Reliable Routing in Large Scale Wireless Sensor Networks

Guo, J.; Orlik, P.; Zhang, J.; Ishibashi, K.

TR2014-071 July 2014

Abstract

Wireless sensor networks have a wide range of applications including target detection and tracking, environment monitoring, industrial process monitoring, hospital monitoring, and public utility service. A sensor network consists of a large number of sensor nodes and a few sink nodes to collect data from sensor nodes. Sensor nodes and sink nodes form a large scale wireless mesh network in which packets are typically delivered between sensor nodes and sink nodes in a multi-hop manner. Reliable packet routing in wireless sensor networks is crucial, especially when network size is large. This paper presents a reliable routing protocol (RRP) to maximize the reliability of data collection and control command delivery in large scale wireless sensor networks. RRP aims to discover multiple bidirectional routes between a sensor node and a sink node. Sink node initiates route construction with an imaginary node as the destination to guarantee complete routing topology buildup. RRP achieves load balance by sending data packets via the route with lighter workload. RRP can be optimized for lightweight routing. Simulation results show that the proposed RRP routing protocol can realize 100% of packet delivery rate and outperforms existing routing protocols in terms of packet delivery rate, routing packet overhead, and end-to-end packet delay.

Ubiquitous and Future Networks (ICUFN)

Reliable Routing in Large Scale Wireless Sensor Networks

Jianlin Guo, Philip Orlik, Jinyun Zhang
Mitsubishi Electric Research Laboratories
Cambridge, USA
{guo, porlik, jzhang}@merl.com

Koichi Ishibashi
Wireless Modules Development Center
Mitsubishi Electric Corporation IT R&D Center
Ofuna, Japan
Ishibashi.Koichi@ce.MitsubishiElectric.co.jp

***Abstract*—Wireless sensor networks have a wide range of applications including target detection and tracking, environment monitoring, industrial process monitoring, hospital monitoring, and public utility service. A sensor network consists of a large number of sensor nodes and a few sink nodes to collect data from sensor nodes. Sensor nodes and sink nodes form a large scale wireless mesh network in which packets are typically delivered between sensor nodes and sink nodes in a multi-hop manner. Reliable packet routing in wireless sensor networks is crucial, especially when network size is large. This paper presents a reliable routing protocol (RRP) to maximize the reliability of data collection and control command delivery in large scale wireless sensor networks. RRP aims to discover multiple bidirectional routes between a sensor node and a sink node. Sink node initiates route construction with an imaginary node as the destination to guarantee complete routing topology buildup. RRP achieves load balance by sending data packets via the route with lighter workload. RRP can be optimized for lightweight routing. Simulation results show that the proposed RRP routing protocol can realize 100% of packet delivery rate and outperforms existing routing protocols in terms of packet delivery rate, routing packet overhead, and end-to-end packet delay.**

Keywords-multi-path routing; verified bidirectional routes; unique route identification; load balance; lightweight optimization; reliable data packet delivery; low routing overhead; low end-to-end delay; large scale wireless sensor network

I. INTRODUCTION

A wireless sensor network is different from conventional mobile ad-hoc network even though there are some similarities between them. Mobile ad-hoc networks are generally peer-to-peer networks. In a sensor network, there could be dozens to thousands of sensor nodes with a few dedicated sink nodes. The data flows in a sensor network are typically multipoint-to-point traffic from sensor nodes to sink node and point-to-multipoint traffic from sink node to sensor nodes. The peer-to-peer traffic is only for relay purpose. The physical topology of a sensor network is relatively stable since sensor nodes are stationary in geometric location or with very low mobility.

Packet delivery in a wireless sensor network may require very high reliability and low latency. For example, when an event occurs, disaster monitoring sensors must detect and reliably report the event to a control center as soon as possible. A few seconds could save a lot of lives in the situation like earthquake or tsunami. Depending on application, data packet transmission in a sensor network could be periodic, event-driven or both. The manner in which data and control packets are routed is critical in large scale wireless sensor networks.

There are several well-known routing protocols for mobile ad-hoc networks. Ad-hoc On-demand Distance Vector (AODV) [1], Dynamic Source Routing (DSR) [2], and Temporally Ordered Routing Algorithm (TORA) [3] are routing protocols for mobile ad-hoc networks. These routing protocols are typically designed for peer-to-peer packet delivery and not suitable for data collection in large scale wireless sensor networks.

AODV is an on-demanding routing protocol and has high routing overhead due to excessive transmission of routing discovery packets. In the AODV routing protocol, each route discovery between a source node and a destination node requires a network-wide broadcast flood. In addition, AODV is a single path routing protocol. DSR is similar to the AODV in that it discovers routes on-demand. DSR has capability to discover multiple routes and it performs well in small networks. The main drawback is that the DSR includes the route information, a node list, in each packet delivery, which causes large packet size and considerable routing overhead, especially when routes are long. TORA is an on-demand routing protocol based on directed acyclic graphs (DAG). It attempts to achieve a high degree of scalability using a non-hierarchical routing method. TORA constructs and maintains a DAG rooted at a destination. It achieves loop-free multipath routing by only allowing packet flows from nodes with higher heights to nodes with lower heights. Thus TORA is good for dense networks. However, routing overhead in TORA is even higher than AODV and DSR. As number of nodes increases, routing overhead increases considerably.

Ad-hoc On-demand Multipath Distance Vector (AOMDV) [4] and A Reverse AODV (RAODV) Routing Protocol in Ad Hoc Mobile Networks [5] are variations of the AODV to discover multiple routes. AOMDV tries to discover multiple disjoint routes between a source node and a destination node. However, the problem is that some nodes cannot discover multiple disjoint routes, but can discover multiple joint routes. As a result, AOMDV only discovers a single route for those nodes. To guarantee loop-free route, AOMDV accepts the first route and subsequent shorter route. These criteria can prevent nodes from discovering multiple routes, especially if the first route is the shortest route. To achieve multi-path routing, AOMDV has higher routing overhead than AODV. The RAODV tries to discover multiple routes between a source node and a destination by flooding network multiple times. Therefore, it has much higher routing overhead than AODV.

The IPv6 Routing Protocol for Low Power and Lossy Networks (RPL) [6] is a proactive routing protocol developed by the Internet Engineering Task Force (IETF). The RPL is another routing protocol based on DAG. It aims to provide reliable and scalable routing for low power and lossy networks. RPL shows good scalability [7]. However, many important issues are left unresolved. There is no practical local route repair mechanism. RPL is not a loop-free routing protocol and does not support load balance. More importantly, RPL may suffer from severe unreliability due to the selection of suboptimal routes with low quality links [7].

In this paper, we propose a proactive routing algorithm called reliable routing protocol (RRP) for large scale wireless sensor networks. We aim to maximize routing reliability and minimize routing overhead by discovering multiple routes from each sensor node to a sink node with only one network-wide broadcast flood. Our routing protocol discovers loop-free routes with each route being verified as a bidirectional communication path between a sensor node and the sink node. The route optimization tries to select disjoint routes as much as possible. Each route is uniquely identified in the network so that the node knows exactly which route to be used for sending or relaying packet. The proposed RRP provides capability to realize load balance and can be optimized for lightweight routing. We compered our routing protocol with existing routing protocols via simulations. The simulation results show that the proposed RRP routing protocol outperforms existing routing protocols. The RRP can achieve 100% of packet delivery rate with low latency even when network size is large and each sensor node frequently transmits data packet.

The rest of this paper is organized as follows. Section II presents the details of the RRP routing protocol. Section III outlines data and control packet transmission. Load balanced routing is given in section IV. Section V describes lightweight optimization. In section VI, we analyze and explain the simulation results. Finally, section VII concludes the paper.

II. MULTI-PATH ROUTE CONSTRUCTION AND ROUTE MAINTENANCE

This paper presents a reliable routing protocol (RRP) to discover multiple bi-directional routes while minimizing the number of broadcast floods, which considerably increase communication overhead, resource consumption and packet transmission interference. In fact, the broadcast floods account for major part of routing overhead in conventional routing protocols. In this paper, a sink node initiates only one broadcast flood to construct a routing topology. Sensor nodes do not initiate network-wide broadcast flood.

A. *Description of Routing Packets*

Three types of routing packets are defined for the purposes of initial routing topology construction, subsequent route discovery, route verification and route confirmation.

The route construction and discovery (RCD) packet is used by sink node to initiate routing topology construction and by sensor node to discover subsequent route. The RCD packet consists of source identification (S-ID), destination identification (D-ID), source type (ST), time to live (TTL), node list (NL), sequence number (SN), and other optional fields. The ST indicates if the RCD packet is originated by a sink node for initial routing topology construction or sent by a sensor node for subsequent route recovery. Specifically, ST = 1 indicates sink node as source node and ST = 2 indicates sensor node as source node. The NL contains a list of nodes the RCD packet traveled through and it provides a route from initiation node to receiving node.

The route verification (RV) packet is used to verify a route as bi-directional. The RV packet consists of S-ID, D-ID, destination type (DT), route identification (R-ID), NL, SN, and other optional fields. DT = 1 indicates sink node as destination and DT = 2 indicates sensor node as destination. R-ID is the ID of the route assigned by node originating route verification process and NL specifies route to be verified.

The route confirmation (RC) packet is used to confirm success of route verification. The RC packet consists of S-ID, D-ID, R-ID, SN, and other optional fields. However, there is no NL field in RC packet.

B. *The Sink Node Initiated Route Construction*

Without loss of generality, we describe the proposed RRP routing protocol by using a sensor network with one sink node and each sensor node attempts to discover two routes to the sink node. However, our routing protocol can be applied to networks with multiple sink nodes and more than two routes.

To distinguish our RRP protocol with existing routing protocols, we introduce an imaginary node as shown in Figure 1. The imaginary node does not physically exist in the sensor network and is assigned an ID different from the ID of any real node. The imaginary node is the key to guarantee all sensor nodes can discover routes to the sink node.

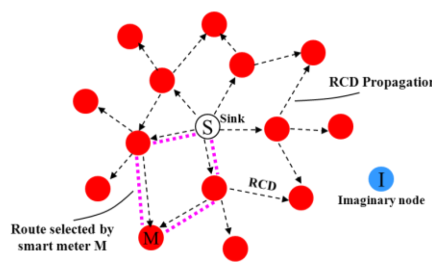

Figure 1. Initial Routing Topology Construction Illustration

The initial routing topology construction is started by the sink node, which broadcasts a RCD packet by setting ST to 1. To make sure that RCD packet can propagate to entire sensor network, the sink node sets the imaginary node as the destination node in RCD packet. During routing topology construction, the imaginary node cannot be reached by any real node including sink node. When sink node broadcasts the RCD packet, any real node in the sensor network is not the destination node. As a result, every sensor node has to rebroadcast the RCD packet. Therefore, each sensor node must receive at least one copy of the RCD packet and discover at least one route to the sink node. In fact, a sensor node can discover multiple routes unless that sensor node cannot physically discover more routes. For example, if a sensor node has only one neighbor that is the sink node, then that sensor node can only discover one route to the sink node.

A sensor node can receive multiple copies of the RCD packet broadcasted or rebroadcasted by its neighbors. Based on the received copies of the RCD packet, a sensor node selects two reverse routes to the sink node if the RCD packet is initially originated by a sink node. The route selection criteria vary according to the different cost functions such as the hop count, the link quality, etc. In this paper, we use the hop count as the cost function to discover two disjoint routes as much as possible since the disjoint routes fail independently, and therefore reliability is enhanced.

The basic flow chart to process a RCD packet originated by a sink node for initial routing topology construction is shown in Figure 2. The receiving node first performs a filtering procedure. The node checks if source node is the sink node. If no, the RCD packet is discarded. If yes, the node checks if its own ID is in the NL field of the RCD packet. If yes, this indicates a loop and the RCD packet is discarded. If no, the node determines if the NL carried in the RCD is same as any NL stored. If yes, the node discards RCD packet. If no, the RCD packet passes filtering.

The RCD packet process consists of processing the 1st RCD packet, processing the 2nd RCD packet, and processing subsequent RCD packets for optimization.

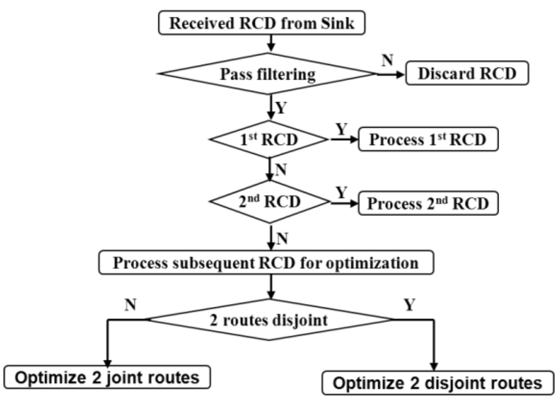

Figure 2. Flow Chart of RCD Processing for Initial Route Discovery

If the receiving node has no route to the sink node that originated the RCD packet, it stores the NL. The stored NL provides the first route to the sink node. The node then performs the RCD packet rebroadcasting.

To rebroadcast the RCD packet, TTL is decreased by 1 first. If TTL is zero, the RCD packet is discarded. Otherwise, the node's ID is inserted into the NL of RCD packet, and the RCD packet is rebroadcasted.

If the receiving node has only one route to the sink node, it stores the NL as the second route to the sink node, and performs the RCD packet rebroadcasting.

The subsequently received RCD packets are used for route optimization. Two routes are said to be disjoint if they do not have a node in common, other than the source node and the destination node. Depending on if two stored routes are disjoint or not, route optimization process is partitioned into optimizing joint routes and optimizing disjoint routes.

If two stored routes are joint, the route optimization is to discover two disjoint routes if possible. If the route carried in the RCD packet disjoints both stored routes, the longer route is replaced with the route carried in RCD packet, and RCD packet is rebroadcasted. If the route carried in RCD packet disjoints only one stored route, the joined route is replaced, and RCD packet is rebroadcasted. If the route carried in RCD packet joins both stored routes, the processing of the RCD packet is optional. The RCD packet can be discarded or used to discover two shorter routes.

If two stored routes are already disjoint, the route optimization selects two shorter disjoint routes. If the route carried in the RCD packet disjoints both stored routes and is shorter than any stored route, the longer route stored is replaced. In this case, the RCD packet retransmission is optional. If the route carried in RCD disjoins only one stored route and is shorter than the stored route which joins it, that stored route is replaced, and the RCD packet can be discarded or rebroadcasted. Otherwise, the RCD packet is discarded.

To show the innovation of the imaginary node in routing topology construction, we illustrate that the mechanism of route request (RREQ) and route reply (RREP) used by AODV, DSR, AOMDV and RAODV fails to build a complete routing topology for some sensor node deployments.

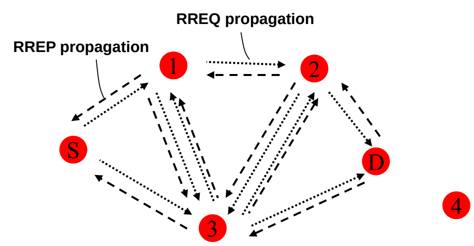

Figure 3. Counter Example of Conventional Route Discovery

As shown in Figure 3, the sink node S initiates route discovery by broadcasting the RREQ packet. The RREQ packet can propagate to the destination node D via different routes, such as nodes S-1-2-D and S-3-D. However, when node D receives the RREQ packet, it does not rebroadcast the RREQ packet because it is the destination node. Instead, the node D transmits the RREP packet back to node S. Because node 4 is out of transmission range of nodes 1, 2, 3 and S, node 4 does not receive the RREQ packet. Therefore, the RREQ packet does not propagate to the entire sensor network. As a result, node 4 cannot discover route to node S.

C. *Route Identification*

It is unnecessary to identify a route in single-path routing protocol such as AODV since each node has only one route to a specific destination node. However, multi-path routing is different. Each node has multiple routes to a destination node. Therefore, based on its preference, a node can select a particular route to send its packet. For example, node 8 in Figure 4 has two routes R-1 and R-2 to node S. To send a packet to node S, node 8 can forward packet to node 7 and specify using route R-1 for packet delivery.

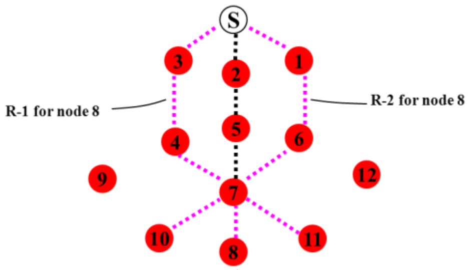

Figure 4. Route Identification Example

How to identify a route in a network has not been addressed by existing multi-path routing protocols. For example, the RPL protocol [6] discovers multiple routes to a sink node. But, it sends all packets to a default route without considering the load balance. In this paper, we propose a route identification mechanism, which can be used for load balance. A sensor node assigns an R-ID to each route it discovered. The tuple (S-ID, D-ID, R-ID) uniquely identify a route in a network. The R-ID is unique within the scope of a node.

D. Aggregated Route Verification

Operations in sensor networks may require bidirectional routes. In a wireless sensor network, the communication links may exhibit asymmetric properties. For some applications, it is required that the reachability of a node is verified before the routes can be used [6]. Initial route construction process uses a broadcast mechanism. The routes discovered are only valid for one direction from the sink node to sensor nodes. Therefore, routes must be verified as valid routes from sensor nodes to the sink node. The route verification process also provides the sink node with routes to each sensor node.

The route verification is performed by using RV packet and RC packet. To verify a route, a sensor node unicasts a RV packet to the sink node with DT set to 1 via the route specified by NL field in RV packet. Upon receiving a RV packet, the sink node stores route information and unicasts a RC packet back to the sensor node along the reverse route obtained from NL of the RV packet. When the source sensor node receives the RC packet, the route has been verified to be a bidirectional route. The sink node can use the stored routes to transmit control packets to sensor nodes in the network.

The RV and the RC packets are relayed by intermediate sensor nodes. When a sensor node on the route receives a RV packet with DT = 1, it stores route information (S-ID, D-ID, R-ID, NL) and forwards the RV packet to the next hop node obtained from the NL field. The stored route at intermediate node serves multiple purposes such as relaying the RC packet back to the source node of RV packet, load balance and aggregated route verification, that is, shorter route is verified as a portion of the longer route. To increase the probability of the aggregation, it is preferred that longer routes are verified earlier. The aggregated route verification can also reduce routing overhead.

To perform aggregated route verification, a sensor network can estimate packet propagation time based on network diameter and wireless technology used. Before transmitting the RCD packet, the sink node can broadcast a time packet to be used by sensor nodes to estimate when route verification starts.

The time packet includes the following fields: S-ID, D-ID, MH (the maximum number of hops allowed), MT (the maximum time needed to propagate the time packet through the entire sensor network), RT (the maximum time needed propagate the RCD packet through the entire network), VT (the maximum time needed to verify all routes), NH (the number of hops time packet traveled), and other options. The NH is initially set to 1 and increased by 1 each time when time packet is rebroadcasted. Each sensor node rebroadcasts time packet only once.

The sink node sets S-ID to its ID, D-ID to imaginary node ID. MT, RT and VT are estimated by using the predefined MH and media access control and physical (MAC/PHY) protocol used.

The time packet is relayed through the entire network by the sensor nodes because the imaginary node is the destination of that packet.

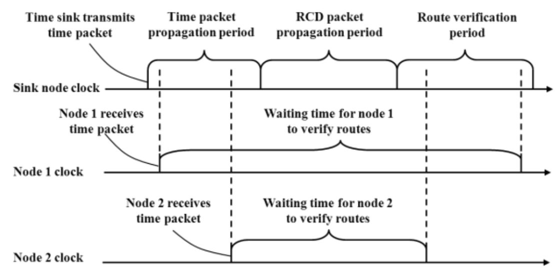

Figure 5. Route Verification Scheduling Example

Upon receiving time packet, the sensor node sets a wait time (WT) for route verification as following:

$$WT = RT + \frac{MH - NH}{MH} * (MT + VT) \quad (1)$$

The WT increase the probability that sensor nodes with longer routes verify routes earlier. As shown in Figure 5, node 1 receives the time packet before node 2 does, because the NH for node 1 is smaller than that for node 2. However, node 2 starts route verification earlier than node 1 does. It should be noticed that Route verification can also be performed once a route is discovered.

E. Route Recovery

Wireless sensor nodes are either stationary or with limited mobility. The deployment of the sensor nodes generally remains constant for long period of time. Therefore, a route can be used until the route is determined to be broken.

When a sensor node detects a broken route, it uses other route for packet delivery. In the meantime, it discovers another route. To do so, the node broadcasts a RCD packet locally by setting ST = 2 and TTL to a small number such as 1 or 2. In this case, the destination node of RCD packet is set to the corresponding sink node instead of the imaginary node.

Upon receiving a RCD packet with ST = 2, a node performs filtering process to make sure that the RCD packet has not been received before by using S-ID and SN, and no loop will be created by using the NL. Also, the RCD packet is not generated by itself.

If the receiving node is the destined sink node, it generates a RV packet with S-ID set to its own ID, D-ID set to S-ID carried in RCD packet, DT set to 2, R-ID set to a proper value, NL set to the NL carried in RCD packet, and SN set to a proper value. The sink node then unicasts the RV packet back to the source node of RCD packet along the route specified by the NL carried in the RV packet.

If the receiving node is not the destined sink node, the process of the RCD packet is as follows.

If the node has a valid route to the destined sink node and that route disjoints the NL carried in RCD packet, it constructs a RV packet by setting S-ID to its ID, D-ID to S-ID in RCD packet, DT to 2, R-ID to a proper value, SN to a proper value. The NL is constructed by attaching NL contained in RCD packet to NL of its route to the sink node. It unicasts the RV packet back to the source node of RCD packet along the route specified by the NL field.

If the node has a valid route to the destined sink node and that route joins the NL carried in RCD packet, the RCD packet is discarded to avoid loop.

If the node has no valid route to the destined sink node, it checks if TTL is zero. If yes, it drops the RCD packet. If no, it updates the RCD packet by inserting its ID into NL and decreasing TTL by 1, and rebroadcasts the RCD packet.

The RV packet is relayed by intermediate nodes to the source node of RCD packet, which assigns an R-ID to the route carried in RV packet and stores the route. If the source node of RV packet is sink node, the source node of RCD packet sends a RC packet back to sink node. If the source node of RV packet is not the sink node, the source node of RCD packet verifies the newly discovered route.

III. Data Packet and Control Packet Transmission

The RRP discovers bidirectional routes. The sink node obtains routes to sensor nodes via route verification. To deliver a packet via a specific route, the tuple (S-ID, D-ID, R-ID) is only route information to be carried in the packet. The NL is not needed. An intermediate node obtains next node via the stored NL. Therefore, routing overhead is greatly reduced.

For dynamic routing optimization, a node can also let next hop node make route decision by setting R-ID to a specific value. In this case, the next hop node should select an optimal route to forward packet further.

IV. Load Balanced Routing

Load balance is critical for routing packets in large scale sensor networks. Unbalanced routing can result in traffic congestion, long packet delay and most importantly packet loss. The tuple (S-ID, D-ID, R-ID) carried in the packet uniquely identifies a route, i.e., a NL. With a given NL, a sensor node can determine exact nodes on the route when it relays a packet for other node. Upon knowing the routes for relay packets, a sensor node can send its own packets via the routes with lighter workload. Using Figure 4 as an example, if node 7 relays data packets for nodes 10, 8 and 11 via either route 7-4-3-S or 7-6-1-S, then node 7 can send its own data packets using route 7-5-2-S.

V. Lightweight Optimization

The sensor nodes typically have limited resources and processing power. Therefore, the sensor networks can’t afford heavy routing protocol.

Unlike the AODV, the proposed RRP protocol does not store any route having a sensor node as the destination. It only stores routes destined to the sink node.

To optimize the RRP for lightweight routing, upon receiving the corresponding RC packet for a RV packet, a sensor node can replace the stored route information (S-ID, D-ID, R-ID, NL) with (S-ID, D-ID, R-ID, Next-Hop-ID) because once the RC packet comes back, the sink node already stored the route to the source node of RV packet, and the tuple (S-ID, D-ID, R-ID, Next-Hop-ID) is sufficient to relay data packets for the source node of RV packet. However, this optimization may limit RRP capability for load balance.

Furthermore, upon receiving the corresponding RC packet for a RV packet, a sensor node can completely delete the tuple (S-ID, D-ID, R-ID, NL). In this case, the sensor node can use its own routes to relay data packets for other sensor nodes.

VI. Simulations

The RRP has been designed by referencing the AODV and the DSR. It can be seen as a proactive version of the AODV. Therefore, the AODV has been used as the main base for performance comparison. We have also compared the RRP with the multi-path version of the AODV, i.e., AOMDV. In addition, to compare the RRP with existing proactive routing protocols, the IETF RPL protocol is used as a reference for performance analysis.

The performance of the AODV has been evaluated considerably by using NS2 simulator. However, most of simulations are performed with the number of nodes less than or equal to 50 and are done using the IEEE 802.11 technology instead of the IEEE 802.15.4 technology, which is designed for wireless sensor networks. Although routing protocols perform better using the IEEE 802.11, the simulation results do not exhibit the desired performance of the routing protocols in wireless sensor networks.

In this paper, we use the NS2 simulator running the IEEE 802.15.4 technology to simulate performance of the RRP in large scale wireless sensor networks. All sensor nodes are stationary and randomly displaced in a rectangle area with the sink node at the center. The size of the rectangle depends on number of sensor nodes, transmission range and network diameter. In the simulations, the transmission range is set to 30 meters, the network diameter is set to 30, and the data rate of the IEEE 802.1.5.4 radio is set to 100kbps, which is much less than data rate of the IEEE 802.11 radio. The constant bit rate (CBR) traffic is employed with 50 bytes of payload. The TwoRayGround and the Shadowing channel models are used in simulations. Performance metrics are data packet delivery rate (PDR), data packet average end-to-end delay (AED) and routing overhead (ROH) per data packet.

TABLE 1. TwoRayGround, N = 500

Metrics	CBR ITV=30 Min		CBR ITV= 1 Min	
	AODV	RRP	AODV	RRP
PDR	96.3%	100%	14.9%	100%
AED	120ms	40ms	520ms	150ms
ROH	12.083	0.167	4.083	0.005

TABLE 2. TwoRayGround, N = 1000

Metrics	CBR ITV=30 Min		CBR ITV=2 Min	
	AODV	RRP	AODV	RRP
PDR	73.2%	100%	11.4%	100%
AED	290ms	70ms	6570ms	80ms
ROH	35.75	0.167	4.417	0.01

Tables 1-2 show simulation results using TwoRayGround channel model and 24 hours simulation time. 500 nodes are deployed in a 250m by 200m rectangle and 1000 nodes are deployed in a 320m by 320m rectangle. Tables show that RRP achieves 100% of PDR in all cases. AODV only achieves reasonable PDR with CBR interval of 30 minutes. For smaller CBR intervals, AODV drops more than 85% of data packets. The AED of the RRP is at least 3 times shorter than that of AODV. For 1000 nodes and 2 minutes CBR interval, RRP is 82 times faster than AODV. The ROH of the RRP is about 1% of the ROH of AODV for 30 minutes CBR interval and is only about 0.2% of the ROH of AODV for smaller CBR interval.

Table 3 shows simulation results for 500 nodes using Shadowing channel model with 4.0 standard deviation, 24 hours simulation time, 250m by 200m rectangle, and 30 minutes of the CBR interval. It is shown that with Shadowing channel model and multiple routes, RRP achieves much higher PDR than AODV. Its PDR ranges from 79.1% to 97%. On the other hand, AODV drops more than 63% of data packets. RRP is at least 84 times faster than AODV. The ROH of RRP is less than 0.4% of the ROH of AODV. Table 3 also shows that as path loss exponent (PLE) increase from 2.0 to 3.0, the performance of RRP and AODV degrades.

One important point is that RRP is simulated with the number of routes (NR) equal to 1 and 2. It is shown that multi-path routing improves performance of RRP considerably when PLE is higher. With two routes, the ROH and the AED are much smaller than that with one route. This feature can't be seen clearly with the TwoRayGround channel model since the route is relatively stable and backup routes are hardly used in case of the TwoRayGround channel model.

TABLE 3. Shadowing, N = 500

Metrics	PLE = 2.0			PLE = 2.5			PLE = 3.0		
	AODV	RRP NR=1	RRP NR=2	AODV	RPL NR=1	RRP NR=2	AODV	RRP NR=1	RRP NR=2
PDR	36.7%	96.2%	**97.0%**	34.1%	88.6%	90.3%	32.5%	42.7%	79.1%
AED	1.53s	0.10s	**0.01s**	1.68s	0.18s	0.02s	1.84s	0.78s	0.02s
ROH	168.75	7.875	**0.51**	188.75	15.88	0.77	550.5	228.63	1.11

To compare the proposed RRP with existing multi-path routing protocols, we simulated AOMDV with 1000 nodes and 2 minutes CBR interval using the TwoRayGround channel model. AOMDV only achieves 58% of packet delivery rate, which is much lower RRP's 100%.

To compare the RRP with existing proactive RPL routing protocol, we simulated RPL with 1000 nodes and 5 minutes CBR interval using the TwoRayGround channel model. The packet delivery rate of RPL is below 90%. Therefore, the proposed RRP protocol outperforms the RPL protocol.

VII. CONCLUSION

A wireless sensor network can consist of a large number of sensor nodes. Reliable packet routing is very important for applications such as industrial monitoring and controlling. In this paper, we present a proactive routing algorithm, called reliable routing protocol (RRP), to discovery multiple loop-free routes with each route being verified as a two-way communications path. The proposed RRP aims to discover disjoint routes from sensor nodes to the sink nodes. Each route is uniquely identified in the network. The identified routes can be used to realize load balanced routing. The RRP can be optimized for lightweight routing. We simulated the RRP by using NS2 simulator with 500 and 1000 nodes and the IEEE 802.15.4 wireless technology. Simulation results show that the proposed RRP performs much better than existing routing protocols. The RRP can achieve 100% of packet delivery rate with much less routing overhead and end-to-end packet delay. The conventional on-demand routing protocols do not fit well in wireless sensor networks due to high routing overhead. The proposed RRP is a feasible routing protocol for large scale wireless sensor networks. For the network with stable connectivity, single path routing protocol can achieve similar performance as multi-path routing protocol. However, for the network with unstable connectivity, the multi-path routing protocol can significantly improve the packet delivery rate, routing overhead and latency.

REFERENCES

[1] C.E. Perkins, E.M. Royer and S.R. Das, "Ad-hoc On-demand Distance Vector (AODV) routing", http://tools.ietf.org/html/rfc3561

[2] D. Johnson, Y. Hu and D. Maltz, "The Dynamic Source Routing protocol (DSR) for mobile Ad Hoc networks for IPv4", http://tools.ietf.org/html/rfc4728

[3] V.D. Park and S.M. Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks", Proceedings of INFOCOM 1997

[4] M.K. Marina and S.R. Das, "On-demand Multipath Distance Vector Routing in Ad Hoc Networks", http://www.nmsl.cs.ucsb.edu/ksarac/icnp/2001/papers/2001-2.pdf

[5] C. Kim, E. Talipov and B. Ahn, "A Reverse AODV Routing Protocol in Ad Hoc Mobile Networks", EUC Workshops 2006, LNCS 4097, pp. 522 – 531, 2006

[6] T. Winter, P. Thubert, et al, "RPL: IPv6 Routing Protocol for Low power and Lossy Networks", http://tools.ietf.org/html/draft-ietf-roll-rpl-19, March 13, 2011

[7] E. Ancillotti, R. Bruno, and M. Conti, "The Role of the RPL Routing Protocol for Smart Grid Communications", IEEE Communications Magazine, vol. 51, no. 1, pp. 75–83, 2013.