A Proposed Solution for Route Reply Storm Problem to Improve DSR Protocol Performance in Wireless Sensor Networks

Dheyaa Jasim Kadhim
Electrical Engineering Department, University of Baghdad, Baghdad, Iraq
E-mail: dheyaa@ceong.uobaghdad.edu.iq

Abstract. Due to the limited transmission range of the wireless sensor network interface, a node may need multiple network hops to exchange data with another node over networks and other issues cause an overhead and bad utilization on the network. As a consequently, if some nodes reply route request at the same time to the same destination, then these simultaneous replies from different nodes will cause collision at the destination which can cause a problem named route reply storm. The dynamic source routing (DSR) protocol is a reactive source routing protocol for mobile IP network where nodes should sense and discover with nearby nodes. Each node acts as a router for sending and receiving the packets to/from other node. In this work, we present a new proposal as a solution for storm route reply problem in DSR; the objective of the new proposed solution is to present a way to reduce unnecessary packet flooding between source and destination nodes in order to enhance DSR protocol. Afterthought, this work proposed some case studies to verify our proposed solution for solving the problem route reply storm, our verifications proves our robustness and correctness of the proposed solution against two main WSN problems that may face any wireless sensor network including coverage problem and link failure problem. The simulation results achieved here for two routing protocols DSR protocol and proposed improved DSR protocol for energy efficiency parameters. Simulation results showed that the energy consumption of proposed approach is minimized by 25 % approximately as compared to previous standard DSR protocol while the network lifetime performance is increased by approximately 35 % as compared to standard DSR protocol. In summary, the proposed solution of DSR protocol can be energy efficient for wireless sensor networks resource management.

1. Introduction
Wireless sensor network is one of the most influential targets in current wireless networks. Considering their strict limits on energy use on widely distributed sensing elements, the expensive tasks of these networks must be pre-defined, and controlled and directed management. There are many routing and management techniques available in wireless sensor networks [1]. These include traditional techniques-flooding and gossiping. When using flooding technology, the sensor nodes repeatedly broadcast the received data and control data packets to the rest of the network until reaching the designated receiver node. It is worth noting that this technology does not consider the power limitation required by WSN [2]. As a result, when this technology is used to route data in a WSN network, it can cause large and complex problems, such as oversaturation, which indicates that because dumping is a blind technology, these duplicate data packets may continue to be routed in the network, so the sensor may receive the duplicate data packet more than once [3]. In order to solve this
problem with a sensor network, gossiping technology has been proposed, whereby the sensor randomly selects one of its neighbors and sends the received data packet to it. Repeat the same process until all sensors receive the data [4,5].

The routing protocol in WSN is designed based on many factors that affect network functions. Therefore, we must first study these factors before we can realize effective and correct communication in WSN network [6,7]. In our work, we will consider two main factors which may constitute the realization of fast and safe communication in WSN network [8]. In this article, we discussed dynamic source routing (DSR) and its importance in wireless sensor networks, and analyzed the performance of the protocol. The DSR protocol dynamically and simultaneously discovers the source path to any destination in the self-organizing network through multiple thoughtful and targeted network hops, and plays an important role in developing the functions of its nodes [9-10]. Then, through the node path, each sent data packet will carry in its header a complete and ordered list of nodes that the packet must pass through, so that the packet routing has a new directed path without requiring forward packet path details anywhere. So, this new path to the host will be included and attached to the header of each data packet, and in the same way, other nodes that reuse or direct any of these packages or listen to them can store this routing information conditionally and for the need to use it in finding future paths [11,12].

The work objective of this research is to consider a specific problem that faces using DSR protocol in WSN which named Route Reply Storm. The reason for this problem comes with using the node its route cache memory to respond to the request of the third-party path it points to, which leads to the formation of route reply storm problem [13]. If a sensor host asks a routing request to another destination host with its neighbors in its path cache, each nearby node may try to send a routing response, thus consumed bandwidth and increasing the collision rate in the area, and affecting the actual communication between the sender and the receiver [14].

In this paper, we propose a new approach of requesting the route so as we can avoid the penalty of route caching, avoid packet header size grows with route length due to source routing and finally avoid flood of route requests may potentially reach all nodes in the network. By using this methodology we can find out the performance of DSR enhanced using new proposal protocol so that the overhead is reduced by preventing route reply storm problem that causes unnecessary packet flooding which minimize the utilization of resources. Then, the proposed solution is verified under consideration through two main problem in WSN includes coverage problem and link failure problem taking into account main performance parameters such as network lifetime, average energy consumption, average throughput and packet delivery ratio.

2. Proposed Solution

The sending host may try some old paths (obtained from the local cache, or answered by other nodes from the cache) to find the new and good path. With the passage of time and the mobility of the host, the old cache may have a negative impact on performance, and one of the problems that face the work of DSR is the aging of the storage path, rather than the always updated path. This is the most important motivation of our proposed solution for enhancing DSR protocol’s performance. So, middleware nodes may use the old cache path to send path responses, thereby polluting other routing caches. So, care must be taken to avoid conflicts between routing requests propagated by entering nodes adjacent to the random delay before RREQ forwarding. If the divergence increases due to too many path responses returned by the node in response to using its local cache, the route reply storm problem is the main problem and challenge that this work focuses on and a new solution is proposed.

Our proposed solution enhances the DSR protocol which dynamically discovers a source route across mobile nodes to any destination in wireless sensor network by two standard phases (Route Discovery (RREQ), Route Reply (RREP)). So our new protocol proposes to prevent route reply storm which is enhance DSR protocol. Through these two phases we consider two influenced problem related to coverage and link failure problems.
2.1. Route Discovery (RREQ) Phase

DSR needs some tools to perform its duties according to the protocol we proposed here: Firstly, the routing packet is sent to the next host, and then the transmitted host creates a source path in the packet header and appends the address of each host through the network to it. After that, it forwards the data packet to the target host through it. Then, the sender sends the packet according to the route it took in the first path. And when the host receives the packet, if this is not the expected host, that is, the final destination of the packet, it will automatically send the received packet to the next stage specified in the source path in the packet header.

After the packet ends and reaches its final destination, the completed path will be stored in the memory module of this host for future use. Secondly, when sending data packets from one host to another, if the path cannot be found, the sender may try to use a route mechanism to discover a host. If host S is the source host, then D is the target host, and S starts to discover the path without a path. Source host S floods route request (RREQ). Each host attaches its own ID when redirecting RREQ. During the waiting period for the path creation of the current data packet, the current host may still normally receive data from all neighboring nodes, and may send and receive data packets from other nodes. The host can store the original data packet as a temporary measure so that it can transmit the data packet once the path is known using route discovery technology, or the host can ignore the data packet and retransmit the data packet by relying on high-level protocol programs if necessary. So, the above procedure will prevent route reply storm occurs at the destination host during route discovery path. Figure 1 below shows the procedure for our proposed route discovery (RREQ) phase.

2.2. Route Reply (RREP) Phase

After the arrival of the first RREQ, target D sends a route reply (RREP). By reversing the additional path to receive RREQ, RREP is transmitted on the path obtained from the first route. RREP has a known path from S to D. Host D first receives RREQ from host S, and the host uses any source path; it monitors the continuation of the right operation of the path. For example, if the sender, destination, or any other named master along the route moves out of the radio transmission range along the next or previous hop of the path, the path will not be used to reach the destination. In addition, if any host in the path is down or down, the path will not work. This monitoring of the right operation of the road in

---

**Figure 1.** Route Discovery (RREQ) Phase’s Procedure.
use is called road maintenance. When path maintenance discovers a trouble within the path in the way, path detection can be deployed another time to find a new right path to the target.

Secondly, each roaming host participating in the wireless sensor network maintains a path buffer in which the learned source path is stored. When a host sends a packet to another host, the sender first checks its routing cache to direct the source to the destination. If a path is found, the sender uses that path to send the packet. Figure 2 below shows the route reply (RREP) phase procedure.

![Figure 2](image)

**Figure 2.** Route Reply (RREP) Phase’s Procedure

3. Applications of Proposed Solution
In this section, we will show how our proposed solution for the problem of route reply storm can be applied to solve the problems of wireless sensor networks so as improving the performance of DSR protocol. This work verifies our proposed approach taking into account two main WSN problems including coverage problem and link failure problem.

3.1. Coverage Problem
In order to verify the correctness and robustness of our proposed solution for route reply storm problem under large coverage area of a wireless sensor network, we consider the network shown in Figure 3 below, this network consists from large number of sensor nodes and we want to coverage the transmission from node D to L note that the path from D to L will pass through so many intermediate nodes and how our proposed solution can deal with this situation. The following procedure will be described how our proposed solution dealing with this route request.

![Figure 3](image)

**Figure 3.** Example WSN for Coverage Problem Verification.
To deal with such situation, we have to suppose some assumptions such we consider to have three main zones in this network examples namely (A’s Zone, G’s Zone and K’s Zone) with each zone has a radius of 2 hops as shown in Figure 4 below.

![Figure 4. WSN supposed Zones.](image)

- **Step 1**: Source host D belongs to A’s Zone then the source will check whether the destination host L is within same zone or not.
- **Step 2**: If the destination host L is in same zone, then node D must be having a route to the destination host using any known proactive WSN routing protocols such (DSDV or OLSR).
- **Step 3**: If the destination host L is not at the same source host A’s zone, then node A has to send a route query (RREQ) to all its peripheral nodes namely (D,F,E,G) using DSR protocol.
- **Step 4**: When the peripheral nodes receive this route query, they will also run the same logic check whether destination host L within same their zones or not.
- **Step 5**: Since the destination host is not in G’s zone, then host G will also send a route query (RREQ) to its peripheral nodes namely (A,E,K,M) using DSR protocol.
- **Step 6**: Node K find out the destination host L is within same its zone and then return route reply (RREP) by reversing the RREQ path such as [L-K-G-A] as described in previous section of our proposed solution to overcome the route reply storm problem.

In summary of the above our proposed procedure to find out the destination over large coverage area to avoid the problem of route reply storm, we can conclude the following facts for above example WSN:

1. A’s zone peripheral nodes (D,E,F,G) uses DSR protocol for out-zone routing while the A’s zone interior nodes (C,B) uses either DSDV or OLSR routing protocol for in-zone routing.
2. G’s zone peripheral nodes (A,E,K,M) uses DSR protocol for out-zone routing while the G’s zone interior nodes (B,J) uses either DSDV or OLSR routing protocol for in-zone routing.
3. K’s zone peripheral nodes (G,M) uses DSR protocol for out-zone routing while the K’s zone interior nodes (J,L) uses either DSDV or OLSR routing protocol for in-zone routing.
3.2. Link Failure Problem

In order to verify the correctness and robustness of our proposed solution for route reply storm problem under link failure or broken at a wireless sensor network, we consider the same network shown in Figure 1 but we will consider the links B-C and F-D are broken as shown in Figure 5 below.

Figure 5. Example WSN for Link Failure Problem Verification.

The following procedure will be described how our proposed solutions dealing with these two links failure B-C and F-D so as we can solve the route reply storm problem in this situation:

**Step 1:** We will construct a directed acyclic graph (DAG) for our network example using partial reversal method as shown in Figure 6 below.

Figure 6. DAG for our Example WSN after Links Broken.

**Step 2:** After Links B-C and F-D are broken, and since node F the only one except the destination node D has no outgoing links, then node F will reverse all the entering links as shown in Figure 7 below.

Figure 7. Node F reverses all its entering links.

**Step 3:** After that each node has only entering links will reverse them, in our case node B will do it as shown in Figure 8 below. Note that node B didn’t reverse link B-F since we use partial link reversal method.
Figure 8. Node B reverses all its entering links.

Step 4: The red nodes those which have already reverses their links, now node A will reverse its entering links as shown in Figure 9 below.

Figure 9. Node A reverses its entering links.

Step 5: The red arrows refer as links already reversed. Now node S will send the reflections because it is the last node, the reflections will go to nodes A and B as shown in Figure 10 below.

Figure 10. Node S reverses its reflection links.

Step 6: The blue dotted arrows refer to the reflection control, and then reflection process will continue similarly for node A and then node B as shown in Figures 11 and 12 respectively.
Figure 11. Node A reverses its reflections links.

Figure 12. Node B reverses its reflection links.

Step 7: After that we reach to first situation shown Figure 6 that’s meaning the broken links are dropped and the route maintenance already done and we can return route reply for route request as [D,E,C,F,B,S] or [D,E,C,F,B,A,S] and may these two paths collide because of hidden terminal problem, as shown in Figure 13 below.

Figure 13. Route reply by [D,E,C,F,B,S] or [D,E,C,F,B,A,S].

In summary of above proposed procedure, we can conclude that a new network configuration is done after any link can fail and we can note also the steps from 1 to 6 represent the route discovery (RREQ) phase while the final step number 7 represents the route reply (RREP) phase which will prove and verify that our proposed solution can solve the problem of link failure against route reply storm problem.

4. Simulation Results
This section deals with the details over the all information which is utilized for experimental evaluation and results of this work. For evaluation of improving DSR protocol, the practical setups and configurations should be explored during this section first. The simulation is done using
MATLAB simulation for existing and improved DSR protocol different network conditions. Through simulation, we measured and compared the main important performance metrics such as network lifetime, average throughput, average energy consumption and PDR. First we discussed the information on simulation background and simulation parameters for proposed work. Then we presented the animated and experimental results for each case (i.e. coverage and link failure problems).

4.1. Simulation Considerations
For every simulation work, there should be the set of assumptions and settings in considerations. For this work, we designed this set with required level of assumptions in simulation background to design and simulate the wireless sensor networks. Below listed are the set of assumptions made for this work:

1. For this work, multihop communication is preferred for communication among source and destination.
2. All nodes in WSN are configured with similar communication ranges and all links are bidirectional.
3. Wireless sensor networks are assumed that they can be designed and implemented by using WSN routing protocols such as DSR with our improvements on it.
4. Networks are assumed that they are designed by considering two main WSN problems including coverage problem and link failure problem.
5. The network duty cycle is assumed to be 100% which means the network is always active.
6. The time units of the simulation clock are approximately 1 second.

4.2. Performance Parameters
To evaluate and verify the work of DSR protocol with our proposed solution for route reply storm problem under two main problems considered in this work, the following performance metrics be chosen:

1. **Network Lifetime**: It is the indicating time of one network sensor node cannot send data packets because of energy running out so this sensor node may be lost which means losing some network functions as well. So we can define the network lifetime as a ratio of still living nodes (active nodes) to energy running out nodes (dead nodes). Then, network lifetime ratio can be given by equation (1):

   \[
   \text{Network Lifetime} = \frac{\text{No of active nodes}}{\text{No of dead nodes}}
   \]  

2. **Average Energy Consumption**: This metrics calculates the average energy consumed in network for the particular time duration in which network is operable. So, mathematically, it is determined as a ratio of overall energy consumed by all sensor nodes in network to the overall number of sensor nodes in this network as given in the following expression of equation (2):

   \[
   \text{Average Energy Consumption} = \frac{\Sigma \text{Energy consumed by each node}}{\Sigma \text{number of overall nodes}}
   \]  

3. **Average Throughput**: This parameter metrics determines the overall packets sent per second and represent the total number of messages sent per second. So, the average throughput can be considered as the total number of bytes that reside in the target destination. This means that it can be calculated as the average number of packets received per amount of time. It is computed by using below formula in equation (3):

   \[
   \text{Average Throughput} = \frac{\text{Overall No of received byte} * 8}{(\text{Last received packet} - \text{First received packet})}
   \]
4. **Packet Delivery Ratio (PDR):** It is the percentage of successful messages received at receiver end. For computing the PDR, we need to have overall number of generated packets and total number of successful received packets. So, this ratio can be calculated by equation (4):

\[
\text{Packet Delivery Ratio} = \frac{\text{Total No. of received packets}}{\text{Total No. of generated packets}} \times 100\% \tag{4}
\]

4.3. **Simulation Configurations**

Two modules are considered as shown below describing the network scenarios and parameters used for this simulation work which can be used to simulate the wireless sensor networks under two considered problems (coverage and link failure) in below modules.

- **Module –I: Coverage Problem Case**
  - Routing Protocol: DSR, DSR with Proposal Solution (RREQ & RREP)
  - Number of Sensor Nodes: 90
  - Size of Network: 1200 * 1200
  - MAC Protocol: IEEE 802.11
  - Simulation Time: 60 sec
  - Nodes Mobility: 20 m/s
  - Topology: Random
  - No. of Coverage Zones: 3
  - Reporting Rate: 10, 20, 30, 40, 50, 60 packets/second

- **Outputs:**
  - Active nodes vs. Network Lifetime
  - Remaining Energy vs. Network Lifetime

- **Module –II: Link Failure Problem Case**
  - Routing Protocol: DSR, DSR with Proposal Solution (RREQ & RREP)
  - Number of Sensor Nodes: 90
  - Size of Network: 1200 * 1200
  - MAC Protocol: IEEE 802.11
  - Simulation Time: 60 sec
  - Nodes Mobility: 20 m/s
  - Topology: Random
  - Source and Destinations: 5
  - No. of Queues: 3
  - Proposed Broken Links: 2, 3, and 4
  - Reporting Rate: 10, 20, 30, 40, 50, 60 packets/second

- **Outputs:**
  - Active nodes vs. Network Lifetime
  - Remaining Energy vs. Network Lifetime

4.4. **Experimental Results**

As per the objectives of this work, we have simulated and evaluated our proposed solution of DSR protocol against existing DSR protocol for wireless sensor networks. In this section we are presenting the results achieved through the experimental simulation work. We have designed network of WSN using 90 users with three sources and one destination in order to claim the efficiency of DSR protocol. The comparative study is presented by varying total number of packets sent per second such as 10, 20, 30, 40, 50 and 60 packets per second. There are main performance metrics which we used for comparative analysis like network lifetime, average energy consumption and packet delivery ratio that mentioned above.
Graphs in Figures 14 and 15 are indicating the scalability and reliability of our proposed solution of DSR protocol under coverage problem consideration. The Network lifetime is varied from 0 to 300 rounds in we have computed the number of active nodes in standard DSR protocol against our improved DSR protocol. The DSR protocol with more number of active nodes at each round interval is considered is efficient approach as showing in Figure 14. Similarly, the remaining energy performance is also checked by varying network lifetime under coverage problem consideration for both standard DSR protocol and our improved DSR protocol as shown in Figure 15 taking into account our solution to solve coverage problem by supposing three consequent zones to reach each destination sensor node.

![Graph showing Active Nodes vs. Network Lifetime under Coverage Problem Case](image1)

**Figure 14.** Active Nodes vs. Network Lifetime under Coverage Problem Case.

![Graph showing Remaining Energy vs. Network Lifetime under Coverage Problem Case](image2)

**Figure 15.** Remaining Energy vs. Network Lifetime under Coverage Problem Case.

In similar way, graphs in Figure 16 and 17 are indicating the scalability and reliability of our proposed solution of route reply storm problem using DSR protocol. At these two Figures, The Network lifetime
is varied from 0 to 300 rounds in we have computed the number of active nodes in standard DSR protocol and our improved DSR protocol taking into account link failure problem case. The method with more number of active nodes at each round interval is considered are efficient method as showing in Figure 16. Then, improved DSR protocol is having more number of active nodes as compared to both standard DSR protocol. Similarly, the remaining energy performance is also checked by varying network lifetime as shown in Figure 17 below.

5. Conclusions
One of the most important challenges in designing any wireless sensor network routing protocol is to reduce power consumption and extend network life. Therefore, certain routing protocols must meet certain requirements, such as high bandwidth, low latency, reliable communication and wide coverage. Other protocols may consider important functions of sensor nodes, such as low power consumption
and low bandwidth; therefore, routing protocols designed to forward information to designated base stations will affect the overall performance of the wireless sensor network. In this work, we developed the basic path detection and path maintenance mechanisms deployed via DSR, and proved how they manage wireless portable nodes to compose a self-organizing and self-configuring wireless sensor network between them. The simulation results achieved for two routing protocols DSR protocol and proposed improved DSR protocol for energy efficiency parameters. The energy consumption of proposed approach is minimized by 25 % approximately as compared to previous standard DSR protocol. The network lifetime performance is increased by approximately 35 % as compared to standard DSR protocol. Overall the proposed solution of DSR protocol achieved energy efficiency for wireless sensor networks resource management. Our current work includes further improvements to DSR performance, such as allowing expansion to bigger networks, and adding smart properties to the protocol, such as multicast routing, adaptive quality of service (QoS) reservation and radio bandwidth allocation. Finally, our target is achieved by improving DSR protocol so as it can work properly against some deviated problem that may face it through working such as coverage challenge and link failure or broken suddenly happened at any time. We also verified these two unwanted problems taking two case studies explained in details in previous section.

References
[1] Quy, Vu Khanh, Nguyen Tien Ban, Vi Hoai Nam, Dao Minh Tuan, and Nguyen Dinh Han. "Survey of recent routing metrics and protocols for mobile Ad-hoc networks." Journal of Communications 14, no. 2 (2019): 110-120.
[2] Saudi, Nur Amirah Mohd, Mohamad Asrol Arshad, Alya Geogiana Buja, Ahmad Firdaus Ahmad Fadzil, and Rairhana Md Saidi. "Mobile ad-hoc network (MANET) routing protocols: A performance assessment." In Proceedings of the Third International Conference on Computing, Mathematics and Statistics (iCMS2017), pp. 53-59. Springer, Singapore, 2019.
[3] Mohapatra, Durga Prasad, and Srikanta Patnaik, eds. Intelligent Computing, Networking, and Informatics: Proceedings of the International Conference on Advanced Computing, Networking, and Informatics, India, June 2013. Vol. 243. Springer Science & Business Media, 2013.
[4] Kadhim, Dheyaa Jasim, and Omar Abdulsattar Hamad. "Improving IoT Applications Using a Proposed Routing Protocol." Journal of Engineering 20, no. 11 (2014): 50-62.
[5] Sarkar, Priyanka, and Hrituparna Paul. "Comparative performance analysis of GZRP, AOMDV and DSR in MANETs." (2013): 175-178.
[6] Kadhim, Dheyaa Jasim. "Performance Evaluation of AODV Routing Protocol in MANET using OPNET Simulator." Anbar Journal of Engineering Sciences 5, no. 2 (2012): 241-257.
[7] Hayder, Syed Irfan. "A Comprehensive Performance Comparison of On-Demand Routing Protocols in Mobile Ad-Hoc Networks." In International Conference on Future Generation Communication and Networking, pp. 354-369. Springer, Berlin, Heidelberg, 2010.
[8] Hussien, Anas Ali, and Safa Ihsan Matloob. "The comparative study some of reactive and proactive routing protocols in the wireless sensor network." Journal of University of Babylon for Engineering Sciences 26, no. 4 (2018): 195-207.
[9] Lafta, Wisam Mahmood, Saba Qasim Jabbar, Dheyaa Jasim Kadhim, and Guangzhi Ma. "Heterogeneous Network Performance Improvement Using Proposed OLRED and OLVRED Strategies." International Journal of Future Computer and Communication 5, no. 5 (2016): 199.
[10] Sumathi, R., and M. G. Srinivas. "A survey of QoS based routing protocols for wireless sensor networks." Journal of Information Processing Systems 8, no. 4 (2012): 589-602.
[11] Nayyar, Anand, and Rajeshwar Singh. "Simulation and performance comparison of ant colony optimization (ACO) routing protocol with AODV, DSDV, DSR routing protocols of wireless sensor networks using NS-2 simulator." American Journal of Intelligent Systems 7, no. 1 (2017): 19-30.
[12] Mahmoud, Waleed A., and Dheyaa J. Kadhim. "A Proposal Algorithm to Solve Delay Constraint Least Cost Optimization Problem." Journal of Engineering 19, no. 1 (2013): 155-160.
[13] Aljiznawi, Raed Abduljabbar, Naseer Hwaidi Alkhazaali, Saba Qasim Jabbar, and Dheyaa Jasim Kadhim. "Quality of service (qos) for 5g networks." International Journal of Future Computer and Communication 6, no. 1 (2017): 27.

[14] Siddiquee, Kazy Noor E. Alam, Faria Farjana Khan, Karl Andersson, and Mohammad Shahadat Hossain. "Optimal dynamic routing protocols for agro-sensor communication in MANETs." In 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), pp. 1-5, 2017.