

# A Hotline-Based Reliable Topology for Wireless Sensor Networks<sup>\*</sup>

Ali Tufail<sup>1</sup>, Syed Ali Khayam<sup>2</sup>, Son Dong Hwan<sup>1</sup>, Ki-Hyung Kim<sup>1</sup>

<sup>1</sup> Graduate School of Information and Communication, Ajou University, Suwon, South Korea

<sup>2</sup> School of Electrical Engineering and Computer Science, NUST, Rawalpindi, Pakistan

**Abstract--** Many anticipated deployment scenarios, in particular military, healthcare, and disaster-recovery applications, of Wireless Sensor Networks require reliable source to sink communication. In this paper, we introduce a novel reliable topology that uses hotlines between sensor gateways to enhance the reliability of end-to-end transmissions. These hotlines reduce the number of average hops from source to the sink and serve as reliable and efficient backbone routing alternatives. We show analytically that communication using hotlines is noticeably more reliable than traditional Wireless Sensor Networks routing.

**Keywords:** WSN, Reliability, Backbone Routers

## I. INTRODUCTION

Recent developments in Wireless Sensor Networks (WSNs) have brought this domain from merely a concept of microelectronics to a new realm of practical applications. A WSN generally comprises of a large number of low powered, low cost, memory/computationally-constrained, intelligent sensor devices. These sensors are generally involved in detecting and measuring some target phenomena.

Due to its inherent energy, footprint and deployment constraints, a WSN is prone to faults and malfunctioning. These faults can be due to hardware/software failures or energy depletion. In hostile deployments, the faults may be caused by natural or human adversaries, e.g., natural disasters in calamity-struck regions or radio jamming in a battlefield [1]. Despite WSN's fault-prone characteristics, mission-critical natures of emerging WSN applications (e.g., military, healthcare, and disaster recovery applications) require that communication to/from sensors is dependable and reliable. The source to sink communication in WSNs is generally dependent on the intermediate relaying sensor nodes. Therefore the reliability of a transmission is dependent on the topology and routing techniques being deployed in the WSN.

In this paper, we propose to enhance WSN routing reliability using high-reliability hotline links between sensor gateways. A WSN typically contains multiple resourceful gateway nodes that provide load balancing, local cluster management and energy saving [2], [3]. Since these gateways are far fewer in number than the sensor nodes, we introduce the concept of using hotline (e.g., high speed Ethernet links) for inter-gateway communication, while traditional multi-hop techniques can be used by the sensors for intra-gateway communication. In addition to load balancing, with multiple hotline-connected gateways we are able to achieve reliable source to sink communication. This paper describes our proposed topology in detail. This is followed by analytical modeling and comparison of hotline-based and traditional WSN communications. Our analytical results show that significant improvements in reliability can be achieved using a hotline based topology.

The rest of this paper is organized as follows. Section 2 outlines related work in this area. Section 3 describes our network model and assumptions. Section 4 explains hotline-based reliable communication topology. Section 5 focuses on the mathematical evaluation and comparison of the proposed topology with existing WSN communications. Section 6 summarizes key conclusions of this work and our future directions.

## II. RELATED WORK

The nodes deployed in a WSN are generally large in numbers and are deployed in close proximity. Therefore there is an intrinsic manageability issue in WSNs. Large number of nodes in WSN can be managed by deploying more than one gateway. Multiple gateway based architecture for IPv6-based Low-power Wireless Personal Area Network (6LoWPAN) has been proposed in [4]. Authors in [4] show that their proposed architecture allows a sensor network to achieve better communication performance. Increase in number of gateways would cost additional hardware resources therefore a tradeoff is required. In [5], the authors propose an intelligent estimation approach to calculate least number of gateways required to fulfill certain data latency threshold. They also discuss the impact of location of gateways on the operation of the network. With the known least number of gateways, arises the need to position gateways in an appropriate layout to meet certain network parameters. An optimum layout for the position of gateways has been proposed in [6]. Authors show that the location of gateways has a marked influence on the data rate and overall power efficiency of the network.

In [2], an algorithm to divide network sensor nodes into well-defined clusters is proposed. A similar topology was also proposed in [3], where the problem is referred to as the Load-Balanced Clustering Problem (LBCP). They argue that clustering improves the stability and enhances the inter node communication. The main idea in [7] is of a forwarding scheme for reliable and energy-efficient data delivery in a cluster-based sensor network. [8] defines reliability of WSNs in terms of two factors: 1) type of the message, and 2) scope of the delivery. Reference [9] discusses the tradeoffs of enhancing the reliability of WSN in a ZigBee network. In [10], the concept of multiple gateways for efficient routing and data delivery within the 6LoWPAN is proposed.

A wireless network that uses few wired links as opposed to all wireless links is known as small-world network, derived from the idea of small world graphs. This network topology has been proposed in [11], where the authors discuss the concept of using wires in some of their links to enhance energy efficiency but they do not evaluate the impact of such a topology on WSN reliability.

<sup>\*</sup> This work is supported by the Brain Korea Project (BK21)

Limited energy at each node has been widely recognized as the main barrier to the deployment of WSNs. A backbone approach has therefore been considered as a viable option for enhancing the overall lifetime of a WSN. Authors in [12] suggest that a construction of energy efficient backbone prolongs network lifetime, brings stability and scalability. Whereas in [13] authors present Sensor DMAC which reduces the overhead of node selection, backbone formation and maintenance, thus increases the overall network lifetime. [14] talks about a protocol for building and maintaining a connected backbone. Their design criteria produce a backbone that can be reconfigured quickly with very little overhead.

Our work is quite different than the prior work described above. While we have utilized few concepts like clustering and multiple gateways from [2]-[10], small world graphs from [11], backbone approach from [12]-[14] and gateway association mechanism from [4], our emphasis is on addressing the reliability issues in WSN using the concept of hotlines between gateways. Most of the previous work, especially in backbone approach, focuses on energy efficiency in WSNs whereas we have combined versatile concepts, like backbone, clustering, hotlines, to suggest and evaluate reliable topology over WSNs.

### III. NETWORK MODEL AND ASSUMPTIONS

In this section we define the basic topology and assumptions of our network model.

We assume a WSN with two-level heterogeneity. At the first level, we have resource-constrained sensor nodes which are deployed densely on a two-dimensional grid. All of the first level nodes have the same resources. At the second level, we have sensor gateways that operate as cluster heads to regulate the flow of traffic and to manage sensor nodes deployed in the given geographical region. The gateways are not resource-constrained and their density is many orders of magnitude lesser than the density of the sensor nodes. Gateways are connected to each other in a bus topology. In the traditional topology, the bus is constructed using long-haul wireless links. Under the proposed hotline-based topology, the gateways are connected via Ethernet cables.

### IV. HOTLINE-BASED RELIABLE WSN TOPOLOGY

We now introduce the important components of our proposed hotline-based reliable WSN topology. Different mechanisms, like dividing the network into clusters, gateway association/dissociation and node-node, node-gateway and gateway-gateway communication will be described in detail in the following sub-sections.

The role of multiple gateways can be made useful in WSN if they are thought of connected as a bus. Gateways are therefore being used to provide an alternative and reliable path for packet routing.

In traditional WSN routing the expected path of end-to-end communication would include multiple hops. The packet delivery is dependent on several intermediate relaying sensor nodes. These sensor nodes would be required to forward the

packets until they reach their destination. WSN has inherent high link error rate and with multi-hop routing the error rate can be as high as 30% [15]. The chances of failure are likely to increase with every additional hop. Reliability is therefore a main concern for deployment of WSN for applications like in military and health care. Our suggested topology addresses the reliability issue by using the concept of hotlines between gateways. Hotlines noticeably reduce the number of average hops between source to destination and provide better reliability as compared to traditional WSN routing.

Figure 1 shows our hotline assisted topology where four gateways are connected to each other as a bus network. This bus network is not only connecting gateways to each other but also connecting gateways to outer world (Internet or IPv6 domain). We would describe the topology in detail in the following sections.

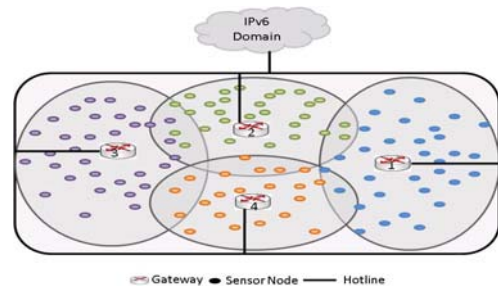


Figure 1: Hotline deployed WSN Topology.

#### A. Network Clusters

Due to the availability of gateways, we can efficiently organize and manage the sensor nodes in a network. Each node would have to associate to a particular gateway making it the default gateway. All the nodes associated to one gateway form one cluster.

One of the important benefits of the clustering approach is to facilitate efficient and reliable communication using gateway hotlines. For example, one set of nodes is sensing the environment to get the data and then that data is being sent to another set of nodes or a sink for further computation. The default gateways can provide a fast and reliable routing mechanism to communicate this data.

Nodes become the part of a cluster depending upon their hop count from the gateway. The nodes would get associated to any gateway as mentioned in [4]. The routers would send router advertisement (RA) messages to help the nodes to associate to a particular gateway. When a sender node receives RA messages from several routers, it would differentiate the messages with help of current time to live (Cur TTL) field. It must be noted that Cur TTL has been modified. Every router sets the value of Cur TTL field to be 255 and with each hop the value is decreased by 1. So the nodes get associated to the router with a maximum Cur TTL, since a higher value of Cur TTL implies less hop count to that router.

#### B. Inter-Node Communication

Under traditional ad hoc routing algorithms like AODV and DSR [16], when a node S has to send data to a destination D,

routes are discovered using a flooding mechanism. As shown in the Figure 2, sender S does not know the path to destination D so the source floods the network with a route request (RREQ). RREQ is then rebroadcasted by every node that receives the message, until it reaches the destination or an intermediate node that has a fresh route to the destination in its cache. The destination node or the intermediate node then replies with a route reply (RREP). As shown in the Figure 2, the route with dotted line is one of the routes discovered using a traditional routing algorithm. Due to the large number of intermediate wireless hops, a message sent through that path would likely be dropped due to wireless channel errors and will also be incurring high end-to-end delay.

In our proposed topology as we have divided the network into different clusters and each cluster is associated with a default gateway. The routing of packets and route discovery is done within the cluster using RREQs. Our approach of intra cluster routing is closer to the approach suggested in [8,10]. (We recommend OSPF for gateway-to-gateway routing, as will be explained in the next section.) All the traffic (inter/intra-cluster and to/from the Internet) is routed through the gateway. The only exception here is the border nodes which are discussed later. Instead of an end-to-end wireless path, a packet is now routed through wireless-wired-wireless path, where the wired path is the communication between gateways via hotline and the wireless paths are used for intra-cluster communication. This approach clearly enhances the reliability of an end-to-end transmission. Under traditional routing, the path discovery process will discover an end-to-end wireless path. This path is less reliable, as shown in the Figure 2, because the packet will traverse many wireless hops and with every hop there is an inherent threat of packet loss due to a variety of reasons like channel errors, collisions, and dead or sleeping nodes. Moreover, under this approach, a number of sensor nodes are acting as relaying nodes. Consequently, more energy is consumed on sensors which results in a shortened network lifetime.

Figure 2 also shows the hotline-assisted path that provides more reliable routing and involves lesser number of hops than traditional routing. A path discovery (RREQ) message will now reach from sender S to the default gateway. The default gateway will route the RREQ packet to the destination gateway. The destination gateway will then route the packet to the destination. The resultant route is more reliable and helps to conserve the energy of individual nodes thereby increasing the network lifetime.

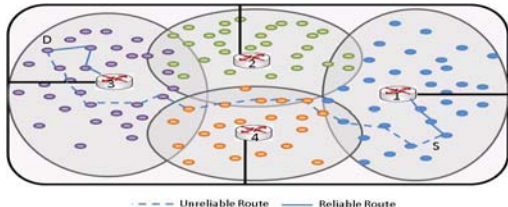


Figure2: Traditional unreliable route and hotline assisted route.

### C. Border Nodes

In a scenario where the source to sink communication is only a few hops but source-gateway-gateway-sink communication has

more number of hops then it would be expensive to communicate using the longer path (i.e. hotline assisted). It would be expensive in terms of overall latency and energy consumption. This case is likely to be true if both the source and the sink are on the border (or overlapping region) of two different clusters. We call these nodes as border nodes and propose a slightly different routing mechanism for communication between them. This mechanism would help towards efficient and reliable communication between the border nodes. The first task is therefore to identify the border nodes.

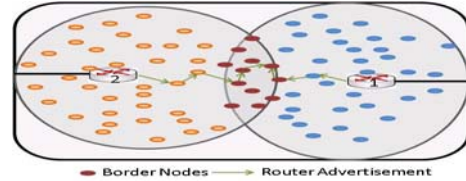


Figure 3: Border nodes can communicate to each other directly.

For simplicity, we take the example of two clusters and two associated default gateways. It can be seen from Figure 3 that nodes in the overlapping region of two clusters are defined as border nodes. The sample node lies in the overlapping region of cluster 1 and cluster 2 because it receives two RA messages from two routers. This node is now responsible for two decisions one is to join a particular gateway and the other is to broadcast or forward the RA messages of the gateways. This decision depends on the value of Cur TTL field in the RA message. Let us take an example scenario. If the node gets a RA message from gateway 1 with Cur TTL value of 252 and another RA message from gateway 2 with Cur TTL of 250, the node would join the gateway with a higher value of Cur TTL and at the same time would broadcast the RA message. It should be noticed here that the Cur TTL field represents the hop count towards the gateway.

In a scenario where a node receives two RA messages from two different gateways with the same value of Cur TTL it can join either of the gateways. The node would forward both the RA messages to its neighboring nodes.

These border nodes when have to send a packet, for instance, they would check from the neighbor table whether the packet is destined to their first hop neighbor. If the packet is destined to the first hop neighbor they would deliver it directly no matter the neighbor belongs to other cluster.

### D. Inter-Gateway Communication

The gateways are connected using high-speed Ethernet cables. Gateways are supposed to exchange certain information that would be required for routing and monitoring the state of the links. Our sensor network has been divided into clusters but overall network can be considered as one autonomous system (AS). We therefore require a protocol configured in gateways that can handle cluster to cluster (Intra-AS) communication. We propose to employ the widely-used Open Shortest Path First (OSPF) protocol for inter-gateway communication. We choose OSPF because of two main reasons: 1) In distance vector routing protocols, each router does not possess information about the complete network topology and consequently there is a slow convergence problem [17]; 2) OSPF works over IP and has a

richer set of extensions and added features [17] as compared to other link state and distance vector routing protocols.

Each gateway has information saved about nodes of the complete network in form of a gateway network table. Every time a node is added or removed from a particular cluster, an update is sent to the default gateway. The default gateway accordingly updates the gateway network table. An update message is eventually sent to all the gateways of the network connected via the hotline. This completes one cycle of the update mechanism. This process is already supported in OSPF by the database synchronization mechanism [17]. The synchronization process begins as soon as the gateway attempts to bring up the adjacency. The database is described by each gateway by sending a series of Database Description packets to its neighbors. As gateways are connected in a bus network, via hotline, all the gateways will synchronize their databases.

Gateways are also deployed with a monitoring mechanism. Specifically, gateways are aware of the health of neighboring gateways and the corresponding links. This monitoring mechanism helps to ensure the connectivity of the gateways and eventually ensuring the availability of the hotline. This mechanism is supported by the OSPF Hello protocol. The neighbor relationship is maintained with the help of the Hello Protocol. It is also responsible of ensuring the bidirectional communication between neighbors. Hello packets are sent periodically on all router interfaces [17].

In summary gateways are configured with dual functionality. They are deployed with two different protocols. One protocol (AODV) is used for intra-cluster or cluster-node communication, the other protocol (OSPF) is used for inter-gateway communication.

## V. RELIABILITY MODEL AND EVALUATION

In this section, we model and compare the reliability of an end-to-end WSN communication under traditional and hotline-assisted routing. Our network has two different homogenous Poisson distributions. The normal sensor nodes are deployed according to a dense homogeneous Poisson distribution and gateway nodes are deployed according to a sparse homogenous Poisson distribution. Throughout this section, we consider a one-dimensional deployment scenario for simplicity.

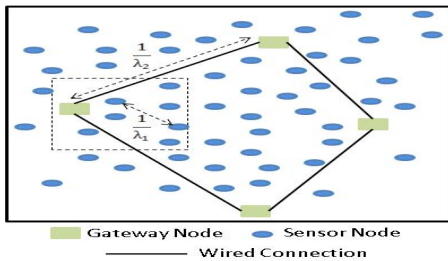


Figure 4: Network model showing distribution scenario of sensor nodes and sensor gateway nodes.

We assume that there are  $\lambda_1$  arrivals of sensor nodes per unit area. In other words there are, on the average,  $\lambda_1$  occurrences of sensor nodes per unit area. As shown in Figure 4, we can

conclude that the average distance between two neighboring nodes in a unit distance will be  $\frac{1}{\lambda_1}$ . Similarly on the average there are  $\lambda_2$  occurrences of sensor gateway nodes per unit distance. The average distance between two neighboring sensor gateway node is therefore  $\frac{1}{\lambda_2}$ . The gateway nodes are connected to each other via a backbone wired link and the occurrences of gateway nodes per unit distance are significantly lesser than that of sensor nodes, leading to the following relation:  $\lambda_2 \ll \lambda_1$ .

Alternatively, we can write the above equation as:

$$\lambda_2 = \alpha \lambda_1, \quad (1)$$

where  $0 < \alpha < 1$

$\alpha$  is the ratio of the gateway node occurrence with respect to the number of sensor nodes per unit distance. The value of  $\alpha$  would vary depending upon specific scenario or the density of sensor nodes and sensor gateway nodes in a given network. If  $\alpha$  is closer to 1 then the network is expected to be a well managed network with a high number of gateway nodes.

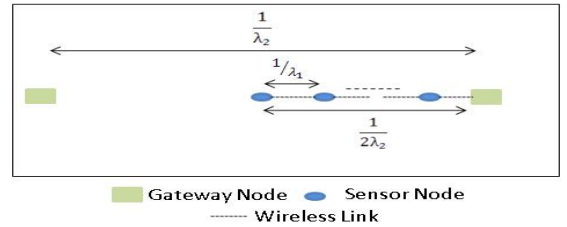


Figure 5: Worst case scenario with a sensor node lying exactly in the middle of two gateway nodes.

We want to compute the reliability and resilience of our proposed topology against the traditional WSN routing mechanism. We take the worst case scenario where we consider a border node that lies exactly at the center of two gateway nodes as shown in the Figure 5. As we already know that the average distance between two gateway nodes is  $\frac{1}{\lambda_2}$ . The node that lies right in the middle of two gateway nodes would have  $\frac{1}{2\lambda_2}$  distance to either of the gateway nodes. But we know that the average distance between two neighboring sensor nodes is  $\frac{1}{\lambda_1}$ . Using (1), we obtain:  $\frac{1}{2\lambda_2} = \frac{1}{2\alpha} \frac{1}{\lambda_1}$ .

In the above equation  $\frac{1}{2\alpha}$  is the factor that provides us required number of  $\frac{1}{\lambda_1}$ 's to cover the whole distance of  $\frac{1}{2\lambda_2}$ .

We are now interested in quantifying the reliability of the traditional and hotline-assisted scenarios. The reliability of communication between a sender and a receiver is the end-to-end probability of successful transmission. As shown in Figure 6(a), there is no gateway available so the reliability would depend on the number of hops,  $n$ , between the sender and the destination. Each of the hops would have same probability of

successful packet transmission; we call this probability  $P_1$ . The reliability without gateway nodes is then:  $(P_1)^n$

In order to find out the reliability of the scenario when gateway nodes are assisting the routing, the overall reliability would be dependent on three different phases. One is the probability of packet reaching from source to the associated source gateway, say  $P_1$ , second is the probability of packet reaching from the source gateway to the destination gateway, say  $P_2$ , and lastly the probability of packet reaching from the associated destination gateway to the destination, which in worst-case is  $P_1$ . This scenario is shown in the Figure 6(b).

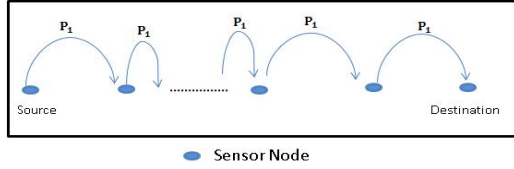


Figure 6(a): Probability of reliable packet transmission without gateway nodes.

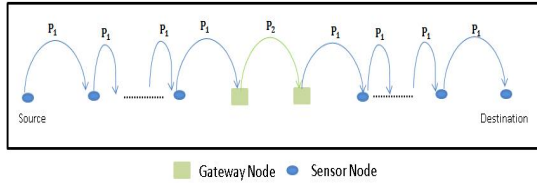


Figure 6(b): Probability of reliable packet transmission with gateway nodes.

We know that in our particular example the probability of successful transmission of packets on wireless domain, where they also have more number of hops, would be much less than that of the hotline-assisted gateway-to-gateway transmission. So we now have the relation:  $P_1 \ll P_2$ .

The above equation can be written as:  $P_1 = \beta P_2$ ,

where  $0 < \beta < 1$ .

The probability of successful transmission in hotline assisted scenario is:

$$(P_1)^{1/2\alpha} (P_2)^h (P_1)^{1/2\alpha} = (P_1)^{1/\alpha} (P_2)^h, \quad (2)$$

where  $h$  is the number of wired hops between source and destination gateway nodes. The minimum value of  $h$  is 1.

In case of traditional all wireless routing, the distance covered by the wired path in a hotline-assisted routing scenario will be replaced by a wireless path. We already know that the average distance between two neighboring gateway nodes is  $1/\lambda_2$  as shown in the Figure 4. From equation (1) we know that  $1/\alpha$  represent the number of wireless hops in the given scenario. To cover the whole distance of  $h$  wired hops, we need the following number of wireless hops:

$$\text{Average Number of Replaced Hops} = h \times \frac{1}{\alpha}.$$

In order to get probability for all wireless successful packet transmission we would get the following equation:

$$(P_1)^{1/2\alpha} (P_2)^{h/\alpha} (P_1)^{1/2\alpha} = (P_1)^{(h+1)/\alpha}. \quad (3)$$

If we compare Equation (2) and (3) we would get:

$$(P_1)^{1/\alpha} (P_2)^h \neq (P_1)^{(h+1)/\alpha}$$

$$(P_2)^h \neq (P_1)^{h/\alpha}.$$

If we evaluate the above equation we can find out the reliability of both the scenarios as highlighted in figure 6(a) and (b). Since  $P_2 \gg P_1$ ,  $0 < \alpha < 1$ , and  $h$  is a positive integer, we have:

$$(P_2)^h \gg (P_1)^{h/\alpha}. \quad (4)$$

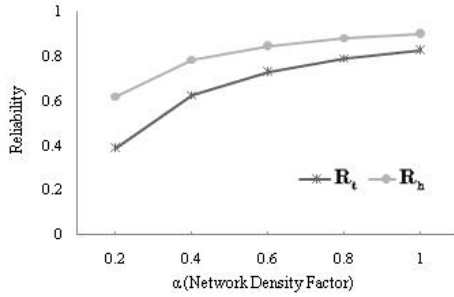
From Equation (2) and (3) we can assume that the hotline assisted reliability is represented by  $\mathbf{R}_h$  and traditional routing reliability is represented by  $\mathbf{R}_t$ . From Equation (4) we know that the following relation should hold:  $\mathbf{R}_h \gg \mathbf{R}_t$ .

Figure 7 compares the reliability of packet transmission in the case when routing is supported by our proposed hotline assisted gateways with the case when the routing is done in a traditional manner. The graphs are drawn against varying values of  $\alpha$ .

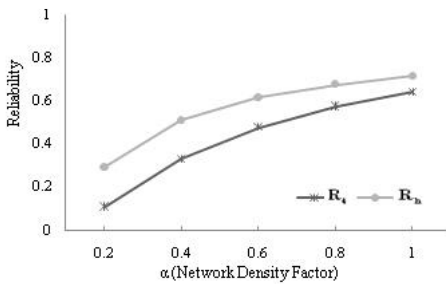
In Figure 7(a) and (b), we use  $h = 1$ . In other words, the number of wired hops between the source and destination gateways is one. Figure 7(a) shows that in case of hotline assisted routing, where the probability of successful packet transmission is assumed to be 0.99, the reliability ( $\mathbf{R}_h$ ) would be dependent on the value of  $\alpha$ ; or the relative densities of sensor and gateway nodes. An increase in  $\alpha$  would increase the reliability of WSN and vice versa. If the value of  $\alpha$  is less, automatically the deployed gateway density reduces, and therefore the reliability of WSN is low. Although in the case of traditional all wireless routing, where the probability of successful packet transmission is assumed to be 0.91, the reliability ( $\mathbf{R}_t$ ) is dependent on the value of  $\alpha$ , but  $\mathbf{R}_t$  is always much less than  $\mathbf{R}_h$  with any given value of  $\alpha$ . This is due to the fact that hotline assisted topology is routing packets through more reliable (wired) links and fewer un-reliable (wireless) hops, Traditional routing, on the other hand, is routing packets through end-to-end unreliable wireless hops.

In Figure 7(b), we have kept all the factors constant but have reduced the probability of successful packet transmission for both  $P_1$  and  $P_2$ . The graph shows that the value of  $\mathbf{R}_h$  is still high than the value of  $\mathbf{R}_t$  for any given value of  $\alpha$ . Please note that the reliability is much less than that provided in 7(a) due to the fact that reliability in our proposed approach is directly

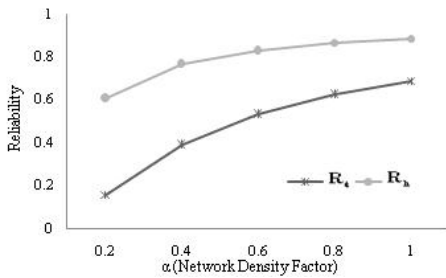
proportional to the probability of successful packet transmission, provided value of  $h$  is constant. With very low value of  $\alpha$  the value of  $\mathbf{R}_t$  is observed to be very low and is much lesser than that of  $\mathbf{R}_h$ , therefore traditional routing provides much less reliability as compared to the proposed hotline assisted gateway routing.



(a):  $P_2 = 0.99$   $P_1 = 0.91$ ,  $h = 1$  and varying  $\alpha$



(b):  $P_2 = 0.89$   $P_1 = 0.80$ ,  $h = 1$  and varying  $\alpha$



(c):  $P_2 = 0.99$   $P_1 = 0.91$ ,  $h = 3$  and varying  $\alpha$

Figure 7: Comparison of hotline based reliability with traditional wireless reliability

In the Figure 7(c) we have increased the number of wired hops (i.e.  $h$ ) from 1 to 3. The increase in wired hops has triggered a dramatic decrease in the overall reliability of traditional all wireless routing ( $\mathbf{R}_t$ ). This is a direct consequence of the fact that in the traditional (all wireless) scenario many new wireless hops are needed to cover the distance that would be covered by the hotlines in our proposed topology. These new wireless hops are inherently unreliable and result in significantly increased packet losses. A slight decrease in the reliability of hotline assisted routing is also observed in Figure 7(c). This reduction in reliability is, nevertheless, negligible in comparison with the reliability penalties incurred by the all-wireless traditional routing scheme.

## VI. CONCLUSION AND FUTURE WORK

In this paper, we showed that gateway nodes in WSNs can be utilized to improve the reliability of WSN communications. We proposed a hotline-based topology to increase the reliability of inter-gateway paths. The proposed topology improved reliability and energy-efficiency of end-to-end WSN communications. We showed mathematically that hotline assisted routing gives noticeably better reliability in comparison to traditional all-wireless ad hoc routing. Moreover, our proposed topology provides reliability which is independent of the number of nodes in a given cluster. This property makes it a good choice for high density WSN deployments. As a future work, we will perform simulation and implementation of the proposed approach on a real WSN test bed. We are also investigating the energy efficiency and network lifetime improvements provided by our proposed topology.

## REFERENCES

- [1] Hosam M. F. AboElFotoh, S. S. Iyengar, Krishnendu Chakrabarty "Computing Reliability and Message Delay for Cooperative Wireless Distributed Sensor Networks Subject to Random Failures," *IEEE Transactions on Reliability*, volume.54, no. 1, 2005.
- [2] Gaurav Gupta, Mohamed Younis, "Load-balanced clustering of wireless sensor networks," *IEEE International Conference on Communications (ICC)*, 2003.
- [3] Chor Ping Low, Can Fang, Jim Mee Ng, Yew Hock Ang, "Load-balanced clustering algorithms for wireless sensor networks," *IEEE International Conference on Communications (ICC)*, 2007.
- [4] Seuk Jung, Ali Hammad Akbar, Byeong-hee Roh, Ki-hyung Kim, "Multiple Routers-based Architecture for IPv6-Based Wireless Sensor Networks (6LoWPANs)," *NEXT*, 2007.
- [5] Youssef Waleed Younis Mohamed, "Intelligent Estimation of Gateways Count for Reduced Data Latency in Wireless Sensor Networks Global Telecommunications Conference," *IEEE GLOBECOM*, 2007
- [6] A. Bogdanov E. Maneva, S. Riesenfeld, "Power-aware Base Station Positioning for Sensor Networks", *INFOCOM*, 2004.
- [7] Jongsik Jung, Taekeun Park, Cheeha Kim, "A forwarding scheme for reliable and energy-efficient data delivery in cluster-based sensor networks," *IEEE Communications Letters*, vol. 9, no. 2, 2005
- [8] S. J. Park and R. Sivakumar, "MobiHoc Poster: Sink-to-Sensors Reliability in Sensor Networks," *ACM Mobile Computing and Communications Review (MobiHoc)*, 2003
- [9] Yuan Guo, Janise McNair, "Reliability enhancements for environment monitoring using wireless sensor networks," *IEEE Wireless Communications and Networking Conference (WCNC)*, 2006.
- [10] Ali Hammad Akbar, Ki-Hyung Kim, Won-Do Jung, Ali Kashif Bashir, and Seung-Wha Yoo, "GARPAN: Gateway Assisted Inter-PAN Routing for 6LoWPANs," *International Conference on Computational Science and its Applications (ICCSA)*, 2006.
- [11] G. Sharma and R. Mazumdar. "Hybrid Sensor Networks: A Small World," *ACM Mobile Computing and Communications Review MOBIHOC*, 2005.
- [12] Basagni, S. Elia, M. Ghosh, R. "ViBES: virtual backbone for energy saving in wireless sensor networks" *MILCOM 2004*.
- [13] Basagni, S., Carosi, A., Petrioli, C. "Sensor-DMAC: dynamic topology control for wireless sensor networks"  *Vehicular Technology Conference*, 2004.
- [14] Stefano B., Chiara P., Roberto P. "Efficiently reconfigurable backbones for wireless sensor networks", *Computer Communications*, vol 31, no. 4, 2008
- [15] Jerry Zhao, Ramesh Govindan, "Connectivity Study of a CSMA based Wireless Network," *USC/ISI Technical Report TR-02-774*, 2002.
- [16] C. E. Perkins et al., "Performance comparison of two on demand routing protocols for ad hoc networks," *IEEE Pers. Commun.*, 2001.
- [17] J. Moy, "Request for Comments 2328," *Ascend Communications, Inc.*, 1998