the response to this query. A query-driven routing protocol can also support data aggregation on intermediate forwarders.
- *Event-driven:* A sensor node sends a measurement towards the base station only if a given event occurs (e.g., the temperature falls below a certain threshold). An event-driven routing protocol can support data aggregation on intermediate nodes.

4 Routing objectives

Some sensor applications only require the successful delivery of messages between a source and a destination. However, there are applications that need even more assurances. These are the real-time and dependability requirements of packet delivery.

Real-time delivery: The assurance of message delivery is indispensable for all routing protocols. This means that the protocol should always find the route between the communicating nodes, if it really exists. This correctness property can be proven in a formal way, while the average-case performance can be evaluated by measuring the message delivery ratio.

Additionally, some real-time applications require that a message must be delivered within a specified time, otherwise the message becomes useless or its information content is decreasing after a time bound. Therefore, the main objective of these modules is to control the network delay. The average-case

performance is evaluated by measuring the message delivery ratio with time constraints.

Dependable delivery: In general, dependability encompasses the following attributes: *availability*, *reliability*, *safety*, *security*, and *maintainability*.

Theoretically, in case of routing, availability means the readiness for correct routing service, where correct routing service is delivered when the service implements the routing function (i.e., it delivers the given packets from the source to the destination). Availability is usually a measure of the delivery of correct routing service with respect to the alternation of correct and incorrect routing service. In general, all techniques which aim at maximizing the network lifetime and increasing the reliability of the routing service belong to this category. Maximization network lifetime is crucial for those networks, where the application must run on sensor nodes as long as possible. The protocols aiming this concern try to balance the energy consumption equally among nodes considering their residual energy levels. However, the metric used to determine the network lifetime is also application dependent. Most protocols assume that every node is equally important and they use the time until the first node dies as a metric, or the average energy consumption of the nodes as another metric. If nodes are not equally important, then the time until the last or high-priority nodes die can be a reasonable metric.

Reliability refers to the continuous delivery of the correct routing service, and it is a measure of the time until a routing failure occurs. These techniques usually achieve reliability by increasing packet delivery ratio. Safety is simply the absence of catastrophic consequences of routing malfunction on the user(s) and the environment, and it is a measure of the time until the occurrence of a catastrophic routing failure. As routing safety is usually considered to be as routing reliability with respect to catastrophic failures, we do not distinguish routing safety and reliability in the sequel.

Note that availability and reliability are strongly related attributes of routing dependability. All mechanisms that increase the reliability of the routing service usually also increase its availability. However, there are some techniques which primarily intend to improve the availability of the service, and not its reliability. These include all mechanisms that attempt to maximize the network lifetime. Clearly, the application of such techniques does not affect the continuity of successful packet delivery, but rather the time how long the service can be eventually invoked.

Security refers to the ability to prevent or mitigate malicious faults that are deliberately caused by the adversary in the routing service. All mechanisms

that prevent an adversary to cause malicious faults in the routing service belong to this group. These include all modules which attempt to increase reliability and can be successfully used against some attacks. For instance, multipath routing, blacklisting, route reconfiguration, probabilistic forwarding, link-reliability metrics, and using multiple base stations can mitigate malicious packet dropping, in case message authentication is assumed.

Finally, maintainability refers to the ability to undergo route repairs, and it is a measure of the time of the continuous delivery of incorrect service. Maintainability includes all techniques which helps the routing service to recover from faults.

5 Routing modules

This section details the identified routing modules. Table 1 contains the routing objectives of each module, whereas Table 2 lists the mainstream implementations of each routing module. Note that a routing module can have multiple objectives, and a single work can propose specific implementations for multiple modules. Finally, in Table 3, we identified the network and operational model of these implementations.

5.1 Low-layer modules

Low-layer modules rely on the functionality of the data-link layer to to achieve better performance in terms of network delay and energy consumption.

Cross-layer module: This module is strongly integrated with the data-link layer (as part of a cross-layer design) and exploits the capability of tuning the transmission power of the sensor devices [3], or identifies the best forwarding candidate during a MAC-layer handshaking (e.g., by means of distributed contention [4]). Adjusting the transmission power, every node can calculate what energy level should be used to transmit a message to a neighboring node. This energy level may be inversely proportional to the cost assigned to the neighboring node.

This module helps to achieve higher delivery ratio, which means that this design can also increase the reliability of the routing service.

Cooperative forwarding: Cooperative forwarding exploits the broadcast nature of wireless communication to improve energy efficiency and packet delivery ratio. Nodes buffer packets, and when enough information have been

received to recover the original packet, a packet combining procedure is executed. This packet combining technique, which can be based on network coding, or error correcting codes, exploits the broadcast medium and spatial diversity of a multi-hop wireless network by using packets overheard at any node. For example, in [5], nodes combine corrupted packets into correct packets. This protocol allows one node to receive two or more corrupted versions of a packet from its upstream nodes through overhearing, and then recovers the original packet by combining the corrected versions of the packet into the original one. Cooperative forwarding has been shown to increase the delivery ratio [5]. Cooperative forwarding is usually strongly integrated with the data-link layer, and it should disregard the mutable parts of a packet from packet combining (i.e., these parts are modified at each hop). Thus, a minimal interaction with the routing protocol is also needed to detect such packet parts.

Cluster-based (opportunistic) forwarding: Cluster-based forwarding also exploits the broadcast nature of wireless communication to improve energy efficiency. These techniques can be used in conjunction with any routing protocol to achieve better energy-efficiency by reducing retransmissions. The idea is that each node forms a cluster such that any node in the next-hop's cluster can take forwarding responsibility. This is motivated by the fact that link quality shows significant variability especially in wireless sensor networks, which would normally require several number of retransmissions from the MAC layer in order to successfully deliver a packet. Two subgroups can be further distinguished.

In the first subgroup, two mechanisms are proposed to diminish the number of retransmissions [6, 7]. The first is to use "helper nodes", which reduces the number of retransmissions by adaptively migrating packet forwarding tasks from weak links to strong links. This means that, instead of retransmitting a packet, the sender "delegates" the retransmission to an intermediate node which has a better quality link to the intended receiver and, opposed to the receiver, has already received the packet by the first transmission. Second, CBF takes advantage of the occasionally successful transmissions over long (and likely lossy) links. In particular, if a (distant) node receives the packet which is closer to the final destination, then the sender does not need to retransmit the packet, because this distant node can forward the packet towards the destination. The module proposed in [6] lies between the data-link and networking layer and it can be used in conjunction with any routing protocols.

Those techniques belong to the second subgroup which also rely on overhearing, and mainly used to implement reliable broadcast protocols. The first time a node hears a broadcast it retransmits the packet unconditionally, as in a normal flood. As additional neighbors transmit the same packet, the node listens and overhears which neighbors have propagated the broadcast. If each node is aware of its one-hop neighborhood, it determines the number of neighbors that are guaranteed to have seen a packet. When this number falls below a predetermined threshold, a node will again retransmit the broadcast packet. This threshold is tuned according to neighborhood density, as higher density neighborhoods require lower thresholds; other neighbors are likely to broadcast as part of the same flood. The protocols belonging to this subgroup (e.g., [8] [9]) can be used with any routing protocols that rely on global broadcast communication.

5.2 Cost calculation modules

These modules are responsible for the computation of the routing cost which is used to select the next-hop forwarder (or route) towards the destination.

Energy-based cost: The routing cost, which is assigned to next-hop forwarders or routes, can incorporate energy-based metrics in order to prolong network lifetime. These metrics include the residual energy of neighbors to avoid their fast depletion, or the average power level needed to send a packet in order to minimize the energy costs. For instance, in [10], the energy cost of a forwarding candidate is calculated as $e^{\alpha} \cdot R^{\beta}$, where e is the energy used to transmit and receive on the link, R is the residual energy of the candidate, and α, β are tunable weighting factors.

Energy-based metrics have a strong relation to link reliability based metrics. In particular, several experimental studies on wireless ad-hoc and sensor networks [11, 12] have shown that wireless links can be highly unreliable and exhibit high packet drops. This results in drastic reduction of delivery rate or increased energy wastage if retransmissions are employed. Therefore, combining the expected number of transmission into routing costs [13, 3] results in lower decreased energy costs and higher delivery rate. For instance, modifying the above energy metric accordingly, e can be calculated as $E(p) \cdot R(p)$ [3], where $E(p)$ is the energy level consumed for transmitting a packet at power level p, while $R(p)$ is the expected number of transmissions before the sender successfully delivers a packet to the candidate using power level p.

Distance-based cost: Each node has a position which is used to calculate the distance between any pair of nodes in the network. This distance is either calculated based on the network's connectivity graph and measured by hop-counts, or it is the Euclidean distance of nodes computed from their geographic positions. In the former case, if a node has a single coordinate (i.e., the number of hops between the source and the destination) an additional unique network identifier of the destination is needed to successfully deliver packets. This metric is employed by the basic version of several routing protocols such as INSENS [14]. In addition, these protocols usually require the discovery of the destination before data forwarding which results in additional costs. In the latter case, each node is aware of its own geographic position, which is used to implement geographic routing. Therefore, unique network identifiers are not needed, as positions are unambiguously assigned to nodes which also eliminates the discovery of the destination in case its position is a priori known. Alternatively, a node can calculate its (virtual) position by measuring its hop-count distance from several pre-defined landmark nodes, and using a similar routing technique like in geographic routing, this virtual position is further used to route data packets towards the destination. Geographic and virtual position based routing is also called as location-based routing protocols.

The advantage of location-based forwarding is that it is scalable (e.g., there is no path setup and recovery latency), it is suitable for both critical aperiodic and periodic packets, and the per-packet path discovery results in self adaptation to network dynamics. In addition, it seems to be more robust against different routing attacks due to its stateless nature (more precisely, routing states consist of the locations of neighboring nodes). On the other hand, each node must be aware of its own position which may require extra hardware components (like GPS), or the extra communication of location coordinates. Moreover, due to its stateless nature, each data packet carries extensive routing information (i.e., node coordinates) which further increases communication overhead.

Geographic positions can be pre-programmed before node deployment or retrieved using external GPS [15, 16, 17, 18, 19, 20, 21, 4, 22, 23, 24, 25, 3, 26, 27, 28, 29, 30]. By contrast, virtual positions are obtained by using only connectivity information, and thus, there is no need for GPS-capable devices. The drawback of these solutions is that a position is described by a location vector which typically have more than 2 or 3 coordinates (e.g., in case of BVR [31] this is around 10 in order to ensure acceptable delivery ratio) which causes extra communication costs as each data packet must carry

at least the location of the destination [31, 32, 33, 34, 35, 36, 37, 38].

Content-based cost: Most sensor applications are data-centric, which means that it is more important *what* data is asked for rather than *who* the originator is. In particular, using content-based forwarding, a query is addressed by the data itself (like what the average temperature is or whether there is an alarm situation) and not with the a sensor's address. The base station subscribes to interested events by sending queries which specifies the interested data (this also can be a complex query), and a sensor node which can resolve the query sends a response back to the base station. In the simplest case, a query floods the entire network, but next-hops can be selected by using more sophisticated information theoretic metrics.

Link reliability based cost: The routing cost can incorporate some link-reliability metric. For instance, this can be a slightly modified version of the expected number of transmissions (ETX) which considers forward and backward reliability to identify high throughput paths [11]. Such a metric allows the routing protocol to consider cumulative link reliability over paths, and find the most reliable end-to-end path. As link delivery rate changes over time due to environment or transient traffic characteristics and link statistics needs to be reasonably responsive to these changes, the estimation of link quality is required [11]. There are active or passive techniques to collect link statistics. Active techniques rely on periodic broadcasts containing link statistics about each neighbor. This can incur higher control message overhead if link reliability changes frequently. Passive probing involves piggybacking link statistics to the outgoing data packets.

Time-based cost: This category includes all metrics which incorporate the propagation delay of routing messages and are used to select a path which satisfies certain real-time conditions. In [39], the propagation delay of control messages are taken as a selection criteria, and thus, it attempts to select the quickest path between the source and destination. In [24], a network wide speed of packet delivery for real-time guarantee is ensured. Particularly, each node maintains the average delay to each neighbor and uses this to evaluate the packet progress speed of each neighbor node and forwards a packet to a node whose progress speed is higher than a pre-specified lower-bound speed t. If each node can find a neighbor that can progress a packet with a speed higher than t, t can be guaranteed in the whole network. A similar approach is employed in [3], where each data packet carries a time-stamp that is used to calculate the required speed v of the packet at each hop. Those neighbors are considered as potential forwarders, which can provide higher reception

speed than v. The delay on each link is estimated as the function of the transmission time of the packet, the contention delay (the time needed to acquire the channel), and the expected number of transmissions before the sender successfully delivers the packet.

Maintenance based cost: In case some nodes become out of order (e.g., they run out of their energy supply), they are needed to be repaired or replaced. The frequency and the cost of these maintenance activities highly influence the time needed to recover the routing service, and eventually the maintainability of the routing service.

The frequency and the cost of maintenance operations in a sensor field is essentially dependent on the way nodes are depleted. As routing protocols mainly influence the energy consumption of sensor nodes, they can help to create a favorable depletion profile which considers maintenance efficiency. For example, if some nodes are deployed on the top of some trees, while others are not, the maintenance cost of the nodes on the trees are likely to be considerably higher. Thus, a maintenance cost aware routing protocol should carefully use these nodes to forward data.

Note that this metric, which is first proposed in [40], can be combined with most routing protocols by simply incorporating the maintenance cost into the routing cost metric.

If a node stores only negligible amount of routing information like the positions of neighbors or its own routing cost, the module is *stateless*. Otherwise, when a node may need more extensive processing or storage resources, the module is *stateful*. Note that most routing protocols combines multiple metrics into a single routing cost. For instance, in [27, 20, 4, 21], the geographic distance is combined with link reliability based and energy-based metrics, while in [3], a time-based metric is also included.

5.3 Route selection modules

These modules are responsible for the selection of a route towards the destination.

Probabilistic selection: The next forwarder is selected probabilistically, where higher probability is assigned to low-cost routes or forwarders. For instance, in [10], the forwarding probability between nodes i and j is calculated as $p_{i,j} = \frac{1/C_{i,j}}{\sum_{\forall k} 1/C_{i,k}}$ in a decentralized manner, where $C_{i,j}$ is the cost between nodes i and j, and k is the index of i's neighbors.

Probabilistic forwarding aids load-balancing, achieves route diversity, and thus, increases routing reliability.

Hierarchical selection: Employing hierarchical routing protocols, a hierarchy level is assigned to each node, and a node only forwards those messages that are originated from a lower-level node. This also helps in-network processing, as a node can aggregate incoming data before forwarding that to upper-layer nodes. The base station resides on the top of the hierarchy. The hierarchy construction can be dynamic or static. Using dynamic construction, the role of the cluster head (CH) is rotated, and all nodes belonging to the same cluster will forward all data to their elected CH. The aim of forming this hierarchy is to prolong the network lifetime and to increase reliability.

Late selection (broadcast-based forwarding): Each node blindly rebroadcasts all received data packets, and each receiver decides whether the received packet should be rebroadcast or not. The decision can be based upon who sends the message, who the originator is, who it is destined to, or what state it has (e.g., accumulated routing cost). Therefore, broadcast-based forwarding is simply the passing of routing decisions to the next-hops. This technique may increase the robustness of delivery, as all neighbors receive the data packet and can easily take over the forwarding responsibility of neighboring nodes. On the other hand, it can have significant communication and storage overhead.

Centralized selection: Each sensor node selects the next-hop towards the destination either by itself using locally available routing information exclusively in a *decentralized* manner, or every node sends its neighbor list (and the corresponding routing information) to the base station which then computes the next-hop forwarders for all nodes in the network in a *centralized* manner. Although centralized computation gives optimal solution, it may yield heavy network communication and it is not scalable.

Route selection towards multiple base stations: In order to improve the robustness of data collection, multiple base stations (or drains) may be employed. The aim of using multiple base stations is two-fold. First, if the size of a sensor network grows, the paths between the base station and sensors become longer. Thus, the energy consumed by each node to route data to the base station will increase, thereby reducing the lifetime of the nodes. The energy consumed in forwarding the data may be reduced if multiple base stations are employed. This can be implemented by requiring each node to route data towards either a single base station, or to multiple base stations

using multi-path routing. Second, in order to be resilient to any single base stations failures, every sensor is required to route data towards two or more distinct base stations. Therefore, employing multiple base stations increases the reliability of the routing service.

Multi-path selection: Multipath routing, which encompasses delivering of data packets on multiple paths towards the destination, is a common technique to achieve robustness and load-balancing. The multiple paths between the source and the destination can be partially or completely disjoint and they are maintained at the expense of increased energy consumption and traffic generation. Apart from load-balancing and robustness against node failures, multi-path routing also inherently provides some defense against malicious packet dropping; in order to prevent a packet to reach the base station, the adversary must control a node on each used path to drop the packet. Multi-path techniques used in sensor networks can be divided into three groups:

- The source makes multiple copies of a packet, and routes these copies on different paths in order to increase robustness [41] [42]. These paths can be calculated in advance and maintained proactively by sending data packets at a low rate *only* on these paths [42]. Alternatively, if the sources have data to send, they flood the *whole* network with data packets at a low rate, and the destination selects the best quality paths according to some network metric [41]. In [42], two further localized methods were proposed to build multiple disjoint paths and braided (partly disjoint) multiple paths.
- The source routes the single copy of each packet on different paths per packet, where the paths are selected in a probabilistic or deterministic fashion in order to aid load-balancing, and thus prolong network-lifetime. In this category, centralized [43] (the paths are calculated by the base station) and decentralized approaches [10] (calculation is done by each node independently from each other) can be further distinguished.
- The source splits the original data packet into fragments, adds some redundancy to each fragment, and then sends each fragment on one of the n available paths. As it was studied in [44], if some forward error correcting code is applied that corrects k $(k < n)$ errors, then the method is a kind of trade-off between amount of traffic and reliability: even if some of the fragments were lost, the original message can still be reconstructed due to the added redundancy to each fragment

(i.e., only k fragments are needed at the destination to reconstruct the original message).

Finally, we note that if nodes use omnidirectional antennas (i.e., a single wireless transmission by a node can be received by every node within its transmission range) multi-path routing can reduce energy consumption (i.e., the availability of the routing service) in one-to-one communication over unreliable links [45].

Route reconfiguration: Some routing protocols forward data along a pre-established single path to save energy, and a high delivery ratio is achieved by path repair whenever a break is detected. There are two main approaches. One is that if a path break (failure) is detected, a notification is sent to the source node, which is responsible for finding an alternative path and resending the data packet (like in AODV [46]). This source-initiated approach can be expensive, if a failure occurs many hops away from the source node. Alternatively, nodes can perform path repairing locally. Here, the node having the broken link is responsible for searching alternative paths, and data is forwarded along one of these path. Although the selected alternative path may not be optimal from the view of the source node, the energy is conserved by preventing potential network floods and avoiding long-distance failure notification.

Although some routing protocols incorporate route reconfiguration, there have been proposed some localized methods (e.g., [47] and [48]), which act as separate modules, and can be used in conjunction with some routing protocols.

5.4 Security modules

These modules primarily intends to detect, and prevent or mitigate malicious faults that are caused by the adversary. Although attacks against routing can be very subtle, all of them are built upon the malicious modification or dropping of existing packets, reordering of packet sequences, and the injection of extra packets.

Blacklisting: Blacklisting is used to eliminate either unreliable and lossy links from the set of links used for data forwarding [49, 50, 13], or misbehaving nodes which do not follow the routing protocol (e.g., they maliciously drop, modify packets, or inject extra ones) [21].

When links are blacklisted, all nodes collect statistics about delivery rates with their neighbors, and only the links with reliability higher than a blacklisting threshold are made available for sending and receiving messages. For

instance, it can be implemented in a way that each packet carries a blacklist, a minimal set of degraded-quality links encountered along its path, and the next hop is determined based on both its destination and blacklist. Alternatively, following a decentralized approach, each node locally identifies links to be blacklisted (e.g., based on some link reliability metric described above) and drops incoming and outgoing packets on each link that it determines to have reliability below the specified blacklisting threshold. Blacklisting of misbehaving nodes is usually based on overhearing. In particular, each node continuously monitors its neighbors and checks whether they faithfully forward messages.

Authentication: To protect against malicious manipulations of routing messages, one can employ different cryptographic primitives. Routing protocols can guarantee source and hop-by-hop authentication for routing messages. In the former case, the origin of the message is verified at each intermediate hop and/or at the destination, while in the latter case each hop can verify the authenticity of the immediate sender (i.e., the previous hop). We further distinguish the authentication of broadcast (and multicast) and unicast data.

Broadcast authentication: As many routing protocols rely on flooding or broadcasting routing information, authentication of broadcast data sent by the base station (or rarely by sensor nodes) is a fundamental issue. There exist multiple techniques to achieve broadcast authentication. These include digital signature-based approaches [51] which are usually based on the optimized implementation of traditional signature schemes (like ECDSA [52, 53]), multiple message authentication based approaches [54, 55] where the origin(s) attach multiple MACs to a message from which some are verifiable by a receiver, TESLA-based approaches [56, 57] which use symmetric-key based cryptography exclusively but assume loosely synchronized clocks, and perturbation-based approaches [58] which employ perturbation polynomial based techniques.

Unicast authentication: The authentication of unicast data is ensured by applying conventional message authentication codes (MACs) optimized for resource-constrained sensor motes [56]. Their implementations are usually provided in the data-link layer [59, 60]. A more complex scheme using location-aware keys and MACs is proposed in [61] to provide end-to-end data authentication.

Encryption: Routing protocols can employ encryption to ensure confidentiality. In the topology discovery phase, it is used to conceal topology information like in [14]. In the data forwarding phase, it ensures that the message content

can only be recovered by the intended receivers [61]. Similarly to unicast authentication, the implementation of required cryptographic primitives are usually already provided in the link layer [60, 59]. In the data forwarding phase, it simply prevents intermediate nodes to eavesdrop data packets [62]. A multicast encryption scheme, which supports various multicast group semantics, is proposed in [63].

Module		Real-time delivery	Dependable delivery			
			Availability	Reliability	Security	Maintainability
Low-l.	*Cross-layer module*	√	√	√		
	Cooperative forwarding	√	√	√		
	Cluster-based forwarding	√	√	√		
Cost calc.	*Energy-based cost*		√			
	Distance-based cost	√				
	Content-based cost					
	Link-reliability based cost	√	√	√	√	
	Time-based cost	√				
	Maintenance-based cost					√
Path selection	*Probabilistic selection*		√	√	√	
	Hierarchical selection		√	√		
	Late selection			√		
	Centralized selection	√				
	Route selection towards multiple BS	√	√	√	√	
	Multipath selection	√	√	√	√	
	Route reconfiguration	√	√	√	√	√
Sec.	*Blacklisting*		√	√	√	
	Authentication				√	
	Encryption				√	

Table 1: Routing modules and their objectives.

Module		Protocols
Low-l.	*Cross-layer module*	MACRO [20], SIGF [21], CCMR [4]
	Cooperative forwarding	SPaC [5]
	Cluster-based forwarding	CBF [6], RBP [8], DRB [9], AsOR [7]
Cost calculation	*Energy-based costs*	MACRO [20], SIGF [21], DAMER [45], CCMR [4], Energy Aware Routing [10], GBR [64], TEEN [65], APTEEN [66], PEGASIS [67], GEAR [22], MECN [23], TTDD [68], SAR (DAM) [69], HPAR [70], RPAR [3]
	Distance-based costs	GOAFR [15], GPSR [16], GEDIR [17], GPSVR [18], GDSTR [19], MACRO [20], SIGF [21], CCMR [4], GEAR [22], BVR [31], GLIDER [32], MAP [33], VPCR [34], MECN [23], SPEED [24], MMSPEED [25], VCap [35], ABVCap [36], GFG [26], Hop ID [37], NADV [27], LCLR [28], CLDP [29], ProgressFace [30], VirtualFace [38], RPAR [3], EFS [13]
	Content-based costs	Directed Diffusion [41], GBR [64], IDSQ/CADR [71], Secure DD [72]
	Link-reliability based costs	MT [11], DAMER [45], CCMR [4], NADV [27], EFS [13]
	Time-based costs	TinyLUNAR [39], Secure-TinyLUNAR [73], SPEED [24], MMSPEED [25], RPAR [3]
	Maintenance-based costs	MER [40]
Path selection	*Probabilistic selection*	ARRIVE [74], SIGF [21], Rumor Routing [75], Energy Aware Routing [10], ACQUIRE [76], MM-SPEED [25]
	Hierarchical selection	TEEN [65], APTEEN [66], PEGASIS [67], MECN [23], TTDD [68], SAR (DAM) [69], HPAR [70]
	Late selection	MCFA [77]
	Centralized selection	HPAR [70], INSENS [14]
	Route selection towards multiple BS	INSENS [14], Colored Tree [78], TTDD [68]
	Multipath selection	ARRIVE [74], INSENS [14], Colored Tree [78], SIGF [21], Secure DD [72], Energy Aware Routing [10], Directed Diffusion [41], GBR [64], MMSPEED [25]
	Route reconfiguration	MT [11], Secure DD [72], Directed Diffusion [41], GBR [64], MECN [23], TTDD [68], SPEED [24]
Sec.	*Blacklisting*	ARRIVE [74], SIGF [21], EFS [13]
	Authentication	INSENS [14], SIGF [21], Secure DD [72], Secure-TinyLUNAR [73]
	Encryption	INSENS [14], SIGF [21]

Table 2: Modules and their implementations.

Protocol	Network model						Operational model					
	Base station			Sensor nodes			Communcation pattern			Reporting model		
	Num.	Mobility	Presence	Deployment	Addressing		N2N	N2BS	BS2N	Time	Query	Event
					Query	Response						
Rumor Routing [75]	One	Fixed	*	Random	Data	ID	×	Rev.M.	Anycast	×	Non-agg.	*
MCFA [77]	One	Fixed	*	*	×	×	×	Rev.M.	×	*	×	*
Energy Aware Routing [10]	More	Fixed	*	*	Data	ID	×	Rev.M.	Anycast	*	*	×
Directed Diffusion [41]	More	Limited	Continuous	*	Data	ID	×	Rev.M.	Anycast	*	*	×
GBR [64]	More	Limited	Continuous	*	Data	ID	×	Rev.M.	Anycast	*	*	×
TEEN [65]	One	Fixed	Continuous	Random	Data	ID	×	Rev.M.	Anycast	×	*	*
APTEEN [66]	One	Fixed	Continuous	Random	Data	ID	×	Rev.M.	Anycast	*	*	*
PEGASIS [67]	One	Fixed	Continuous	Random	Data	ID, Location	×	Unicast	Anycast	*	*	×
ACQUIRE [76]	More	Limited	Continuous	*	Data	ID	×	Rev.M.	Anycast	×	Non-agg.	×
IDSQ/CADR [71]	More	Fixed	*	*	Data	ID, Location	×	Rev.M.	Anycast	×	*	×
Geographic Routing [15, 16, 17, 18, 19, 26]	More	Mobile	*	*	Location	Location	Unicast	Unicast	Unicast	Non-agg.	Non-agg.	Non-agg.
GEAR [22]	More	Limited	*	*	Location	Location	Unicast	Rev.M., Unicast	Anycast	Non-agg.	Non-agg.	Non-agg.
MECN [23]	One	Fixed	*	*	×	Location	×	Rev.M.	Anycast	*	×	*
TTDD [68]	More	Mobile	*	*	Location	Location	×	Rev.M.	Anycast	Non-agg.	Non-agg.	×
SAR (DAM) [69]	More	Limited	*	*	×	ID	×	Rev.M.	Anycast	×	×	*
HPAR [70]	One	Fixed	*	*	*	*	×	Rev.M.	*	*	*	*
SPEED [24]	More	Fixed	Continuous	*	Location	Location	*	*	*	Non-agg.	Non-agg.	Non-agg.
TinyOS Beaconing [79]	One	Fixed	*	*	×	ID	×	Rev.M.	×	*	×	*
TinyLUNAR [39]	More	Mobile	*	*	*	ID	*	*	*	Non-agg.	Non-agg.	Non-agg.
Secure-TinyLUNAR [73]	More	Mobile	*	*	*	ID	*	*	*	Non-agg.	Non-agg.	Non-agg.
Virtual Geographic Routing [31, 32, 33, 34, 35, 36, 37]	More	Limited	*	*	Location	Location	Unicast	Unicast	Unicast	Non-agg.	Non-agg.	Non-agg.
INSENS [14]	One	Fixed	*	*	*	ID	*	*	*	*	*	*
Secure DD [72]	More	Limited	Continuous	*	Data	ID	×	Rev.M.	Anycast	*	*	×
ARRIVE [74]	One	Fixed	*	*	×	ID	×	Rev.M.	×	*	×	*
MT [11]	One	Fixed	*	*	×	ID	×	Rev.M.	×	*	×	*
SIGF [21]	More	Mobile	*	*	Location	Location	Unicast	Unicast	Unicast	Non-agg.	Non-agg.	Non-agg.
Colored Tree [78]	More	Fixed	*	*	×	ID	×	Rev.M.	Anycast	*	×	*
MACRO [20]	More	Mobile	*	*	Location	Location	Unicast	Unicast	Unicast	Non-agg.	Non-agg.	Non-agg.
DAMER [45]	One	Fixed	*	*	*	ID	*	*	*	*	*	*
CCMR [4]	More	Limited	*	*	Location	Location	Unicast	Rev.M., Unicast	Anycast	Non-agg.	Non-agg.	Non-agg.
RPAR [3]	More	Fixed	Continuous	*	Location	Location	*	*	*	Non-agg.	Non-agg.	Non-agg.

Table 3: The operational and network model of each module implementation. '×' denotes that a feature is not supported at all by an implementation, while '*' means that all values of a feature are supported.

6 Summary

Existing surveys on sensor network routing hardly support the development of sensor network applications due to their rough operational and network models. Moreover, they tend to neglect dependability concerns as well as routing modules which function only as a part of a routing protocol. In this work, we proposed a modular approach to design routing protocols for sensor network applications, where a routing protocol is a combination of different routing modules and each module has some routing objectives. Following this approach, the main steps of designing a routing protocol are as follows: (1) identification of the routing objectives, (2) selection of routing modules based on the identified objectives such that a module from each core component must be selected (Table 1), (3) identification of the network and operational model of the application, (4) selection of specific module implementations based on the identified network and operational model (Tables 2 and 3), (5) integration of selected implementations.

References

[1] J. N. Al-Karaki, A. E. Kamal, Routing techniques in wireless sensor networks: a survey, IEEE Wireless Communications 11 (2004) 6–28.

[2] K. Akkaya, M. Younis, A survey of routing protocols in wireless sensor networks, Elsevier Ad Hoc Network 3 (3) (2005) 325–349.

[3] O. Chipara, Z. He, G. Xing, Q. Chen, X. Wang, C. Lu, J. Stankovic, T. Abdelzaher, Real-time power-aware routing in sensor networks, in: 14th IEEE International Workshop on Quality of Service (IWQoS)., 2006, pp. 83–92.

[4] M. Rossi, N. Bui, M. Zorzi, Cost and collision minimizing forwarding schemes for wireless sensor networks, IEEE INFOCOM 2007. 26th IEEE International Conference on Computer Communications (2007) 276–284.

[5] H. Dubois-Ferrière, M. Vetterli, Packet combining in sensor networks, Proceedings of the 3rd international conference on Embedded networked sensor systems (2005) 102–115.

[6] Q. Cao, T. Abdelzaher, T. He, R. Kravets, Cluster-based forwarding for reliable end-to-end delivery in wireless sensor networks, IEEE INFOCOM 2007. 26th IEEE International Conference on Computer Communications (2007) 1928–1936.

[7] C. Wei, C. Zhi, P. Fan, K. B. Letaief, Asor: an energy efficient mult-hop opportunistic routing protocol for wireless sensor networks over rayleigh fading channels, IEEE Transactions on Wireless Communications 8 (5) (2009) 2452–2463.

[8] F. Stann, J. Heidemann, R. Shroff, M. Murtaza, Rbp: robust broadcast propagation in wireless networks, Proceedings of the 4th international conference on Embedded networked sensor systems (2006) 85–98.

[9] A. Keshavarz-Haddad, V. Ribeiro, R. Riedi, Drb and dccb: Efficient and robust dynamic broadcast for ad hoc and sensor networks, Sensor, Mesh and Ad Hoc Communications and Networks (SECON) (2007) 253–262.

[10] R. C. Shah, J. Rabaey, Energy aware routing for low energy ad hoc sensor networks, in: Proc. EEE Wireless Communications and Networking Conference (WCNC), Orlando, FL, 2002.

[11] A. Woo, T. Tong, D. Culler, Taming the underlying challenges of reliable multihop routing in sensor networks, Proceedings of the 1st international conference on Embedded networked sensor systems (2003) 14–27.

[12] J. Zhao, R. Govindan, Understanding packet delivery performance in dense wireless sensor networks, in: SenSys '03: Proceedings of the 1st international conference on Embedded networked sensor systems, 2003, pp. 1–13.

[13] K. Seada, M. Zuniga, A. Helmy, B. Krishnamachari, Energy-efficient forwarding strategies for geographic routing in lossy wireless sensor networks, in: SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems, ACM, 2004, pp. 108–121.

[14] J. Deng, R. Han, S. Mishra, Insens: Intrusion-tolerant routing for wireless sensor networks, Computer Communications 29 (2) (2006) 216–230.

[15] F. Kuhn, R. Wattenhofer, A. Zollinger, Worst-case optimal and average-case efficient geometric ad-hoc routing, in: Proc. 4th ACM International Conference on Mobile Computing and Networking, 2003.

[16] B. Karp, H. T. Kung, Greedy perimeter stateless routing for wireless networks, in: Proceedings of ACM Mobicom, 2000.

[17] Stojmenovic, Lin, Loop-free hybrid single-path/flooding routing algorithms with guaranteed delivery for wireless networks, IEEETPDS: IEEE Transactions on Parallel and Distributed Systems 12.

[18] B. Leong, S. Mitra, B. Liskov, Path vector face routing: Geographic routing with local face information, in: Proc. ICNP, , 2005.

[19] B. Leong, B. Liskov, R. Morris, Geographic routing without planarization, in: Proc. NSDI, 2006.

[20] D. Ferrara, L. Galluccio, A. Leonardi, G. Morabito, S. Palazzo, Macro: an integrated mac/routing protocol for geographic forwarding in wireless sensor networks, In Proceedings IEEE INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies 3.

[21] A. D. Wood, L. Fang, J. A. Stankovic, T. He, SIGF: A family of configurable, secure routing protocols for wireless sensor networks, in: Proceedings of the ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN), 2006.

[22] Y. Yu, D. Estrin, R. Govindan, Geographical and energy-aware routing: A recursive data dissemination protocol for wireless sensor networks, UCLA Computer Science Department Technical Report.

[23] V. Rodoplu, T. H. Meng, Minimum energy mobile wireless networks, IEEE Journal Selected Areas in Communications 17 (8).

[24] T. H. et al., Speed: A stateless protocol for real-time communication in sensor networks, in: Proc. International Conference on Distributed Computing Systems, Providence, RI, 2003.

[25] E. Felemban, C.-G. Lee, E. Ekici, Mmspeed: Multipath multi-speed protocol for qos guarantee of reliability and timeliness in wireless sensor networks, IEEE Transactions on Mobile Computing 5 (6) (2006) 738–754.

[26] P. Bose, P. Morin, I. Stojmenovic, J. Urrutia, Routing with guaranteed delivery in ad hoc wireless networks, ACM Wireless Networks 7 (2001) 609?616.

[27] S. Lee, B. Bhattacharjee, S. Banerjee, Efficient geographic routing in multihop wireless networks, in: MobiHoc '05: Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, 2005, pp. 230–241.

[28] Y.-J. Kim, R. Govindan, B. Karp, S. Shenker, Lazy cross-link removal for geographic routing, in: Proceedings of the ACM Conference on Embedded Networked Sensor Systems (SenSys), 2006.

[29] Y.-J. Kim, R. Govindan, B. Karp, S. Shenker, Geographic routing made practical, in: Proceedings of the ACM Symposium on Networked Systems Design and Implementation (NSDI), 2005, pp. 217–230.

[30] C.-H. Lin, S.-A. Yuan, S.-W. Chiu, M.-J. Tsai, ProgressFace: An algorithm to improve routing efficiency of GPSR-like routing protocols in wireless ad hoc networks, IEEE Transactions on Computers, to appear.

[31] R. Fonseca, S. Ratnasamy, J. Zhao, C. T. Ee, D. Culler, S. Shenker, I. Stoica, Beacon-vector routing: Scalable point-to-point routing in wireless sensor networks, in: In Proceedings NSDI, 2005.

[32] Q. Fang, J. Gao, L. Guibas, V. de Silva, L. Zhang, GLIDER: Gradient landmark-based distributed routing for sensor networks, in: Proc. of the 24th Conference of the IEEE Communication Society (INFOCOM), Vol. 1, 2005, pp. 339–350.

[33] J. Bruck, J. Gao, A. Jiang, MAP: Medial axis based geometric routing in sensor networks, in: Proc. of the ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), 2005, pp. 88–102.

[34] J. Newsome, D. Song, GEM: Graph embedding for routing and data-centric storage in wireless sensor networks, in: In Proceedings of ACM SenSys, 2003.

[35] A. Caruso, S. Chessa, S. De, A. Urpi, R. Urpi, Gps free coordinate assignment and routing in wireless sensor networks, in: In IEEE International Conference on Computer Communications (INFOCOM), 2005, pp. 150–160.

[36] M.-J. Tsai, H.-Y. Yang, B.-H. Liu, W.-Q. Huang, Virtual-coordinate-based delivery-guaranteed routing protocols in wireless sensor networks, IEEE/ACM Transactions on Networking 17 (4) 1228?1241.

[37] Y. Zhao, Y. Chen, B. Li, Q. Zhang, Hop ID: a virtual coordinate based routing for sparse mobile ad hoc networks, IEEE Transactions on Mobile Computing 6 (2007) 1075?1089.

[38] M.-J. Tsai, F.-R. Wang, H.-Y. Yang, Y.-P. Cheng, VirtualFace: An algorithm to guarantee packet delivery of virtual-coordinate-based routing protocols in wireless sensor networks, in: IEEE International Conference on Computer Communications (INFOCOM), 2009.

[39] E. Osipov, tinylunar: One-byte multihop communications through hybrid routing in wireless sensor networks, in: New2AN 2007, 2007.

[40] A. Barroso, U. Roedig, C. Sreenan, Maintenance efficient routing in wireless sensor networks, Embedded Networked Sensors, 2005. EmNetS-II. (2005) 97–106.

[41] C. Intanagonwiwat, R. Govindan, D. Estrin, Directed diffusion: a scalable and robust communication paradigm for sensor networks, in: Proc. ACM MobiCom, Boston, MA, 2000.

[42] D. Ganesan, R. Govindan, S. Shenker, D. Estrin, Highly resilient, energy efficient multipath routing in wireless sensor networks, Mobile Computing and Communications Review (MC2R) 8 (2).

[43] Q. Li, J. Aslam, D. Rus, Hierarchical power-aware routing in sensor networks, in: Proceedings of the DIMACS Workshop on Pervasive Networking, 2001.

[44] S. Dulman, T. Nieberg, J. Wu, P. Havinga, Trade-off between traffic overhead and reliability in multipath routing for wireless sensor networks, in: Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), 2003.

[45] Q. Dong, S. Banerjee, M. Adler, A. Misra, Minimum energy reliable paths using unreliable wireless links, Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing (2005) 449–459.

[46] C. Perkins, E. Belding-Royer, S. Das, Ad hoc On-Demand Distance Vector (AODV) Routing, RFC 3561 (Experimental) (Jul. 2003).
URL `http://www.ietf.org/rfc/rfc3561.txt`

[47] J. Deng, R. Han, S. Mishra, A robust and light-weight routing mechanism for wireless sensor networks, 1st Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks (DIWANS).

[48] N. D. T. Georganas, Energy efficient routing with guaranteed delivery in wireless sensor networks, IEEE Wireless Communications and Networking, 2003. WCNC 2003 3.

[49] S. Nelakuditi, S. Lee, Y. Yu, J. Wang, Z. Zhong, G. H. Lu, Z. L. Zhang, Blacklist-aided forwarding in static multihop wireless networks, Sensor and Ad Hoc Communications and Networks, 2005. IEEE SECON 2005 (2005) 252–262.

[50] O. Gnawali, M. Yarvis, J. Heidemann, R. Govindan, Interaction of retransmission, blacklisting, and routing metrics for reliability in sensor network routing, Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004 (2004) 34–43.

[51] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, P. Kruus, Tinypk: Securing sensor networks with public key technology, in: In Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks (SASN), 2004.

[52] A. Liu, P. Ning, Tinyecc: A configurable library for elliptic curve cryptography in wireless sensor networks, in: Proceedings of the 7th International Conference on Information Processing in Sensor Networks (IPSN 2008), SPOTS Track, 2008, pp. 245–256.

[53] K. Ren, W. Lou, Y. Zhang, Multi-user broadcast authentication in wireless sensor networks multi-user broadcast authentication in wireless sensor networks, in: 4th Annual IEEE Communications Society Conference onSensor, Mesh and Ad Hoc Communications and Networks (SECON), 2007, pp. 223–232.

[54] S. Zhu, S. Setia, S. Jajodia, P. Ning, An interleaved hop-by-hop authentication scheme for filtering false data in sensor networks, in: IEEE Symposium on Security and Privacy, 2004.

[55] F. Ye, H. Luo, S. Lu, L. Zhang, Statistical en-route filtering of injected false data in sensor networks, in: IEEE International Conference on Computer Communications (INFOCOM), 2004.

[56] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. D. Tygar, SPINS: Security protocols for sensor networks, Wireless Networks Journal (WINE) 8.

[57] D. Liu, P. Ning, Multi-level μTESLA: Broadcast authentication for distributed sensor networks, ACM Transactions in Embedded Computing Systems (TECS) 3 (4) (2004) 800–836.

[58] W. Zhang, N. Subramanian, G. Wang, Lightweight and compromise-resilient message authentication in sensor networks, in: IEEE International Conference on Computer Communications (INFOCOM), 2008.

[59] C. Karlof, N. Sastry, D. Wagner, TinySec: A link layer security architecture for wireless sensor networks, in: Proceedings of the ACM Conference on Embedded Networked Sensor Systems (SenSys), 2004.

[60] M. Luk, G. Mezzour, A. Perrig, V. Gligor, Minisec: A secure sensor network communication architecture, in: Proceedings of the Sixth International Conference on Information Processing in Sensor Networks (IPSN 2007), 2007.

[61] K. Ren, W. Lou, Y. Zhang, Leds: Providing location-aware end-to-end data security in wireless sensor networks, IEEE Transactions on Mobile Computing 7 (5) (2008) 585–598.

[62] F. Armknecht, D. Westhoff, J. Girao, A. Hessler, A lifetime-optimized end-to-end encryption scheme for sensor networks allowing in-network processing, Computer Communications 31 (4) (2008) 734–749.

[63] K. Ren, W. Lou, S. Jajodia, Secure and efficient multicast in wireless sensor networks allowing ad-hoc group formation, IEEE Transactions on Vehicular Technology 58 (4).

[64] C. Schurgers, M. B. Srivastava, Energy efficient routing in wireless sensor networks, in: MILCOM Proceedings on Communications for Network-Centric Operations: Creating the Information Force, McLean, 2001.
URL http://citeseer.ist.psu.edu/551495.html; http://www.janet.ucla.edu/ curts/papers/MILCOM01.pdf

[65] A. Manjeshwar, D. P. Agarwal, TEEN: a routing protocol for enhanced effeciency in wireless sensor networks, in: Proc. 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, , 200.

[66] A. Manjeshwar, D. P. Agarwal, APTEEN: A hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks, in: Proc. Parallel and Distributed Processing Symposium (IPDPS), , 2002.

[67] S. Lindsey, C. Raghavendra, PEGASIS: Power-effcient gathering in sensor information systems, in: Proc. IEEE Aerospace Conference, , 2002.

[68] F. Ye, H. Luo, J. Cheng, S. Lu, L. Zhang, A two-tier data dissemination model for large-scale wireless sensor networks, in: Proc. ACM/IEEE MOBICOM, , 2002.

[69] Q. Fang, F. Zhao, L. Guibas, Lightweight sensing and communication protocols for target enumeration and aggregation, in: Proc. ACM MOBIHOC, , 2003.

[70] Q. Li, J. Aslam, D. Rus, Hierarchical power-aware routing in sensor networks, in: Proc. DIMACS Workshop on Pervasive Networking, , 2001.

[71] M. Chu, H. Haussecker, F. Zhao, Scalable information-driven sensor querying and routing for ad hoc heterogeneous sensor networks, International Journal of High Performance Computing Applications 16 (3).

[72] H. Yang, S. Wong, S. Lu, L. Zhang, Secure diffusion for wireless sensor networks, in: IEEE International Conference on Broadband Communications, Networks, and Systems (Broadnets), 2006.

[73] G. cs, L. Buttyn, Designing a secure label-switching routing protocol for wireless sensor networks, To appear in Periodica Polytechnica (http://www.pp.bme.hu/).

[74] C. Karlof, Y. Li, J. Polastre, Arrive: Algorithm for robust routing in volatile environments, Computer.

[75] D. Braginsky, D. Estrin, Rumor routing algorithm for sensor networks, in: Proc. First Workshop on Sensor Networks and Applications (WSNA), Atlanta, GA, 2002.

[76] N. S. et al, The ACQUIRE mechanism for efficient querying in sensor networks, in: Proc. First International Workshop on Sensor Network Protocol and Applications, Anchorage, Alaska, 2003.

[77] F. Ye, A. Chen, S. Liu, L. Zhang, A scalable solution to minimum cost forwarding in large sensor networks, in: Proc. International Conference on Computer Communications and Networks (ICCCN), , 2001.

[78] P. Thulasiraman, S. Ramasubramanian, M. Krunz, Disjoint multipath routing to two distinct drains in a multi-drain sensor network, IEEE International Conference on Computer Communications (INFOCOM).

[79] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, K. Pister, System architecture directions for networked sensors, in: Proceedings of the International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), 2000.