Network Working Group
Technical Report: 453
Category: Experimental

A. Klein
University of Wuerzburg

October 2008

Statistic-Based Routing (SBR)

Status of this Memo

This technical report defines an Experimental Protocol for the wireless mesh, sensor, and ad hoc community. Discussion and suggestions for further improvement are strongly requested. Its distribution is unlimited.

Copyright Notice

General Notice

Many mechanisms are still subject to change. Please check the following web page for latest changes. http://www.routingprotokolle.de

Abstract

The Statistic-Based Routing (SBR) protocol has been originally designed to meet the requirements of sensor networks. During the simulation and experimental phase it soon turned out that the protocol represents a good choice for mobile wireless mesh and ad hoc networks as well. The key characteristics of the protocol are high end-to-end reliability (in fix and mobile networks), load balancing capabilities, smooth continuous routing metrics, quick adaptation to changing network conditions, low processing and memory overhead, support of unidirectional links, and simplicity.

Table of Contents

1. Introduction

The Statistic-Based Routing (SBR) protocol generates reliable end-to-end routes in highly mobile multi-hop wireless networks. It can be configured to operate like a hybrid or a proactive routing protocol depending on the capabilities and the requirements of the network. The protocol uses a continuous adaptive metric to balance the traffic load evenly in the network. Due to the continuous adaptive metric, acceptable performance is achieved even for non optimized configurations. The metric is used to calculate a forwarding delay which allows the modification of the routes in the network. The advantage of the delay based approach lies in the fact that any kind of routing metric can be used. Moreover, the protocol is able to detect link breaks and unidirectional links within a short amount of time making it an attractive choice for indoor and mobile scenarios.

Like other routing protocols SBR uses unique sequence numbers for each destination. Thus, each flooding sequence uses the same sequence number for differentiation. The usage of sequence numbers in combination with a hop count field represent the simplest way to prevent routing loops.

2. Overview

SBR defines two types of routing messages which are passed to the underlying mac and physical layer. Due to the fact that the latest available sensor nodes are able to support Internet Protocol (IP) we focus in the following on the implementation of the protocol on top of the IP stack. Hello Messages (HM) and Short Hello Messages (SHM) are transmitted and received via UDP. Thus, the protocol uses the IP addresses to differentiate the nodes in the network. The messages are broadcasted by using the IP broadcast address. The dissemination of the messages is limited by using a predefined Time-To-Live value which is set in the IP header. However, it is also possible to use multicast addresses to further limit the flooding.

The protocol can operate either in proactive or in hybrid mode. In the proactive mode all nodes in the network periodically transmit hello messages which are disseminated in the network. A node receiving a hello message, rates the neighbor through which the message was received by using a cumulative function. The node stores the calculated value in its routing table. If a node wants to transmit a packet to a destination in the network it sends the packet to its neighbor with the highest routing entry.

Thus, the routing entries can be regarded as gradient pointing towards the destination. A cumulative continuous metric is used to differ routes with equal hop length. Due to the cumulative metric more reliable links are preferred over less reliable links. Packets are forwarded along the reverse route of the hello messages. Therefore, the used links have to be bidirectional which makes an additional mechanism necessary to provide end-to-end connectivity if unidirectional links are present.

In hybrid mode no hello messages are generated in the absence of data traffic. Thus, it significantly reduces the amount of routing overhead in networks with low data rate and event triggered communication. In the case that a node wants to transmit data packets to another node for which it does not know a next hop it starts to send out hello messages which cover the function of route requests. Intermediate nodes forward the message if the message is considered to be new. These requesting hello messages contain the address of the destination. If a node recognizes its own address in a hello message it starts to transmit hello messages by itself which represent the reply of the destination. The originating node stops the transmission of requesting hello messages if a hello message from the destination is received. A destination node stops the transmission of hello messages in the case that it does not receive any data packet for a duration longer than active route timeout which is set by default to three times the hello message interval.

Short Hello Messages are used by the protocol to detect unidirectional links. These messages are similar to ordinary hello messages. The major difference is represented by the TTL value which is set to two. As a consequence one hop neighbors forward the message whereas two hop neighbors discard the message because of the TTL value of zero. The link to a neighbor is assumed to be bidirectional if the originating node recognizes that the neighbor forwards its hello messages. If no message is forwarded by a neighbor for a certain amount of time, the link to this neighbor is marked as unidirectional. Hello messages that are received via a unidirectional marked link are discarded without further evaluation.

3. SBR Terminology

2-hop neighbor

All nodes that can be reached by a node X via exactly two hops.

active route

The term active route is used if the protocol is in hybrid mode. If a node receives a data packet for which it is the final destination or a hello message with its own address in the destination field, it (re-)starts the active route timer. The node has at least one active route as long as the timer is pending. Furthermore, the node transmits hello messages if it has an active route.

address

Address is a unique label of a participating node in the network. Due to the fact that most networks use the IP on the network layer we use the term address as a synonym for IP address, too.

best neighbor

The neighbor of node X with the highest routing entry in for a destination Y is called best neighbor of node X for node Y.

bidirectional link

A link is called bidirectional if it connects two nodes X and Y such that node X hears node Y and node Y hears node X. Keep in mind that the term bi-directional does not imply the same link quality in both directions.

broadcast

Broadcasting means transmitting a packet to all one hop neighbors of a node.

flooding

Flooding means transmitting a packet to all nodes within the network. However, we assume an intelligent flooding such that packets are only forwarded if they are considered new and received by the best neighbor as specified in section 6.10.

forwarding node

A node that agrees to forward messages and packets destined for another node, by retransmitting them to a next hop according to its information stored in the routing table.

forward route

A route set up to send data packets from a node originating a Route Discovery operation towards its desired destination.

invalid route

A route that has expired, denoted by a state of invalid in the routing table entry. An invalid route is used to store previously valid route information for an extended period of time. An invalid route cannot be used to forward data packets, but it can provide information useful for route repairs, and also for future RREQ messages.

neighbor node

A node X is a neighbor of node Y if node Y can hear node X.

originating node

A node that creates and transmits a new hello message is referred to as originating node of the message.

passive node

A passive node does not forward routing messages. However, passive nodes rate incoming messages to build up their routing entries. Furthermore, it does not forward any data packets. Thus, a passive node only can generate and transmit its own data packets.

sequence number

A monotonically increasing number maintained by each originating node. A node increases its sequence number by one before generating a new hello message. The sequence number is used in combination with the time-to-live by nodes in the network to distinguish hello messages.

uni-directional link

A link is called uni-directional if two nodes X and Y communicate via that link such that node X hears node Y but node Y does not hear node X or vice versa.

valid route

See active route.

4. Applicability Statement

The SBR protocol is designed to provide good performance under various conditions. It can be configured to achieve high throughput and reliability in networks with high mobility and high data rate due to its load balancing capabilities and short reaction time. It is also possible to use it in low data rate networks or even in wireless sensor networks with asynchronous sleep times. The continuous metric makes it applicable to operate in many different scenarios. If energy efficiency plays a major role we strongly recommend that the protocol is configured to operate in hybrid mode which reduces overhead in a significant way. Especially in the case that there is only a small number of data sinks in the network. Scalability represents a serious issue for routing protocols that use broadcasting mechanisms to disseminate routing messages in the network. In low data rate networks with a high node density it is possible to further reduce the overhead if not all nodes participate in the forwarding of hello messages. These passive nodes can be used in heterogeneous networks to build a backbone of active nodes which is used as infrastructure by the passive nodes.

Scalability

Scalability represents a serious issue in large networks with low data rate. However, typical networks like IEEE 802.11 provide a data rate that is sufficient to support up to several hundred nodes

even if the protocol is operating in proactive mode with a short hello message interval of 1.0 second. Nevertheless, routing overhead should always be kept as small as possible. Therefore, we recommend the hybrid mode since it achieves nearly the same performance as the proactive mode. The overhead in hybrid mode increases linearly with the number of nodes and the number of data sinks in the network.

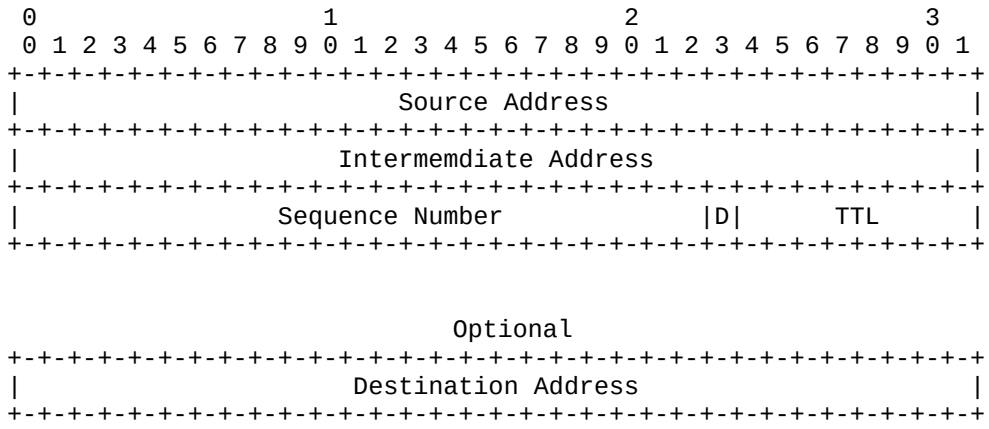
Consider, a network consisting of 100 nodes with a single data sink. In hybrid mode only the data sink would broadcast messages whereas all 100 nodes would transmit messages if the proactive mode is used. Thus, the overhead that the protocol generates in this example in the hybrid mode is one percent of the overhead that is generated in the proactive mode. If the single source would permanently transmit a hello message every second the maximum recognize routing overhead in a worst case scenario would be 9600 bits per seconds which is quite acceptable for a network with 100 nodes.

5. Message Formats

The protocol uses two types of messages which are usually encapsulated as payload in a UDP packet.

5.1 Hello Message Format

The basic layout of a hello message in SBR is as follows (omitting IP and UDP headers):



Source Address

The source address represents the IP address of the originator of the message.

Intermediate Address

The intermediate address field is used by intermediate nodes to store their IP address in the packet before forwarding.

Sequence Number

The originator of the message assigns a unique identification number that is stored in the 23 bits long Sequence Number field. This number is inserted into the message and increased by one for each new hello message. Intermediate nodes do not change the Sequence Number field in a message. The Sequence Number and the TTL allow to distinguish received messages to prevent unnecessary retransmission of the message.

D

In the case that the protocol operates in the hybrid mode it is necessary to inform the destination that it should transmit hello messages. Thus, the D bit is used to indicate whether a destination field is appended to the hello message which holds the IP address of the destination. If the D bit is set to one a Destination Address is appended to the message. Otherwise, the protocol does not check the destination field.

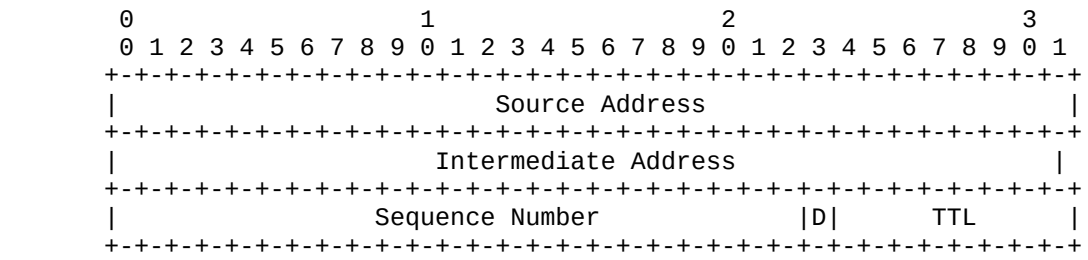
TTL

The Time-To-Live (TTL) field represents the number of allowed retransmissions of the message. It is used to differentiate messages and to prevent infinite retransmission of a message. Furthermore, it can be used to limit the forwarding in the network. Thus, overhead can be significantly decreased.

Destination Address

The Destination Address field is only present if the protocol is in the hybrid mode. It is used by a data source to inform the data sink to transmit hello messages which is required to build up routing tables. Hello messages with a destination field cover the function of route requests. Messages without a destination field are used as route replies.

5.2 Short Hello Message Format



Source Address

The source address represents the IP address of the originator of the message.

Intermediate Address

The intermediate address field is used by intermediate nodes to store their IP address in the packet before forwarding.

Sequence Number

The Sequence Number in the Short Hello Message is the same Sequence Number as specified in the hello message. The value is also increased before a Short Hello Message is transmitted.

D

The D field is always set to zero since Short Hello Messages are not used build end-to-end routes.

TTL

The Time-To-Live field covers the same function as specified in the hello message. The difference to hello messages lies in the that the value is usually set to two since Short Hello Messages are mainly used to increase the capability of the protocol to detect unidirectional links.

6. SBR Operation

In this section the behavior of the protocol in proactive and in hybrid mode are described. First, the mandatory and optional configuration parameters are introduced to give a better understanding of the features of the protocol. After introducing these parameters the generation of routing messages and the maintenance of routing tables are specified. Furthermore, the way how the routing and data messages are handled depending on the state and the configuration of the protocol is described. We focus on the default values of the parameters which provide a good performance in many different scenarios. However, it is clear that they can be used to tweak the protocol in order to meet the desired requirements.

In the following we assume that all routing messages are sent to port 654 using UDP.

6.1. Mandatory Configuration Parameters

The parameters that are introduced in this sub section are required to configure the basic functions of the protocol. In Section 6.1.1. the minimum configuration is shown if the protocol is run in the proactive mode. The hybrid mode requires two additional parameters which are described in Section 6.1.2. Besides the basic functions advanced features can be enabled. Their configuration is introduced in Section 6.2.

6.1.1 Required - Parameters

Six configuration parameters have to be set of the SBR protocol to operate in the proactive mode.

Hello Message Interval

The Hello Message Interval (HMI) specifies the time between two consecutive hello message transmissions. The default value is 2.0 seconds.

Decrease Routing Value Interval

The Decrease Routing Value Interval (DRVI) specifies the time interval at which the Decrease Routing Value Function is called. The interval is set by default to 3.0 seconds.

Increase Routing Value Function

The Increase Routing Value Function (IRVF) is used to modify an existing routing entry. The Equation 3 is used per default.

$$I_{n+1} = 2I_{n} + \frac{4}{I_{n}^2 + 1} \qquad \text{(Eq.3)}$$

I_{n+1} represents the new value whereas I_{n} is the previous value. The function is called each time a new hello message is received via neighbor.

Decrease Routing Value Function

The Decrease Routing Value Function (DRVF) is used to limit the increase of the routing entries.

$$D_{n+1} = \frac{D_{n}}{2} \qquad \text{(Eq.4)}$$

D_{n+1} represents the new value whereas D_{n} is the previous value.

Hello Message TTL

The Hello Message Time-To-Live value limits the number of retransmission. It should be set to the net diameter to allow communication between all nodes in the network. The default value is set to 16.

Maximum Routing Value

The Maximum Routing Value (MRV) is required to define an upper bound of the routing entries. Thus, it prevents the infinite increase of the values which is necessary to improve the reaction time of the protocol to topology changes.

6.1.2. Hybrid Mode - Parameters

The hybrid mode of the SBR protocol requires two additional parameters in order to work properly.

Active Route Timeout

The Active Route Timeout (ART) defines the amount of time that a node assumes any route to be active/valid without receiving any data packets. As long as the ART is pending the node will periodically transmit hello messages. If the timer expires the node stops the transmission of hello messages in order to reduce routing overhead.

Hello Message Retransmission

Hello Message Retransmission (HMR) is the maximum number of requesting hello messages that are sent out by a node which wants to transmit data packets to another node. If no hello message from the destination is received after HMR hello messages the destination is assumed to be unreachable. The requesting node stops the transmission of hello messages if it receives a hello message from the destination or the maximum number of hello message retransmissions is reached. The HMR default value is three.

6.2. Optional Configuration Parameters

In addition, SBR offers possibilities besides the previously introduced functionality that to improve its performance. The following three sub sections describe these additional features and their configuration.

6.2.1. Routing Metric

The SBR protocol offers a smooth possibility to affect the routes that are used by the protocol. Every kind of routing metric can be used due to the fact that the protocol uses a cumulative IRVF and only considers the first arrival of hello messages. Thus, the routes can be modified if nodes defer the forwarding of hello messages depending on a predefined routing metric. Typical metrics consider e.g. the number of hops, the link utilization, the link costs, the absolute node speed, the relative node speed, the geographic distance to a certain point, the hardware capabilities, the battery power, or simply the current routing entry value through which the corresponding hello message was received to calculate a forwarding delay. The route with the lowest delay and the highest reliability is used in the case that the messages are forwarded without any delay.

Forwarding Delay

The forwarding delay of hello messages should be limited to the quotient of the HMI and the minimum of the net diameter and the hello message ttl. The maximum delay is required to ensure that only one hello message of a node is flooded at a time. Otherwise, an originator would send a new hello message while its previous hello message is still on its way through the network.

Forwarding Delay Function

Any function can be used to calculate the delay as long as the returned values are larger than zero and smaller than the maximum forwarding delay.

6.2.2. Unidirectional Links

Links are usually bidirectional in wired networks. However, in wireless networks especially in wireless sensor and ad hoc networks nodes have to deal with the problem of unidirectional links. Thus, a routing protocol for wireless networks has to be able to detect unidirectional links to route data traffic according to the capabilities of the links in the network.

SBR protocol tries to avoid unidirectional links as these links are often unreliable in wireless networks. A mechanism similar to acknowledgements is required to check if a link is unidirectional or bidirectional. Instead of using acknowledgements the nodes listen to the air interface in order to find out whether their neighbors forward their hello messages. If a node receives its own hello message with a TTL value of hello message TTL - 1, it marks the link to the neighbor as bidirectional. A link to a neighbor is marked as unidirectional if no hello message is forwarded by the neighbor for a duration longer than neighbor expiration interval.

Short Hello Message

A node periodically transmits Short Hello Messages if this parameter is enabled. Short Hello Messages are disabled by default.

Short Hello Message Interval

The Short Hello Message Interval defines the time between two consecutive SHM transmissions. A default value of one second is used.

Short Hello Message TTL

The maximum number of retransmissions of hello messages is specified by the Short Hello Messsage time-to-live. The default value is two. Therefore, only one hop neighbors forward the short hello message. However, larger values lead to more detailed knowledge of the topology around a node which can be helpful in case of high mobile networks.

Communication between two neighbors is not possible in the case that both mark the link between them as unidirectional. This error can not be resolved immediately since both nodes will not forward the hello message of the other node. As a consequence, the routing value of the links will decrease until they are removed from the routing tables. If

6.2.3. Advanced Mobility Support Parameters

a hello message is received from a node which is not in the table, the link to this node is set to bidirectional.

Neighbor Expiration Interval

The Neighbor Expiration Interval (NEI) defines the time interval after which the link to a neighbor is marked as unidirectional if the neighbor does not forward hello messages of the node.

Observation Interval

The Observation Interval is the interval during which changes in the neighbor list are counted. The adding and the deletion of neighbors are counted as changes. The counted value is used as input for the forwarding delay calculation c.f. 6.3. For that reason, the interval has a large impact on the performance since its duration mainly affects the neighborhood change and thus the forwarding delay of the routing messages. The duration has to be chosen in respect to the topology change and link break rate. Duration of twice the hello message interval is used by default since this value provides good performance for many scenarios. It has to be kept in mind that the duration affects the time which is required by the protocol to recognize changes in the neighborhood.

6.3. Mobility Routing Message Forwarding Delay

The end-to-end reliability in wireless networks strongly depends on the mobility of the network. The faster the speed of the nodes, the more link breaks occur in the network. An approach is to take advantage from nodes with correlated movement since relative movement speed is mainly responsible for link breaks. These nodes should be selected as next hop due to their more reliable links as a consequence of their correlated movement. The problem is to detect the correlated node movement if no position information is available.

Thus, a metric is required that is used to estimate the current relative movement speed of a node. Each node is able to estimate its speed by keeping track of the presence of its surrounding nodes. A change in its neighborhood indicates that the node has moved away from the other nodes or the other nodes are moving away from it.

The basic idea is to defer the forwarding of routing messages depending on the change of the neighborhood. More changes in the neighborhood result in a higher delay of the routing messages. Therefore, the routing protocol has to choose nodes with a lower

relative node speed since these nodes forward routing information more quickly. It is obvious that a mobile node or a cluster of mobile nodes with correlated movement may have peaks in their neighborhood change if they move through certain areas e.g. crossing of a road or an area of high node density. Thus, a mechanism is required to reduce the variation of the metric and make it robust against short temporary changes. The exponential weighted moving average algorithm is used to minimize the impact of peaks. The neighborhood change metric is calculated according to the following equation.

$$e_t = \alpha * e_{t-1} + (1-\alpha)*X_t, \quad \alpha = 0.9 \quad \text{(Eq.5)}$$

The chosen smoothing factor alpha represented the best trade-off between reaction time and peak suppression in the simulated scenarios. X_t is the number of changes in the neighbor list during the last observation interval.

6.3.1. Neighborhood Change Detection

Changes in the neighbor list are counted during each observation interval. The counter is increased by one each time a node is added to the list or removed from it.

6.3.2. Neighborhood List

The neighborhood list consists of neighbor entries. Each entry stores information about the neighbor e.g. time of last contact. If a node receives a packet for another node it checks whether the originator of the packet is in the list. In the case that the node is not in the list a new entry is created and inserted. Otherwise, the existing corresponding entry is updated.

6.3.3. Neighbor Expiration

The NEI time has to be chosen carefully since it depends on the traffic pattern. Each node keeps track of its surrounding nodes by periodically transmitting hello messages. To minimize changes in the neighbor list if some nodes are temporarily unavailable, the neighbor expiration time is set by default to four times the duration of the hello message interval.

6.3.4. Mobility Routing Message Forwarding Delay Calculation

The time a node defers the forwarding of a routing message is in the following referred to as forwarding delay. The delay delta is calculated from the neighborhood change metric e, of the last observation interval according to the following equation.

$$delta = \frac{hmi}{lambda} * \left(1 - \frac{phi}{e + phi} \right) \qquad \text{(Eq.6)}$$

The quotient of the hello message interval hmi and lambda represents the maximum forwarding delay. Thus, lambda covers the function of a delay limiter. The second factor of equation 6 is influenced by phi, and is used to divide the maximum forwarding delay into smaller steps. A smaller phi value increases the delay for a smaller number of neighbor changes. A default phi value of ten is used since it results in a good accuracy of differentiation in a large spectrum of neighbor list changes. The additional delay has to be chosen according to the net diameter in number of hops, the underlying medium access layer, and the traffc load of the network. In most scenarios, an additional delay of several milliseconds is quite sufficient to modify the topology of the network. The impact on the end-to-end delay of data traffc is minimized due to the fact that only routing messages are deferred.

6.4. Route Table Entries

The Routing Table Entries represent the quality of the link towards the corresponding destination. Due to the cumulative metric a higher value indicates a better link quality. If a node receives a new hello message from one of its neighbors it searches for the corresponding entry in the table. In the case that no entry exists a new entry is created and inserted in the list. The routing entry consists of a double value which represents the link quality, a boolean indicating whether the link to this neighbor is unidirectional or bidirectional, and the sequence number of the destination. To create the first routing value, zero is used as input for the IRVF resulting in a value of four. If the routing value of an entry becomes lower than the minimum routing value of 0.2 it is removed from the table since the link is assumed to be broken.

6.5. Maintaining Sequence Numbers

Every node has its own sequence number. The sequence number is increased by one before a hello message or a short hello message is transmitted. The maximum sequence number is 8388608 (2^23) resulting from the 23 bit size of the sequence number field. If the maximum value is reached the sequence number is reset to zero.

The entries in the routing table contain the sequence number of the corresponding destination. These sequence numbers are only modified if new hello messages or short hello messages are received. If an incoming message is assumed to be new, the sequence number of the routing entry is set to the value of the message. Incoming messages are considered as new if the sequence number in the message is larger than the number that is stored in the table.

6.6. Generating Periodic Hello Messages

A node periodically transmits hello messages if the protocol is set to proactive mode. In addition, hello messages are periodically transmitted in the case that the protocol is in hybrid mode and the node has at least one active route.

The originating node places its own address in the Source Address and the Intermediate Address field. The sequence number is increased by one and inserted into the Sequence Number field. The D field is set to zero and the TTL field is set to hello message ttl.

6.7. Generating Request Hello Messages

Request hello messages are only generated if the protocol is in hybrid mode and a node wants to establish a route to a destination. The generation of request hello messages is similar to the generation of periodic hello messages. Except the D field which is set to one to indicate that this is a request hello message with a Destination field. The address of the destination is stored in the Destination field.

6.8. Establishing a Route

Routes are only established if the protocol is used in the hybrid mode. Otherwise, routes do not have to be established since the nodes in the network periodically transmit hello messages in proactive mode

even in the absence of traffic. If a node is in hybrid mode and receives a packet from the higher layer dedicated for a destination for which it does not have a valid next hop, it starts the establish process.

Therefore, requesting hello messages are generated and broadcasted as described in 6.7. The node keeps on broadcasting requesting hello messages periodically every HMI until it receives a response from the destination or the maximum number of requesting hello message transmission is reached. The maximum number of retransmissions is specified by the HMR.

Only one route establish process should be active at a time to limit the routing overhead since requesting hello messages are sent in addition to periodic hello messages. In the case that the routing protocol receives a packet for a destination for which it does not have a valid next hop, it stores the packet in its waiting queue. Furthermore, it starts the route establish process for that destination as soon as the current process has finished.

6.9. Generating Short Hello Messages

Short hello messages are periodically transmitted by a node if the protocol is in proactive mode and short hello messages are enabled. The messages are transmitted every SHMI. A node places its own address in the Source Address and the Intermediate Address field. The D bit is set to zero and the ttl is set to the configured short hello message ttl which is usually set to two. The main purpose of SHMs is to improve the detection of unidirectional links and to reduce the time the protocol needs to detect link breaks in its one hop neighborhood.

6.10. Forwarding of Short Hello Messages and Hello Messages

A hello message or a SHM is only forwarded if it is received by the neighbor with the highest routing entry towards the originator of the hello message. Messages that are received via a unidirectional link are discarded without further evaluation. If the link is bidirectional the receiving node compares the address that is stored in the intermediate field with the best neighbor address. Furthermore, the ttl value in the message has to be higher or equal than one. Otherwise, the message is discarded.

The received hello message is forwarded if the message passes the following tests.

* Bidirectional

* Received by the best neighbor

* TTL higher than zero

The node inserts its own address in the intermediate field and decreases the ttl field by one before forwarding the message.

6.11. Forwarding Data Packets

If a node receives a data packet it reads the destination field of the packet in order to find out whether this packet is dedicated for itself or for another node. In the case that the packet has to be 0forwarded, the node looks up the routing entry with the highest routing value towards the destination and forwards the packet to the corresponding neighbor. If several routing entries have the same routing value, the next hop is randomly chosen from one of the highest entries. The received packet is discarded if no valid routing entry for the destination is stored in the table.

6.12. Passive Nodes

In dense large networks where nodes are very limited in their capabilities due to energy limitation or data rate of the interface most of the nodes can be set to passive mode to improve the performance. Passive nodes distinguish from ordinary nodes as they do not forward routing messages. The consequence of this passive behavior is that other nodes do not chose these nodes as best neighbor. However, even passive nodes broadcast hello messages in proactive mode to enable other nodes to send them data packets.

Passive nodes have to be selected such that the network is still connected. The active nodes build then a backbone which can be used by all nodes in the network.

7. Proposed Configurations

Different configurations are introduced in this section. These configurations provide a good performance in most scenarios. Nevertheless, they only represent a starting point for further optimization.

7.1. Default Configuration

The default configuration represents a good choice for typical wireless sensor networks. We assume that the used wireless interface has a maximum data rate of 256 kb/s, the network has an average of five nodes and consists of up to 100 nodes. Furthermore, most of the nodes are fix or move slowly and the reliability of the links is relatively high.

Parameter Name	Value
Hybrid Mode	
Active Route Timeout	1,0 Seconds
Hello Message Interval	2,0 Seconds
Decrease Routing Value Interval	3,0 Seconds
Increase Routing Value Function	Eq.
Decrease Routing Value Function	Eq.
Hello Message TTL	16
Maximum Routing Value	20
Hello Message Retransmission	3
Routing Metric	None
Unidirectional Links	enabled
Short Hello Message	enabled
Short Hello Message Interval	2,0 Seconds
Short Hello Message TTL	2
Passive Mode	disabled

7.2. High Data Rate Wireless Networks

The High Data Rate (HDR) configuration is optimized for networks that consist of networks with nodes that provide > 1 Mbit/s interfaces. Additionally, the number of nodes should be limited to 64 nodes in order to keep the overhead on a low level. To minimize the reaction time of the protocol it should run in proactive mode. For indoor scenarios we strongly recommend to enable the support for unidirectional links and the transmission of short hello messages. No specific routing metric is required in such networks since the protocol selects the next hop in respect to delay and reliability if none is chosen as routing metric.

Parameter Name	Value
Proactive	
Hello Message Interval	1,0 Seconds
Decrease Routing Value Interval	1,5 Seconds
Increase Routing Value Function	Eq.
Decrease Routing Value Function	Eq.
Hello Message TTL	16
Maximum Routing Value	30
Routing Metric	None
Unidirectional Links	enabled
Short Hello Message	enabled
Short Hello Message Interval	1,0 Seconds
Short Hello Message TTL	2
Passive Mode	disabled

7.3. Mobile Wireless Networks

The configuration that is introduced in this sub section is optimized for mobile and high mobile networks that provide a data rate of approximately 1 Mbit/s and have an average node density of up to 10 nodes. Additionally, the number of nodes should be limited to 64 nodes in order to provide high performance. All settings are similar to the configuration which is shown in 7.2.. However, the routing metric should be set to mobile to increase the reliability by approximately 10 to 20 percent since the protocol chooses nodes for forwarding that have small changes in their neighborhood.

Parameter Name	Value
Proactive	
Hello Message Interval	1,0 Seconds
Decrease Routing Value Interval	1,5 Seconds
Increase Routing Value Function	Eq.
Decrease Routing Value Function	Eq.
Hello Message TTL	16
Maximum Routing Value	30
Routing Metric	Mobility (c.f. 6.3.)
Unidirectional Links	enabled
Short Hello Message	enabled
Short Hello Message Interval	1,0 Seconds
Short Hello Message TTL	2
Neighbor Expiration Interval	2,5 Seconds
Observation Interval	1,5 Seconds
Passive Mode	disabled

7.4. Low Power Low Data Rate Networks

Low power low data rate networks usually have an interface that provides a maximum transmission rate of 32 kb/s and often consist of more than 100 nodes. Furthermore, nodes are usually fixed and have asynchronous sleep times in order to save as much energy as possible. Due to these constraints we strongly recommend to use the hybrid mode in combination with long time intervals for the active route timeout, the hello message interval, and the decrease routing interval. The forwarding of hello messages should be done depending on the battery capacity that is available. Thus, a node should delay the forwarding of hello messages or even switch to passive mode if too much energy is drained from the battery. The following configuration is just a starting point since low power sensor networks may differ significantly in their demands on the routing protocol.

Parameter Name	Value
Hybrid	
Active Route Timeout	10,0 Seconds
Hello Message Interval	20,0 Seconds
Decrease Routing Value Interval	30,0 Seconds
Increase Routing Value Function	Eq.
Decrease Routing Value Function	Eq.
Hello Message TTL	32
Maximum Routing Value	20
Routing Metric	Battery Capacity
Hello Message Retransmission	5
Unidirectional Links	enabled
Short Hello Message	disabled
Passive Mode	Battery Threshold

7.5. Development

The development configuration only covers the basic parameters of the protocol. We recommend implementing the proactive mode in combination with linear routing value increase and decrease functions to simplify debugging. Thus, an initial value of zero is used and the minimum value is set to zero.

Furthermore, large HMI and DRVI should be used such that the routing entry values in the table increase slowly (HMI slightly smaller than the DRVI). Routing messages should not be deferred during development since the deferring of messages requires all other protocol mechanisms to operate properly.

Parameter Name	Value
Proactive	
Hello Message Interval	5,0 Seconds
Decrease Routing Value Interval	10,0 Seconds
Increase Routing Value Function	Linear increase by one(init value = 0)
Decrease Routing Value Function	Linear Decrease by one(minimum = 0)
Hello Message TTL	16
Maximum Routing Value	10
Routing Metric	None
Unidirectional Links	disabled
Short Hello Message	disabled
Passive Mode	disabled

8. Security Considerations

Currently, SBR does not specify any special security measures. However, in the following we specify several types of attacks, their impact on the network, and possible ways to detect or to minimize the impact that an intruder might have on the network.

8.1 Rebuild and Broadcasting of Hello Messages

An intruder can generate massive routing overhead and routing errors if he is able to transmit valid hello messages. This requires the following knowledge of the network.

- Access to the network

- Valid Node Address

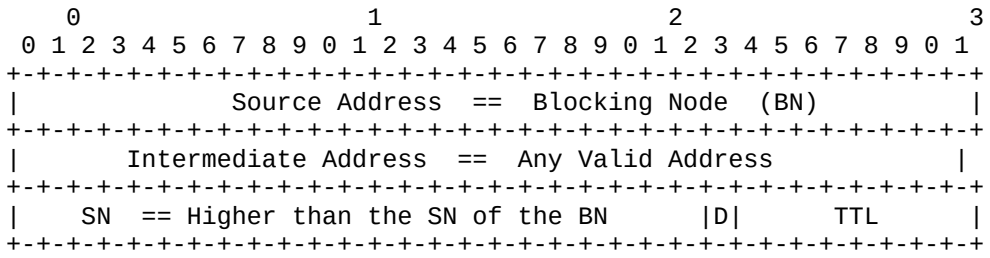
- Error Node Address

- Knowledge of the current sequence number

Using such knowledge an intruder can rebuild any type of hello message. Thus, the intruder can manipulate the routing entries of nodes in the network.

8.2 Blocking of Nodes

Consider a scenario in which the intruder broadcasts hello messages using the address of another node in the network in combination with a high sequence number. The neighbor nodes that receive the message will consider this message as new and will increase their routing entries and forward the message. A modified hello message may look like this.



However, the increase of the routing entries that indicate the next hop towards the destination represent a secondary problem. The main problem is that the forwarding nodes will use the new sequence number to verify if an incoming hello message from this originator is new or not. As a consequence, intermediate nodes will discard hello messages originated by the BN since their sequence number is lower than the one that is stored in the routing entries of the intermediate nodes. There are several possibilities to detect the manipulation by an intruder.

The BN can recognize the manipulation when it receives a hello message with its own address in the source address field and a sequence number which is higher than its own sequence number. An intelligent intruder would therefore broadcast modified hello messages with a ttl smaller than the distance in number of hops from itself to the BN. The distance to the BN can be simply discovered by listening for hello messages originated from the BN. Therefore, the BN can not detect the intruder since the modified hello messages do not reach it.

An intruder can be detected by intermediate nodes if the nodes recognize a significant increase in the sequence number in combination with an increased hello message rate. Furthermore, intermediate nodes will alternately receive valid and invalid hello messages from the same originator which is a clear sign that an intruder tries to manipulate the network.

8.3 Jamming of Hello Messages

If an intruder manages it to successfully sign on to the network, he is able to flood the network by frequent transmission of hello messages. The jamming of messages represents the easiest way to harm the network. However, its also the modification which is very simple to recognize. Nodes in the network have store a threshold which specifies the maximum allowed frequency of hello message transmission. In the case that a node exceeds the threshold for hello message transmission no further hello messages are forwarded for this originator. Such a feature limits the impact that the intruder has on a single node.

8.4 Passive Jamming

Low power low data rate networks are very limited in terms of available energy and bandwidth. Therefore, these two constraints represent their weak points. In general, the protocol will be configured such that it operates in hybrid mode to save both resources as much as possible. An intruder that has successfully registered to the network and knows the addresses of the nodes in the network is able to transmit requesting hello messages. Recall, that a node in hybrid mode will start to transmit hello messages if it recognizes its own address in the destination field of a new hello message. Thus, the intruder is able to remotely trigger the transmission of hello messages by another node by using requesting hello messages.

Passive jamming can be limited if the nodes use a short active route time out. If the modified node does not receive any data packet, it will only transmit up to three hello messages until the transmission is stopped.

Furthermore, the impact can be limited if the forwarding of requesting hello messages is limited by a certain threshold. In the case that the intruder does not have a valid address it has to use the address of another node in the network. This usage than leads to repeated invalid sequence numbers which represent an indication of an intruder. The manipulation range of the intruder is limited by its distance towards the node from which it is using the originator address. Otherwise, the node will notice that there is an intruder in the network by recognizing its own address in a routing message which was not transmitted by itself.

9. Acknowledgments

We acknowledge Dirk Staehle from the wireless working group at the University of Wuerzburg and Prof.Dr.P.Tran-Gia for their inspiring input regarding several protocol mechanisms. Furthermore, we like to thank Christoph Aultizky and Falk Schubert for their discussions regarding the mobility support mechanism.

In addition, great thanks to all researchers and developers of routing protocols for their recommendations.

Special thanks to Jirka Klaue and Manuel Saez for their help during implementation and testing phase.

10. References

[1] Alexander Klein and Phuoc Tran-Gia, "A Statistic-Based Approach towards Routing in Mesh Networks.", In Proceedings of the First IEEE International Workshop on Enabling Technologies and Standards for Wireless Mesh Networking Mechtech, Pisa, Italy, October 2007.

[2] Alexander Klein, "Performance Comparison and Evaluation of AODV, OLSR and SBR in Mobile Ad-Hoc Networks.", International Symposium on Wireless Pervasive Computing (ISWPC), Santorini, Greece, May 2008.

11. Authors' Addresses

Alexander Klein
Department of Computer Science
Distributed Systems
University of Wuerzburg
Am Hubland
97074 Wuerzburg
Germany

Phone: +49 89 607 21685
Fax: +49 89 607 21685
EMail: alexander.klein@eads.net

12. Full Copyright Statement