ExScal Backbone Network Architecture *

Anish Arora Prasun Sinha Emre Ertin Vinayak Naik Hongwei Zhang
Mukundan Sridharan Sandip Bapat

The Ohio State University, Columbus, OH - 43210
USA

1 Introduction

ExScal stands for Extreme Scaling of *ALineInTheSand* system [1]. The objectives of *ALineInTheSand* and ExScal systems are to provide detection, classification, and tracking of an intruder using a wireless sensor network.

ALineInTheSand used 100 sensor nodes spread over a length of 18m X 5m. ExScal used 1000 sensor nodes spread over a length of 1.26Km X 0.3Km [4]. The objective of ExScal is to scale the low cost, power efficiency , robustness, accuracy, ease of deployment, and self configurability properties of *ALineInTheSand*.

The latency and reliability provided by the sensor network do not satisfy the real time requirements of ExScal application. Hence, a backbone ad hoc network of 802.11 battery powered nodes was laid over the sensor network. We adopted the Stargate platform for the backbone tier to serve as the basis for developing an efficient, robust, and easily deployable backbone service. The challenge was to develop energy efficient and reliable transport services, viz. convergecast and broadcast for an ad hoc 802.11 network.

In this article, we present a network architecture of energy efficient and reliable protocols for structured convergecast, structured and unstructured broadcast for a large scale 802.11 ad hoc network. The structured convergecast protocol is a link estimation based protocol that uses data traffic instead of beacons for its link measurements. The structured broadcast protocol uses TDMA based transmissions for a near-optimal connected dominating set of the nodes. We provide the performance results measured on a network of around 200 802.11 nodes which is likely the largest 802.11b ad hoc network deployed.

2 System Model

XSM Hardware and Network: XSM stands for an eXtreme Scaling Mote. It is designed for detecting rare, random, and ephemeral events [3]. The XSMs were placed at a distance of 9m each. *ALineInTheSand* showed us that to reliably detect a target, it is necessary to limit the maximum number of hops to 5 motes [2]. Therefore, the XSM network was partitioned into sub-networks of 50 XSMs each. Each sub-network had one mote as its *head*.

XSS Hardware and Network: XSS stands for eXtreme Scaling Stargate. A stargate is a linux-based single board computer. It has a 400 MHz processor, 64 MB SDRAM, 32 MB flash memory, and a mote connector serial port. An XSS is equipped with a radio operating at 2.4 GHz, a 9dBi omnidirectional antenna of length 1.82 m, and a GPS unit. The radio uses IEEE 802.11b MAC in an ad hoc mode.

The network topology consisted of 203 XSSs deployed at a distance of 45m each [4]. The head of each XSM sub-network was connected to an XSS through the mote connector port. In total, 45 of 203 XSSs were connected to the heads of XSM sub-network. One XSS was connected through wired ethernet to the *base station* which is a PC running intruder detection application and management console.

Fault Model: The common faults affecting an XSS are failure to acquire a location due to malfunctioning of the GPS units, intermittent connectivity to the neighboring XSS due to loose connection of the antenna cable, partitioning from the network as a result of its toppled antenna, and permanent damage due to adverse outdoor conditions.

3 Backbone Network Architecture

uniComm - A Structured Reliable Convergecast Service: The primary use of the reliable convergecast is to transport event detection messages from the XSS sub-network head to the base station. The traffic is bursty due to the synchronous nature of the event detection phenomenon.

uniComm uses a combination of geographic locations and link estimation as a metric for distance vector routing. For energy efficiency, instead of using beaconing uniComm uses data traffic to detect node failures and to estimate the link quality. Specifically, it uses the latency of MAC layer acknowledgments pertinent to the data traffic. The reliability is pro-

*This work was sponsored by DARPA NEST contract OSU-RF program F33615-01-C-1901.

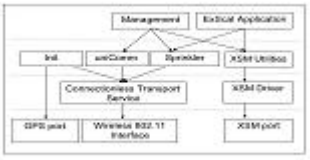

Figure 1: Architecture Diagram

vided on a hop by hop basis.

Sprinkler - A Structured Reliable Broadcast Service: The primary use of the reliable broadcast is reprogramming of the XSMs. The maximum size of an XSM's program for ExScal is 200 KB. Since the payload is a program, the reliability has to be 100%.

Sprinkler exploits the overhearing property of broadcast transmission to reduce the number of transmissions. The base station computes a connected dominating set (CDS) of the XSS topology using the geographic locations of the XSSs. The broadcast transmission is vulnerable to hidden terminal effect. Hence, a TDMA schedule is computed at the base for the XSSs in the CDS to avoid hidden terminal effect. The schedule exploits the spatial multiplexing of transmissions to reduce latency.

Initd - An Unstructured Broadcast Service: In order to compute a CDS and a TDMA schedule, the base station needs a network service that collects the geographic locations of all the XSSs. Each GPS location is 32 bytes.

We designed Initd to contact all the XSSs and collect their IDs and GPS location at the base station. Initd uses controlled flooding to superimpose a tree in distributed manner on all the active XSSs. This tree is used to collect data from all the XSSs at the base station.

Management Service: The management service uses Sprinkler to disseminate the management queries and uniComm to report back the status. It is used to check the status of the CDS and the processes on all the XSSs.

4 Performance Results

The average latency for uniComm was 0.25 seconds. Sprinkler reliably broadcasted 100 KBytes of payload in minimum of 12.08 seconds. The number of transmitted messages were 0.07 times of that required for randomized flooding. Initd was able to achieve an average latency of 6.5 seconds.

5 Conclusion and Future Work

The designed architecture fulfilled the specifications of an intruder detection application for a large scale sensor network.

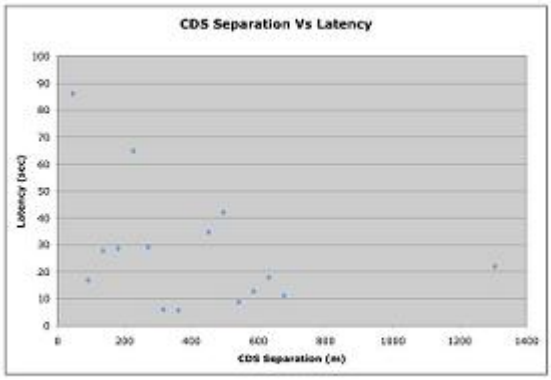

Figure 2: The average latency of Sprinkler for 100 KBytes of payload for different CDS separation

Currently, we are working on extending the computations of CDS and a corresponding TDMA schedule for any planar graph. We are also working to improve the latency of Initd. The next step would be to distribute (a) the CDS and TDMA computations of the Sprinkler, (b) monitoring and recovery of the management service in the network.

References

[1] A. Arora, P. Dutta, S. Bapat, V. Kulathumani, H. Zhang, V. Naik, V. Mittal, H. Cao, M. Demirbas, M. Gouda, Y. Choi, T. Herman, S. Kulkarni, U. Arumugam, M. Nesterenko, A. Vora, and M. Miyashita. A line in the sand: A wireless sensor network for target detection, classification, and tracking. *Computer Networks Journal*, 46(5):605–634, 2004.

[2] S. Bapat, V. Kulathumani, and A. Arora. Reliable estimation of influence fields in unreliable sensor networks. Technical Report OSU-CISRC-8/04-TR49, The Ohio State University, Computer Science and Engineering Department, August 2004.

[3] P. Dutta, M. Grimmer, A. Arora, S. Bibyk, and D. Culler. Design of a wireless sensor network platform for detecting rare, random, and ephemeral events. In *The Fourth International Conference on Information Processing in Sensor Networks*, April 2005.

[4] S. Kumar and A. Arora. Topology and naming for clean point demonstration. Technical Report ExScal-OSU-EN03-2004-12-05, The Ohio State University, Computer Science and Engineering Department, http://www.cast.cse.ohio-state.edu/exscal/content/SubSystem/Topology/-Topology_Extreme_Scaling_Clean_Point_Demo_-Final.pdf, December 2004.