

“Second Activity Report” *

Faisal Karim Shaikh
Dept. of Computer Science
Technische Universität Darmstadt, Germany
fkarim@deeds.informatik.tu-darmstadt.de
<http://www.deeds.informatik.tu-darmstadt.de/faisal>

Abstract

There exists several applications of sensor networks where reliability and ordering of messages can be critical. Keeping this in view I have started to look around how messages are passed and what are the critical issues involved in it. This report focus on my research activities during last month.

1. Introduction

This report describes about the different papers which I have gone through. The papers discussed in this report are mainly from the proceedings of International Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc).

The rest of the report is organized as follows: Section 2 describes general papers from MobiHoc on addressing and security issues in ad hoc mobile Networks. Section 3 focusses on reliable message delivery issues. Section 4 covers other conferences. Finally, Section 5 concludes the report.

2. MobiHoc

Nitin [4], in this paper describes about the technique to overcome the deficiencies of *duplicate address detection* (DAD) schemes which are working on timeout mechanisms. He argued that DAD procedures do not provide reliability, when the message delay between atleast one pair of nodes in a network are unbounded and when the network is partitioned for unbound time period. So he proposes a scheme called as Weak DAD, which also suffer shortcoming, and overcome with Extended Weak DAD.

Weak DAD does not require the duplicate address detection, but it focuses on routing of data to the desired node even if duplicate addresses are available in the network, for

this he suggest changes in the routing control packets, without changing the IP headers. He used link state and dynamic source routing (DSR) protocols to demonstrate Weak DAD as an example.

For implementing weak DAD in link state, he propose to update the routing table by including the unique key¹ assigned to a node, along with the address of node. The same update is required in link state packet transmitted by a node. So if duplicate addresses exists in the network they can be detected by looking at routing table, and this information can be propagated by using routing control packets.

The weak DAD shows unexpected behavior for upper layer protocols, to cope with this situation Extended Weak DAD suggest that if a service at node X want to send data to a service at node Y than the routing table of both nodes must be consistent.

For DSR the same procedure is adopted, i.e to append the unique keys in routing table and routing control packets.

Seapahn *et al.*,[5] have developed a localized algorithm for solving optimization problems in wireless ad-hoc networks. The theme is to locally process the data, and request to those nodes who are potential candidates to contribute in final decision. They have applied this optimization technique on *location discovery* and *exposure*-based coverage. The approach consists of five components:

data acquisition facilitates which data to collect from which node.

optimization provides partial or complete solution for a task.

search expansion searches best node to contact.

bounding specify which nodes are not considered next.

termination halt the mechanism.

*Research supported in part by “MUET & DEEDS, TU Darmstadt ”

¹Unique key can be public key of node, MAC address or any other unique combination

For location discovery, authors have used the multilateration mechanism, in which a node requires only the location information from neighbors to estimate its location. [5] have introduced some changes in the standard mechanism of multilateration, firstly, the algorithm specifies in which order the nodes in network estimate their locations, secondly instead after first trilateration the node will not accept the final location for itself, rather it will continue to accept the locations from other nodes and adjust its position estimate. The algorithm has four parts; during initialization nodes exchange the messages to estimate the distances. They can use RSSI or GPS measurements as well. In the second phase nodes exchange information about their states. In third stage nodes perform trilateration depending on the number of neighbors. After that each node calculates the object function to determine the order by which nodes estimate the location. At fourth stage objective functions are compared and only nodes whose objective function value is lower than all nodes will accept the estimates from previous state.

For localized exposure the authors have used voronoi diagram to partition the sensor field. As the space is continuous and exposure integral does not have simple analytical solutions, therefore authors used generalized grid. The algorithm constructs graph corresponding to the grid covering voronoi polygons (VP). The minimal exposure path can be calculated from one point to other point on the boundary of VP using generalized Dijkstra's algorithm. Algorithm tasks can be viewed as four cases; in first case, node receives request to find minimum exposure, let's say from point A to B as *Path request*. In the second case node receives *Edge update* to continue search minimum exposure path. Aborting conditions are notified using *Abort update* as third case. As a fourth case destination reached notification is broadcast as *Dest update* message.

The authors have also showed some experimental results that are comparable to centralized algorithms.

3. Data Delivery

Seung-Jong Park *et al.*, [1] has considered the problem of reliable data transmission from sink to sensor nodes. It's a point to multi point data delivery model. They have presented a GARUDA² approach for reliable data delivery. They have also described four reliability semantics as shown in figure 1 that is required in Wireless Sensor Networks (WSNs).

1. Delivery of data to the entire region,³
2. Delivery of data to a subregion,

²A mythological bird that reliably transported gods

³region covered by a sink node

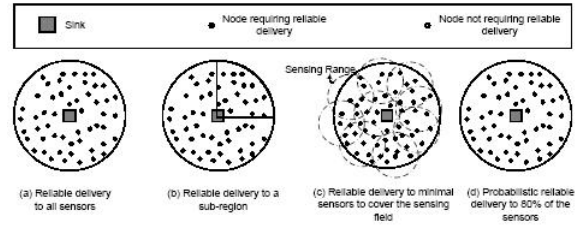


Figure 1. Types of reliability Semantics [1]

3. Delivery of data to some nodes such that the entire sensing network is covered, and
4. Delivery to a probabilistic subset of nodes.

GARUDA's design is composed of following things (i) for short message delivery they used pulsing based solution; (ii) a virtual infrastructure called the core; (iii) a two-stage Negative Acknowledgments (NACK) based recovery process that effectively minimizes the overheads of the retransmission process; and (iv) a simple candidacy based solution to effectively support the different notions of reliability that might be required in a WSN. The important element of GARUDA's design is its core construction which is basically the development of minimum dominating set (MDS). MDS is developed during single packet flooding using pulsing based approach. For loss recovery process the core forms set of local designated servers dynamically for each message and approximate MDS each time. The *hop-count* of nodes are determined by reliable delivery of first packet, which is the distance of a node from the sink.

A node elects itself as a core if its *hop-count* is multiple of *three* and if it has not heard from any other core node. In this scheme out-of-order forwarding is used for message forwarding. To avoid NACK behavior for retransmission of out-of-order forwarding GARUDA uses Availability map (A-map) exchanged between core nodes. A-map contains information regarding the availability of packets at upstream core node. This definitely increases the overhead but authors claim that it is less compared with NACK retransmission overheads. The loss recovery of packets is two stage. In first stage, loss of data at core nodes is recovered by making a request to upstream core node and by checking in A-map. In second stage non core nodes are recovered only when these nodes have heard an A-map from core node, that it has all packets available.

For reliable first packet delivery GARUDA uses Acknowledgment (ACK) based scheme using Wait-for-First-Pulse (WFP), consisting of small finite series of short pulses and repeated periodically. When sink wants to send data it first sends WFP for finite time. The nodes in its range upon receiving the WFP start sending WFP as well until the complete network comes to know that first packet is arriving.

After finite time, sink sends first packet in regular manner and stops sending WFP.

To achieve other reliability semantics as shown in figure 1 the authors introduce the candidacy problem and during the core construction only those nodes can participate who choose themselves as candidate. All other features of GARUDA remain the same. To maintain the connectivity of candidate nodes to sink, forced candidacy approach is used in which if downstream candidate core node does not hear from upstream core node, it will request upstream node to make itself as a candidate node.

Basile C. *et al.*,[3] in this paper presented the notion of inner-circle consistency, where local interaction of nodes⁴ is used to tackle the errors/attacks and their propagation in network, and this is achieved by combining a secure topology service, a deterministic voting technique (embeds application-aware checks for validating information), static voting technique (improves accuracy by using proposed *fault-tolerant(FT) cluster* algorithm) and threshold cryptography. They have evaluated the *inner-circle* framework on ns2. The architecture of a node implementing this framework consist of i) *inner-circle Interceptor*, which intercept messages and redirect them to inner-circle services, also it is used to block the data from suspected nodes. ii) *Suspicions Manager*, maintains list of suspected nodes. iii) *Secure Topology Service*, maintains topology of neighbors. iv) *Inner-circle Voting Service*, for performing statical or deterministic voting. v) *Inner-circle Callbacks*, used to customize inner-circle voting depending upon application needs. The architecture of node also consists of Crypto-Processor and Fault-Tolerant Cluster Processor.

The authors demonstrate the idea of inner-circle consistency in two significant wireless scenarios: (1) the neutralization of black hole attacks in AODV networks and (2) the neutralization of sensor errors in a target detection/localization application executed over a wireless sensor network.

Comments: The notion of inner-circle is good but based on assumption of high density of powerful middle layer nodes which seems to be unrealistic. With the fact that a node also requires two extra processors making it infeasible in terms of cost.

Estrin D. *et al.*,[7] emphasized on localized algorithms for sensor network coordination. In this paper they have described the localized algorithms and discussed *directed diffusion* as an example. They have argued that, as sensing is inherently distributed so sensor applications will be distributed as well and believed that localized algorithms will produce scalable and robust applications. To achieve global tasks, sensors efficiently coordinate their local interactions by using clusters. One of the coordination tasks for sensor networks can be, to elect extremal sensors to form

⁴in a one hop neighborhood

widest baseline to locate external object. It will be energy efficient that cluster heads only participate in the election of extremal nodes instead of all nodes. Other example is data aggregation in clusters. They have also presented a localized clustering algorithm, which elects cluster-head sensors in such a way that all sensors in network are associated with cluster-head sensor as parent.

WSN using directed diffusion have following properties. Each node *names* data with attributes. Nodes who require information expresses *interests*. Interests establishes *gradient* for diffusion of data. A sink may query for some information by sending an interest. Nodes in network propagating the interest, alongside associating gradient to path and also maintain the reverse path so that data can be diffused back when the desired interest is matched.

4. Other Conferences

Stankovic J. A. *et al.*,[2] in this paper describe the general research challenges in WSN. They have also identified some basic solutions as well. Authors structured the general research challenges in WSN as follows:

Paradigm Shift; messages should be sent to group of nodes instead of individual nodes as WSN's are inherently data centric. For example, if we want to know about the temperature of room A, as there can be many sensors in that room so we will not ask any particular sensor to send data but we will be interested in aggregated answer from those sensors. So some paradigm shift is required for addressing WSN.

Resource Constraint; resources such as power, CPU execution speed, memory and communication bandwidth are major constraints in WSN.

Unpredictability; Also WSN are deployed in very unpredictable environments, i.e. in forest to sense fire, individual nodes are also unpredictable, network topology and routing patterns are changing frequently, power resource are varying on different nodes, new nodes can be added and old will be removed, sensors can be faulty and so on.

High Density; the WSN consists of large number of nodes, which result in a large scale system. Research is required for self stabilizing protocols and algorithms to sustain in such vast networks.

Real Time; timing requirement is inherent in WSN, for example if presence of something is sensed than it must be propagated as early as possible to the station. These challenges are due to large scale and unreliable nature of WSN.

Security; WSN have very limited resources as described earlier and security algorithms are resource greedy, requiring research in this domain.

Authors further classify more specific research challenges in Networking, OS and middlewares. In networking of WSN they have elaborated different protocols and algorithms at MAC, Network and Transport layer. For MAC layer they have talked on Scheduling-Based, Collision-Free Real-Time, Contention-Based, Hybrid MAC protocols and suggested that existing wireless MAC protocols does not consider the requirements of WSN and more focuses on throughput of the system. For the network layer they have discussed the different issues of Ad-Hoc routing, Multicast and Anycast protocols and urged that the existing algorithms can not be used directly for WSN, and they need to be modified. Very recently the research community start talking about the reliable end-to-end communication in wireless ad-hoc networks. It has been observed that TCP is not reliable for ad-hoc networks due to many reasons, so especial transport protocols for WSN are needed which provide reliability, good congestion control and fairness.

There are additional challenges for WSN, existed at OS and middleware layers. These layers are responsible for additional functionality such as distributed resource management, aggregate control and team formation of nodes for tracking an object. These challenges starts from the level of a single node. As the node is having severe resource limitations, realtime constraints, bandwidth limitations so it requires creative kernel implementations and to support the kernel some high level of abstraction is needed which can be handled by virtual machines. Context Awareness is also a major challenge for WSN. Till now partial context awareness is achieved and much more work is done in the location aware protocols. There is a need for full vision of context awareness. On the other hand group formation is also one of the challenges. Most of the prior work on group communication is with respect to static systems. As described earlier due to dynamic nature of WSN where one node become part of group and one is leaving the group very frequently, so real time properties of group communication is needed.

Desnoyers P. *et al.*, [6] have described a proxy based storage architecture for Sensor Networks in which they use predictive techniques on cached current and past data, to answer the queries. They called this architecture as PRESTO which attempts to provide the interactivity of data streaming approach. PRESTO suggested the archival of important data at remote nodes and caching at proxies and predicted that in future the remote node will be having sufficient flash memory⁵ for archiving. They have divided sensor network in three tiers, the lowest tier consist of high number of low power nodes, the middle tier consist of much powerful prox-

⁵1GB and more

ies, which can use resources continually and the top tier consists of user terminals.

In response to a query, proxy first examine the cache for possible response. If cache hit encountered the query is processed locally, in the event of cache miss proxy try for extrapolation, if succeeded send the result back otherwise proxy fetch the data from archived data at remote sensors.

PRESTO proxy consists of two components; cache of summary information and prediction engine. Prediction engine is used for three purposes:

model-driven push; PRESTO uses predictive modeling to enable model-driven push from the remote nodes. For this proxy sends parameters of model; which capture expected results; to all remote nodes. The sensor nodes compare the sensed data against that model and send the data to proxy when the model fails.

extrapolation; the prediction engine can extrapolate missing data as needed by query as long as query precision is met.

Query-Sensor matching; the prediction engine is responsible to match the needs of queries to the operations of remote sensors.

The PRESTO sensor node has a energy efficient archival file-system and time-based index structures for efficient service read requests, alongwith low power sensors, micro-controller and a radio. The aim of PRESTO is to provide a single logical view of data available at distributed sensor nodes.

5. Conclusions and Future work

To provide end to end delivery of messages with reliability, dependability and security as key attributes the tiered approach to Wireless Ad hoc Sensor Networks (WASN) seems to be feasible. WASN is classified as three tiered architecture, in which upper tier consists of users, having much more powerful nodes which can transmit messages to middle tier via wired or wireless media having continues availability of resources. Middle layer is relatively more powerful than lower tier and used to organize different tasks at lower tier. Third tier consists of low power nodes.

In future I'll be focusing on these tiers and try to formalize the problems at each stage and probable solutions, like the need of clusters at lower tier, the need of voting at middle layer, security issues to be dealt at lower layer or at middle layer etc.

I'm also looking for ns2 or Opnet for modeling the behavior of messages at different tiers.

References

- [1] Seung-Jong Park, Ramanuja Vedantham, Raghupathy Sivakumar, Ian F. Akyildiz, "A scalable approach for reliable downstream data delivery in wireless sensor networks," *Proceedings of the 5th ACM international symposium on Mobile ad hoc networking and computing*, pp. 78–89, 2004.
- [2] Stankovic, J.A.; Abdelzaher, T.E.; Chenyang Lu; Lui Sha; Hou, J.C., "Real-time communication and coordination in embedded sensor networks," *Proceedings of the IEEE*, pp. 1002- 1022, 2003.
- [3] Claudio Basile, Zbigniew Kalbarczyk, Ravi K. Iyer, "Neutralization of Errors and Attacks in Wireless Ad Hoc Networks," *Proc. of the Intl Conf. on Dependable Systems and Networks*, 2005.
- [4] Nitin H. Vaidya, "Weak Duplicate Address Detection in Mobile Ad Hoc Networks," *Proceedings of ACM, MobiHoc*, 2002.
- [5] Seapahn Meguerdichian, Sasa Slijepcevic, Vahag Karayan, Miodrag Potkonjak, "Localized Algorithms In Wireless Ad-Hoc Networks: Location Discovery And Sensor Exposure," *roceedings of ACM, MobiHoc*, 2001.
- [6] Peter Desnoyers, Deepak Ganesan, Huan Li and Prashant Shenoy, "PRESTO: A Predictive Storage Architecture for Sensor Networks," *Tenth Workshop on Hot Topics in Operating Systems (HotOS X)*, June 2005.
- [7] D Estrin, R Govindan, J Heidemann, S Kumar, "Next century challenges: Scalable coordination in sensor networks," *Proceedings of ACM, MobiCom*, 1999.