Analysis of Flow data in Wireless sensor network and method to adopt Fast routing

T. Sendhil kumar[1], A. Parthiban [2], R. Baskarane [3]
[1,2]Student Final Year M. Tech, (CSE) Department, Christ College of engineering and technology, Pondicherry University, Pondicherry, India,[1,2]
[3]Senior Assistant Professor and HOD (CSE) Department, Christ College of engineering and technology, Pondicherry University, Pondicherry, India.[3]
senshine21@gmail.com[1], parthiban139@hotmail.com, [2], csehodchrist@gmail.com.[3]

Abstract-The Analysis of flow data in Wireless Sensor Network (WSN) is important to report about efficient throughput. This paper aims to study the reliability of a data flow in wireless sensor networks with multiple hops. Initially, a method is adopted in the wireless sensor network model, to describe its terms of limited node battery energy and shadowed fading channels. We also focus on the routing protocols which might differ depending on the application and network architecture. In this paper, we present a survey of the state-of-the-art routing techniques in WSNs. Then, in order to analyze the network reliability, the network link reliability and the node energy availability are reviewed, correspondingly. Furthermore, the expressions of the instantaneous network reliability and the mean time to leave are derived. Finally, the simulation results validate the correctness and accuracy of the results.

Index Terms- Network, Routing, link consistency, flow data, Wireless Sensor Network (WSN).

1. INTRODUCTION

An Extensive analysis has been studied in many traditional wireless communication networks. Chen and Lyu [10] analyzed the end-to-end expected instantaneous reliability for wireless common object request broker architecture (CORBA) Dominiak et al. [14] analyzed the terminal-pair (two-terminal) reliability for IEEE 802.16 mesh networks. Liu et al. [15] proposed a more general region failure model to assess the reliability of wireless mesh networks affected from a region failure. Egeland and Engelstad [16] analyzed the k-terminal reliability for both planned and random wireless mesh networks. However, due to the non-repairable nodes and the limited node battery energy in WSNs, the traditional reliability evaluation methods are not applicable for WSNs.

The established wireless sensor network in the current year has integrated concepts of adapting the IPFIX protocol to the needs of wireless sensor networks have been investigated, resulting in the development of the protocol like TinyIPFIX, which is an adaptation of the IP Flow Information Export (IPFIX) protocol. The new protocol has been assessed in a representative use case involving a building application. TinyIPFIX has been extended with compression capabilities and by aggregation functionality. Furthermore, extensions to support secure data transmission have been developed, using the protocol Datagram Transport Layer Security (DTLS). The solution ensures that data collected by sensor nodes is transmitted via secure channels to a global data sink, and that authorized access is ensured from a data sink to a wireless sensor network. For validation, a system has been realized that allows configuration of the network components dynamically, and that supports visualization of the current network status and the collected data in real time. Image based flow measurement and on-site flood modeling require support that is not typically present in WSN environments: specifically, network overlay support for data-flows between nodes, support for sporadic high-bandwidth communications, and in network computing.

This paper will try to analyze the data flow in the event-driven WSNs with multiple sending and receiving turns mission approach without acknowledgments is a new technique. Considering the things from wireless links, traffic loads, energy consumptions, and node failures, a more precise system model is described for a data flow in the event-driven way. Based on the proposed system model, wireless link consistency and node energy availability are analyzed respectively. Than, the instantaneous network consistency and the mean time to leave of the data flow in WSNs are derived.

2. REQUIREMENTS OF APPLICATION DATA FLOW

The networking requirements imposed by the reporting of depth readings, in-network computational flood modeling and image-based flow analysis is as follows:

2.1. *Reporting of depth readings*

The system sends data from pressure-based depth sensors to a GSM uplink for dissemination off-site. Each sensor reading comprises a 1 byte node identifier, a timestamp and two 12 bit ADC readings, giving a total size of 5 bytes per sensor reading. Pressure sensors are sampled at intervals of five minutes and during sampling, one sensor reading is taken per second for a period of 20 seconds. Thus, depth sensors generate a predictable data flow rate of 100 bytes at intervals of five minutes, which must be relayed from 15 sensor nodes to a single gateway. Reporting of depth readings occurs during non-flood conditions and generates a classic low bandwidth many-to-one data flow from sensor nodes to the GSM gateway. This functionality is implemented by a spanning tree implementation running on the 433MHz radios [4]. Due to the ability of flood models to deal with sporadic and imperfect data, only a small cache of sensor readings is maintained at each node with comprehensive logging / archiving being performed off-site.

2.2. *In-network computational flood modeling*

The system also supports in-network computational flood modeling, which allows the system to provide flood warning functionality without the necessity of connection to off-site computational facilities [1]. The necessary per-node computation requires data (this is a sequence of sensor readings, along with predictions from the computation on the remote node) from a small number of other nodes. The flood models can tolerate latency of multiple seconds and require a maximum throughput of no more than 10kbps [5]. In-network flood modeling occurs when flooding is predicted and generates a bi-directional data flow between nodes located in geographic relevant locations. As the relevance of remote nodes is dependent upon the output of the flood model, these data flows may change dynamically. This data flow is served by an ad-hoc networking infrastructure implemented over the low bandwidth 433MHz radios. In order to ensure resiliency against data loss during critical flood periods, each node sends its last three updates along with the current update.

2.3. *Image-based flow measurement*

The system also supports image-based flow measurement. This is an emerging technique which uses cheap off the shelf digital cameras to measure flow rates [1]. Image-based flow measurement requires the dissemination of multiple high resolution images among sensor nodes, which must be distributed in a timely fashion. This requires up to 1MBPS of bandwidth and thus cannot be supported by low power radio hardware. Image based flow measurement occurs during periods of flooding and high flow rates. This generates a bi-directional high bandwidth many-to-one data flow between the nodes equipped with digital imaging hardware and nodes participating in image analysis. This is served by ad-hoc 802.11b networking. In terms of data storage, the camera-equipped nodes maintains a large cache of recent image files, while each remote node participating in the distributed image analysis will receive a set of up to 4MB of images.

3. PACKET AND FLOW-BASED TRAFFIC MEASUREMENT

It deals with the collection of traffic traces which contain packet header information and optional parts of the payload as well. Typical systems performing packet-based traffic measurements are network analyzers and network-based intrusion detection systems which analyze the captured packets directly. However, it is also possible to capture the traffic at routers and network monitors, which export the resulting measurement data to a remote analysis system. A recent IETF standard for the export of packet reports to a remote collector is the PSAMP protocol specified in RFC5476.

3.1. *Packet-based traffic measurements*

It is a high-speed networks require a lot of computation and memory assets. A less demanding alternative is flow-based traffic dimensions which gather statistics about flows of packets sharing a set of common properties called flow keys. A typical set of flow keys consists of the IP quintuple of transport protocol, source IP address, destination IP address, source port, and destination port. The IETF standard for exporting flow records is the IPFIX protocol specified in RFC5101.Further standardization initiatives concern the secure and efficient transport of monitoring data using encryption and compression methods.

3.2. *Attack and Anomaly Detection*

The detection of harmful traffic caused by attacks, worms, or botnets still is an interesting research topic. Although abundant research work has been conducted in this area, the emergence of new security threats and the ever changing characteristics of benign network utilization require a continuous research effort. The research activities in this area deal with the investigation of worm and Bonet traffic management. With the resulting knowledge, we develop innovative monitoring and detection functions which enable the detection of such malicious traffic with limited computational and memory resources. Furthermore, The methods for detecting traffic anomalies in flow data is in progress. Since many anomalies are the result of risk-free traffic variations, the principal objective is to find suitable traffic metrics and detection methods which are primarily sensitive to incidents which are of potential relevance for the network administrator.

3.3. *Traffic organization*

The Network operators are interested in identifying the traffic of different applications in order to monitor and control the exploitation of the available network resources. Since the traffic of many new applications cannot be identified by specific port numbers, Deep Packet Inspection (DPI) is the current technology of choice. However, DPI is very costly as it requires a lot of computational resources as well as up-to-date signatures of all relevant applications. Furthermore, DPI is limited to unencrypted traffic. In order to overcome the limitations and drawbacks of port and content-based traffic classification, the development of statistical classification methods has become an important area of research. As part of the LUPUS project, the primary goal is to find new traffic properties and metrics which can be derived from passive traffic measurements and which allow us to better distinguish between different protocols and applications. Thereby, we concentrate on statistical methods which are easy to implement and to deploy in real networks.

4. CHALLENGES AND DESIGN ISSUES IN WSNS

Despite the innumerable applications of WSNs, these networks have several restrictions, e.g., limited energy supply, limited computing power, and limited bandwidth of the wireless links connecting sensor nodes. One of the main design goals of WSNs is to carry out data communication while trying to prolong the lifetime of the network and prevent connectivity degradation by employing aggressive energy management techniques. The design of routing protocols in WSNs is influenced by many challenging factors. These factors must be overcome before efficient communication can be achieved in WSNs. In the following, we summarize some of the routing challenges and design issues that affect the routing process in WSNs.

4.1. *Node Deployement*

Node deployment in WSNs is application dependent and affects the performance of the routing protocol. The deployment can be either deterministic or randomized. In deterministic deployment, the sensors are manually placed and data is routed through pre-determined paths. However, in random node deployment, the sensor nodes are scattered randomly creating an infrastructure in an ad hoc manner. If the resultant distribution of nodes is not uniform, optimal clustering becomes necessary to allow connectivity and enable energy efficient network operation. Inter-sensor communication is normally within short transmission ranges due to energy and bandwidth limitations. Therefore, it is most likely that a route will consist of multiple wireless hops.

4.2. *Energy consumption without losing accuracy*

Sensor nodes can use up their limited supply of energy performing computations and transmitting information in a wireless environment. As such, energy-conserving forms of communication and computation are essential. Sensor node lifetime shows a strong dependence on the battery lifetime [1]. In a multihop WSN, each node plays a dual role as data sender and data router. The malfunctioning of some sensor nodes due to power failure can cause significant topological changes and might require rerouting of packets and reorganization of Data Reporting Model: Data sensing and reporting in WSNs is dependent on the application and the time criticality of the data reporting. Data reporting can be categorized as either time-driven (continuous), event-driven, query-driven, and hybrid [13]. The time-driven delivery model is suitable for applications that require periodic data monitoring. As such, sensor nodes will periodically switch on their sensors and transmitters, sense the environment and transmit the data of interest at constant periodic time intervals. In event-driven and query-driven models, sensor nodes react immediately to sudden and drastic changes in the value of a sensed attribute due to the occurrence of a certain event or a query is generated by the BS. As such, these are well suited for time critical applications. A combination of the previous models is also possible. The routing protocol is highly influenced by the data reporting model with regard to energy consumption and route stability.

4.3. *Node/Link Heterogeneity*

In many studies, all sensor nodes were assumed to be homogeneous, i.e., having an equal capacity in terms of computation, communication, and power. However, depending on the application a sensor node can have different roles or capability. The existence of heterogeneous set of sensors raises many technical issues related to data routing. For example, some applications might require a diverse mixture of sensors for monitoring temperature, pressure and humidity of the surrounding environment, detecting motion via acoustic signatures, and capturing the image or video tracking of moving objects. These special sensors can be either deployed independently or the different functionalities can be included in the same sensor nodes. Even data reading and reporting can be generated from these sensors at different rates, subject to diverse quality of service constraints, and can follow multiple data reporting models. For example, hierarchical protocols designate a cluster-head node different from the normal senses. These clustered can be chosen from the deployed sensors or can be more powerful than other sensor nodes in terms of energy, bandwidth, and memory. Hence, the burden of transmission to the BS is handled by the set of cluster-heads.

4.4. *Fault Tolerance*

Some sensor nodes may fail or be blocked due to lack of power, physical damage, or environmental interference. The failure of sensor nodes should not affect the overall task of the sensor network. If many nodes fail, MAC and routing protocols must accommodate the formation of new links and routes to the data collection base stations. This may require actively adjusting transmit powers and signaling rates on the existing links to reduce energy consumption, or rerouting packets through regions of the network where more energy is available. Therefore, multiple levels of redundancy may be needed in a fault-tolerant sensor network.

4.5. *Scalability*

The number of sensor nodes deployed in the sensing area may be in the order of hundreds or thousands, or more. Any routing scheme must be able to work with this huge number of sensor nodes. In addition, sensor network routing protocols should be scalable enough to respond to events in the environment. Until an event occurs, most of the sensors can remain in the sleep state, with data from the few remaining sensors providing a coarse quality.

4.6. *Network Dynamics*

Most of the network architectures assume that sensor nodes are stationary. However, mobility of both BS's or sensor nodes is sometimes necessary in many applications [19]. Routing messages from or to move nodes is more challenging since route stability becomes an important issue, in addition to energy, bandwidth, etc. Moreover, the sensed phenomenon can be either dynamic or static depending on the application, e.g., it is dynamically in a target detection/tracking application, while it is static in forest monitoring for early fire prevention. Monitoring static events allow the network to work in a reactive mode, simply generating traffic when reporting. Dynamic events in most applications require periodic reporting and consequently generate significant traffic to, be routed to the BS.

4.7. *Transmission Media*

In a multi-hop sensor network, communicating nodes are linked by a wireless medium. The traditional problems associated with a wireless channel (e.g., fading, high error rate) may also affect the operation of the sensor network. In general, the required bandwidth of sensor data will be lower, on the order of 1-100 KB/s. Related to the transmission media is the design of medium access control (MAC). One approach of MAC design for sensor networks is to use TDMA based protocol that conserves more energy compared to contention based on the protocols like CSMA.

4.8. *Connectivity*

High node density in sensor networks precludes them from being completely isolated from each other. Therefore, sensor nodes are expected to be highly connected. This, however, may not prevent the network topology from being variable and the network size from being shrunk due to sensor node failures. In addition, connectivity depends on the, possibly random, distribution of nodes.

4.9. *Coverage*

In WSNs, each sensor node obtains a certain *view* of the environment. A given sensor's view of the environment is limited both in range and in accuracy; it can only cover a limited physical area of the environment. Hence, area coverage is also an important design parameter in WSNs.

4.10. *Data Aggregation*

Since sensor nodes may generate significant redundant data, similar packets from multiple nodes can be aggregated so that the number of transmissions is reduced. Data aggregation is the combination of data from different sources, according to a certain aggregation function, e.g., duplicate suppression, minima, maxima and average. This technique has been used to achieve energy efficiency and data transfer optimization in a number of routing protocols. Signal processing methods can also be used for data aggregation. In this case, it is referred to as data fusion where a node is capable of producing a more accurate output signal by using some techniques such as beamforming to combine the incoming signals and reducing the noise in these signals.

4.11. *Quality of service*

In some applications, data should be delivered within a certain period of time from the moment it is sensed, otherwise the data will be useless. Therefore bounded latency for data delivery is another condition for time-constrained applications. However, in many applications, conservation of energy, which is directly related to network lifetime, is considered relatively more important than the quality of data sent. As the energy gets depleted, the network may be required to reduce the quality of the results in order to reduce the energy dissipation in the nodes and hence lengthen the total network lifetime. Hence, energy-aware routing protocols are required to capture this requirement.

5. SYSTEM MODEL

Consider a data flow with a source node, ***N*** relay nodes, and a sink node in an event-driven WSN. The source node generates data packets by sensing events and transmits the packets to the sink node through the ***N*** relay nodes. To simplify the control mechanism and reduce buffer size at nodes, a multiple sending approach without acknowledgments is adopted as the transmission scheme. Such transmit approach has been proved to be similar to the acknowledgment-based scheme, especially under high channel error rate. Except for the sink nodes, all other nodes do not guarantee their functioning over the time and they are normally equipped with low voltage batteries that limit their lifetimes. Without loss of generality, the initial energy available for the source and relay nodes are denoted as E_0^{init} and $\boldsymbol{E_n^{init}}$ $\boldsymbol{(n = 1,2,\ldots, \mathrm{N})}$, respectively. When the available energy of a node is less than a

Threshold level ***it***, the node will lose its functioning. To prolong the lifetime, the source node is usually operated in power-saving strategy to save energy. At this strategy, the source node operates either in active mode (i.e., sending or transmitting) or sleep mode. Since sensing is an energy-consuming operation, the source node generally has its own duty cycle, for instance, 1%, which corresponds to 10 ms sensing event per second. Thus, the energy consumed by the source node to the sensing event from time 0 to time ***t*** can be given by

$$E_0 (t) = a P_0 t, \qquad (1)$$

Where α is the duty cycle, P_0 is the power required by sensing event per second. If some event is detected, the radio module of the source node is turned on and a packet is transmitted to the nearest relay node. Let ***K*** denote the number of packet copies sent out by each node in the WSN and assume that totally *M (t)* events are detected during [0, t], then the energy spent in transmitting packets at the source node can be expressed as

$$E_0 (t) = \frac{-P_0^e + P_0^t KLM(t)}{r} \qquad (2)$$

Where $\boldsymbol{P}_0^e$ is the power dissipation of the source node to run the transmitter circuitry, $\boldsymbol{P}_0^t$ is the power used by the transmit amplifier (i.e., the transmit power), ***L*** is the packet length in bit and ***r*** is the transmission rate in bit per second. If no event is detected, the radio module of the source node is kept unavailable. Note that the counting process $\boldsymbol{M\ (t)}$, $\boldsymbol{t} > 0$ which denotes the number of events that are detected by the time ***it*** is assumed to be a non-homogeneous Poisson process (NHPP) with intensity function $\boldsymbol{X\ (t)}$**.**

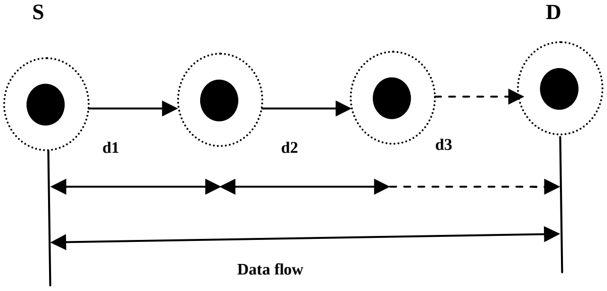

Fig. 1. The Data flow system in WSN

Here, an event-driven WSN consisting of *N* uniformly placed relay nodes in a *D*-meter-long linear region is used as a test system. To simplify the simulation, assume that the source node and all relay nodes have the same initial energy (i.e., $E0^{nit} = E\wedge^{nit} = \bullet\bullet\bullet = E^{1}\wedge = E^{lnit}$) and run the transmitter circuitry with the same power (i.e., $P_0^e = Pe = \bullet\bullet\bullet = PN = P^e$). Moreover, the transmit power of the source node and all relay nodes are also supposed to be the same (i.e., $P0 = Pj = \bullet\bullet\bullet = PN = P^t$).

Figure 2 illustrates the wireless link reliability versus transmit power with different numbers of the relay nodes. As the figure clearly illustrates, with the increase of the transmit power, the larger received SNR at each receiver occurs, which results in the increase of wireless link reliability. Simultaneously, the results in Figure 2 indicate that the relay node number affects the wireless link reliability significantly. Specifically, the wireless link reliability with *N* = 5 is much higher than that with *N* = 3. The reason is that a larger relay node number will result in smaller distance between two adjacent nodes, which will further result in higher link reliability. In addition, it can be observed from Figure 2 that the simulation results of wireless link reliability match with the theoretical results very well.

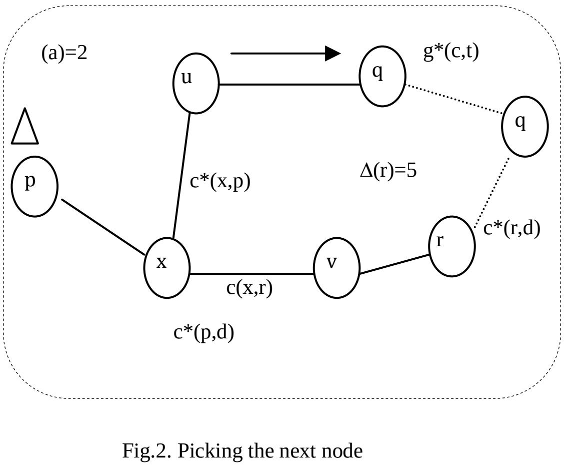

Fig.2. Picking the next node

We now present the details of the method. Let $G = (C, A)$ be an undirected connected graph with node set C and arc set A. For x *e* C, let $C(x)$ be the set of neighbors of x, where a neighbor of x is a node one arc away from x. We associate with each undirected arc (i,j) *e* A a cost $c(i,j)$, and require each $c(i,j)$ to be a positive integer. (The integer valued restriction can always be met by approximating, to the desired accuracy, each arc cost by an improper fraction, and then multiplying all the fractions by the least common multiple of the fraction denominators.) For i,j *e* C, let $c^*(i,j)$ be the cost of the shortest path in G between i and j. When using *Route (s, d)* for fast re-route in the event of an arc failure, which is the target application, $c^*(i,j)$ represents the shortest path cost *before* the IGP has reconverged in response to the link failure. Let s be a given source node, and d be a given destination node. In procedure *Route(s, d)* below, P is an ordered list of nodes that have been visited, and $P \wedge \{P, x\}$ means that x is inserted after the rightmost element in P. Also, $A(n)$ is the *multiplicity* of node n, indicating how many times n has been visited by the current packet.

```
procedure Route(s, d)
1 initialize: P = 0, A(n) = 0 for n e C, and x = s;
2 while (x = d) {
3     Let Y = {y e C(x) | A(y) = min_{n€M}{x) A(n)};
4     Pick any y eY for which the sum
          c(x, y) + c*(y, d) is smallest;
5     Set A(x) ^ A(x) + 1, P ^ {P,x},
          and send the packet and P from x to y;
6     Set x ^ y;7}
```

In words, if x *is the latest node to receive the packet, we find the set of neighbors of* x *with lowest multiplicity. From this set, we pick the neighbor* y *for which* c(x, y) + c*(y, d) *is smallest. We append* x *to* P, *augment the multiplicity of* x *by 1, and send the packet and* P *to y. Note that* P *can be used to compute the multiplicities; e.g., if* P = {s,f,g,f,s,d,c, a, c, f, g, s, d, c, a} *then* A(a) = 2, A(c) = *3,* A(d) = 2, A(f) = *3,* A(g) = 2, *and* A(s) = *3. This example also shows that instead of sending* P *to the next node, we could instead send only the nodes visited and their multiplicities, e.g., we could send* {A(a) = 2, A(c) = *3,* A(d) = 2, A(f) = *3,* A(g) = 2, A(s) = *3}.*

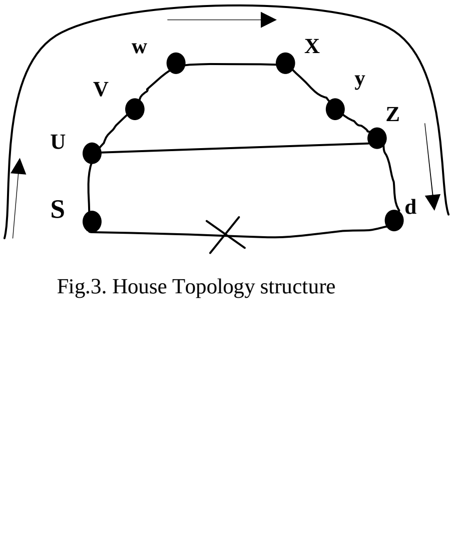

Fig.3. House Topology structure

Note that we optionally could add a step, immediately following Step 2, which says that if d *e* $C(x)$ then forward the packet to d.

Steps 3 and 4 are illustrated in Fig. 3. The neighbors of x are p, q, and r; of these, p and q have the lowest multiplicity. Since $c(x,$ q) + $c^k(q, d) < c(x,p) + c^k(p,$ d), the packet is next forwarded to q.

If we apply the method to the square of Fig. 1, with sources, destination d, and link (s, d) failed, s will forward the packet to u. Since now A(v) = 0 and A(s) = 1, then u forwards the packet to v. Since now A(d) =0 and A(u) = 1, then v forwards the packet to the destination d. Thus the method easily computes an alternate route for the square, which is a case where LFA fails.

A more interesting example is provided by Fig. 4, where all arcs have cost 1, except for (z,d) with cost 10. Suppose (s,d) fails and the IGP has not yet re-converged. If in Step 4 of *Route(s,t)* we break ties by picking the lexicographically smallest node (e.g., closer to “a” in the alphabet), then the path taken is $s \wedge u \wedge v \wedge w \wedge x \wedge y \wedge z \wedge d$. If in Step 4 of *Route(s, t)* we break ties by picking the lexicographically largest node (e.g., closer to “z” in the alphabet) then u forwards the packet to z, and z forwards the packet to y, since A(y) = A(d) = 0 but $c(z,y) + c^k(y,d)$ = 1+4 < $c(z,d)$ = 10. The packet will eventually reach d, but by a longer path than with the “lexicographically smallest” rule.

This jumping between loops can occur at most H times, where H is the number of arcs in path $P_{s,d}$. Thus $P_{s,d}$ never reaches d, which contradicts the definition of $P_{s,d}$. Hence this second sub-case z *e Np* yields a contradiction, and hence the second case *x e Np* cannot hold.

Having shown that both *x e Np* and *x e Np* cannot hold, we conclude that there is no path $P_{s,d}$ from s to d.

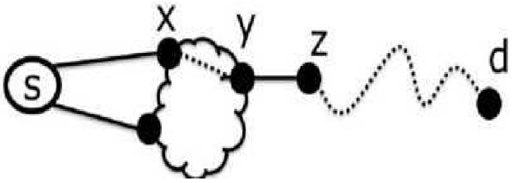

Fig.4. Numerical analysis of fast rerouting techniques

We consider two sub-cases. Suppose first that z *e Np* Consider the iteration where the path P generated by *Route(s, d)* has traversed loop i once, and then later returns to y. Then each node on this loop has multiplicity at least 1, but z has multiplicity 0, since z *e Np*. By Step 3 of *Route(s,d)*, z will be picked before again selecting a node on loop i. But *Route(s, d)* did not pick z, and instead traversed this loop a second time. Hence it must be that z *e Np*.

Finally, consider the second sub-case, where we assume z $e\ Np$. Since by definition z is not on loop i, then z must lie on some other loop, say loop j, where $j = i$. By the same arguments as above, the path $P_{s,d}$ must leave loop j, and when it does so it must immediately visit another loop.

A number of projects have tackled the problem of providing flood support using WSN technology. The Floodnet project uses a platform similar to GridStix v1 (an XScale CPU with 802.11b networking) to implement flood monitoring on a tidal river in South East England, though this system supports only simple data flows, providing no support for in-network computation. The Hydrowatch project uses low power Telos motes to implement river monitoring in the Sierra Mountains in northern California. This project is currently focused on supporting the planning of micro-solar installations to support environmental monitoring WSNs. The mote platform used in Hydrowatch does not have sufficient resources to support in-network computation, though the project does offer support for more complex data flows through the use of 6LowPAN on-site networking.

The approach of separating the concerns of networking and sensing from application processing is also used in Dust Networks ‘Smart Mesh’ products which provide reliable mesh networking and basic sensing functionality with the expectation that developers will add their own application processor; while the GainSpan GS1010 [7] provides separate application and network processors. Such a separation allows power-hungry application processors to be activated only when needed. We are currently evaluating the Dust Networks SmartMesh-XT 2135 alongside the GridStix 1.5 low-power personality for providing low power networking support.

6. CONCLUSION & FUTURE WORK

We have described a WSN node architecture that employs two personalities: a low power one and high performance one. We have also discussed in outline how the new capabilities enabled by this platform are controlled and managed by our Open Overlays middleware. Based on this combination of hardware and software, we expect that our flood system deployments can survive for significantly longer durations while offering support that is specifically tailored for the diverse data flows of the flood warning application.Several research in WSN focus upon deploying the GridStix 1.5 flood monitoring platform at the new site on the River Dee. The GridStix 1.5 platform will then be evaluated more thoroughly in this deployed environment. As well as evaluating low-level system functionality, we are particularly interested in evaluating the role of adaptation in improving system performance. This includes adaptation between personalities as discussed in this paper, as well as more fine grained adaptation, such as the adaptation of networking behavior. The wireless link consistency, node energy availability, instantaneous network, and MTTF are investigated in this paper. However, the node energy availability expression and the system, thereby making calculations cumbersome. To bypass this problem, two propositions are developed which make it possible to calculate the node energy availability and the system instantaneous reliability easier. The simulation results show that the analytical expressions are accurate enough. Furthermore, the results are useful in designing a WSN to obtain good network performance. For future work, the analysis of a data flow in WSN with acknowledgment-based transmission scheme and the reliability evaluation of the WSNs with a random node distribution will be investigated.

REFERENCES

[1] IF Akyildiz, W Su, Y Sankarasubramaniam, E Cayirci, A suivey on sensor networks. IEEE Commun. Mag. 40(8), 102-114(2002)

[2] MN Nguyen, C Bao, KL Tew, S Teddy, XL Li, Ensemble based real-time adaptive classification system for intelligent sensing machine diagnostics. IEEETrans. Reliability 61(2), 303-313 (2012)

[3] J Li, H Kao, J Ke, Voronoi-based relay placement scheme for wireless sensor networks. IET Commun. 3(4), 530-538 (2009)

[4] J Li, G AlRegib, Network lifetime maximization for estimation in multihop wireless sensor networks. IEEE Trans. Signal Process. 57(7), 2456-2466
(2009)

[5] N Wang, XL Shen, Research on WSN nodes location technology in coal mine, in *International Forum on Computer Science-Technology and Applications*, vol. 3, (IEEE, Chongqing, China, 2009), pp. 232-234

[6] J Bredin, E Demaine, M Hajiaghayi, D Rus, Deploying sensor networks with guaranteed fault tolerance. IEEE/ACM Trans. Netw. 18(1), 216-228
(2010)

[7] K Sun, P Ning, C Wang, Fault-tolerant cluster-wise clock synchronization for wireless sensor networks. IEEE Trans. Dependable and Sec. Comput. 2(3), 177-189 (2005)

[8] D Fontanelli, D Petri, An algorithm for WSN clock synchronization: uncertainty and convergence rate trade off, in *IEEE International Workshop on Advanced Methods for Uncertainty Estimation in Measurement* (IEEE, Bucharest, 2009), pp. 74-79

[9] D Ho, S Shimamoto, Highly reliable communication protocol for WSN-UAV system employing TDMA and PFS scheme, in *IEEE GLOBECOM Workshops* (IEEE, Houston,

2011), pp. 1320-1324

[10] X Chen, M Lyu, Reliability analysis for various communication schemes in wireless CORBA. IEEE Trans. Reliability 54(2), 232-242 (2005)

[11] JL Cook, JE Ramirez-Marquez, Two-terminal reliability analyses for a mobile *ad hoc* wireless network. Reliability Eng. Syst. Safety 92(6), 821-829 (2007)

[12] JL Cook, JE Ramirez-Marquez, Mobility and reliability modeling for a mobile *ad hoc* network. IIE Trans. 41(1), 23-31 (2008)

[13] JL Cook, JE Ramirez-Marquez, Reliability analysis of cluster-based *ad-hoc* networks. Reliability Eng. Syst. Safety 93(10), 1512-1522 (2008)

[14] S Dominiak, N Bayer, J Habermann, V Rakocevic, B Xu, Reliability analysis of IEEE 802.16 mesh networks, in *2nd IEEE/IFIP International Workshop on Broadband Convergence Networks* (IEEE, Munich, 2007), pp. 1-12 G Egeland, P Engelstad,The availability and reliability ofwireless multi-hop networkswith stochastic linkfailures. IEEEJ. Select. Areas Commun. 27(7), 1132-1146 (2009)

[15] T Kurp, RGao, S Sah, An adaptive sampling scheme for improved energy utilization in wireless sensor networks, in *IEEE Instrumentation and Measurement Technology Conference* (IEEE, Austin, 2010), pp. 93-98

[16] H AboElFotoh, E ElMallah, H Hassanein, On the reliability ofwireless sensor networks, in *IEEEInternational Conference on Communications*, vol. 8, (IEEE, Istanbul, 2006), pp. 3455-3460

[17] M Shazly, E Elmallah, H AboElFotoh, A three-state node reliability model for sensor networks, in *IEEE Global Telecommunications Conference* (IEEE, Miami, December 2010)

[18] BC Cheng, HH Yeh, PH Hsu, Schedulability analysisfor hard network lifetime wireless sensor networks with high energy first clustering. IEEE Trans. Reliability 60(3), 675-688 (2011)

[19] HCWong,JMSNogueira,AAFLoureiro,Fault managementin event-driven wireless sensor networks, in *the 7th ACM International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems* (ACM, Venice, 2004), pp. 149-156

[20] RK Shakya, YN Singh, NK Verma, Optimizing channel access for event-driven wireless sensor networks: analysis and enhancements. Arxiv preprint arXiv:1203.5874 (2012)

[21] H Luo, H Tao, H Ma, S Das, Data fusion with desired reliability in wireless sensor networks. IEEE Trans. Paral. Distributed Syst. 22(3), 501-513 (2011)

[22] H Pham, *System SoftwareReliability* (Springer, New York, 2006)

[23] TSRappaport, *Wireless Communications: Principles and Practice* (Prentice Hall, NewJersey, 1996)

[24] F Haight, *Handbook of the Poisson Distribution* (Wiley, New York, 1967)

[25] ABenjamin,A Benjamin,J Quinn, *Proofs That Really Count: The Art of Combinatorial Proof* (The Mathematical Association ofAmerica, Washington, 2003)