Efficient Routing in Suburban Ad-Hoc Networks (SAHN)

Muhammad Mahmudul Islam
Ronald Pose
Carlo Kopp

Monash University, School of Computer Science & Software Engineering
Clayton, Victoria 3168, Australia
{sislam,rdp,carlo}@csse.monash.edu.au

Abstract

A suburban ad-hoc network (SAHN) is an economical, high-speed alternative for communities of cooperating users. The SAHN aims to provide broadband suburban area connectivity for local area networks with low costs using wireless technology. There exists a plethora of efficient routing solutions for ad-hoc networks. However, less attention has been paid towards optimizing these protocols for ad-hoc networks with a quasi-static topology[1]*. In this paper we outline an efficient routing algorithm, particulary for a suburban ad-hoc network, to make efficient use of network resources. Our primary comparison results are with respect to DSR and AODV.*

Keywords - *Suburban, ad-hoc, SAHN, QoS, on-demand, quasi-static*

1 Introduction

Communication through the Internet is growing rapidly every day. People want to have access to information in various forms such as raw data, audio, video. The ever increasing trend towards transferring huge amounts of data at high speeds has inspired researchers to come up with many new efficient networking technologies. Unfortunately most of the new technologies offering high rates of data transfer require costly infrastructure and high service charges which are only feasible for large educational institutions, governmental organizations, companies and research groups. People in small offices, companies and homes can only enjoy similar performance at great cost. To alleviate these expensive, oversubscribed and area limited solutions, a networking framework has been proposed termed the 'Suburban Ad-Hoc Network' [1] or SAHN. The SAHN is a low-maintenance, decentralized, cooperative wireless networking architecture offering low cost internetworking solutions among its users. The inherent symmetric throughput in both upstream and downstream channels at reasonably high rates allows the facility to provide traditional costly broadband throughput at low cost. The security scheme at the network layer is particularly appealing to security conscious business users. Additionally the wireless interconnecting property makes the SAHN suited to extend the Internet infrastructure to areas of inadequate wired facilities.

Many networking groups[2] have been formed to provide wireless internetworking facilities by connecting households, schools and local businesses together at low initial costs and almost no service charges. But these solutions are threatened by unauthorised intrusions. Moreover participants in a community have to rely on centralised routing nodes for intercommunication. This results in performance bottlenecks as well as inefficient use of aggregate network capacity.

[1] A network with some dynamic attributes

As a consequence these solutions are still less attractive than the traditional and costly solutions provided by various telecommunication service providers. It can even be argued that Nokia's wireless broadband solution (Nokia RoofTop) for residential users, which has an optimized IP protocol stack with custom-built OS for routing, may result in marginal performance in ad-hoc wireless networks. The SAHN goes far beyond these limitations [1]. Each of the SAHN nodes/participants has its own routing module acting as a central gateway. The underlying quality of service (QoS) facility of the routing protocol makes a good use of the aggregate network capacity. Also there is an authentication scheme in the network layer to provide secured data transfer between authorised participants. The SAHN features all the basic facilities provided by traditional community networking solutions.

We have organized our paper as follows. In Section 2, we have made some analyses of available ad-hoc routing protocols to adopt in the SAHN. Then we have outlined the SAHN routing protocol in Section 3. We have presented our simulation results in Section 4, based on our preliminary protocol implementation, to compare our solution with two existing ad-hoc routing protocols.

2 Why a Customized Routing Protocol for the SAHN

The SAHN routing protocol shares the properties of both ad-hoc on-demand and static table driven routing protocols. Notably, the protocol adopts the idea of keeping the neighbor information up-to-date like any of the static table driven routing protocols. On the other hand to find a route to an unknown node, as well as to maintain it, it adopts an on-demand route discovery and maintenance mechanism derived from the Dynamic Source Routing (DSR)[3] protocol [4]. For data transmission over known routes with sufficient QoS attributes, the SAHN routing protocol exploits mixed principles of DSR and the Ad-hoc On Demand Distance Vector Routing (AODV) [5] protocol. As the SAHN does not carry source routes in each data packet, a large network overhead can be eliminated in networks with many nodes[5].

Most of the ad-hoc on-demand routing protocols do not perform a periodic neighbor discovery procedure, since the nodes are considered highly dynamic in terms of mobility[6]. However nodes in SAHN are static (not mobile), though they may occasionally disappear or appear. This quasi-static property of the SAHN makes it possible to maintain up-to-date information about neighboring nodes using table driven routing protocols [7, 8]. Having neighbor information before route discovery starts, can reduce the route discovery latency. Though the SAHN employs the basic idea of DSR during route discovery, various optimization techniques are employed. An example is the introduction of parallel tables to reduce processing time of route request packets at each intermediate node.

Multiple routes to a particular destination can avoid delays associated with route discovery when a working route breaks during data transmission. These redundant routes can also be used to provide a load balancing facility during data transmission which ensures efficient use of aggregate network capacity. In MSR (Adaptive Multipath Source Routing in Wireless Ad Hoc Networks) [9, 10] a special type of packet called the probing packets are periodically transmitted to each of the known paths to get their round-trip times (RTT) for load balancing and also for route maintenance[10]. Network traffic increases for the periodic transmission of these probing packets. Moreover, the RTT alone is not enough to consider as a QoS metric to choose suitable routes in ad-hoc networks. It has been argued in [11, 12, 13, 14] to include other critical factors, such as route reliability (error rate), saturation (available bandwidth) and latency (delay), to measure QoS in an ad-hoc network. These values can be combined with the weighting factors of various resource types (various types of data) to provide the required QoS. In a SAHN, initial

QoS information of new routes can be gathered during the route discovery procedure by adding some extra fields in the route request packets. QoS information can be updated periodically by sending special control packets along associated routes. Data can be transmitted along those routes which conform to the minimum QoS requirements of the corresponding session.

The SAHN routing module is also responsible for network level security. The nodes participating in the SAHN are considered valid or legal. All other nodes are deemed invalid or illegal. Though it is not possible to block requests from invalid nodes, the SAHN can ignore them. In the SAHN, valid requests are transmitted and received by valid nodes in encrypted format. Only a valid node has the ability to decrypt valid requests and hence respond accordingly [4]. Throughout this paper, if not mentioned explicitly, it will be assumed that all packets have been encrypted before their transmission according to the negotiated shared key. The same assumption will be applied to the packets being received.

To provide the desired QoS to multimedia applications, the network should be able to control resources properly. This feature is known as resource access control. Due to different quality of service requirements of various types of resources, initially resources can be divided into following types in the SAHN: (a) authentication of nodes entering the SAHN, (b) specific protocol for efficient transmission of audio/video data, (c) any other types of data, (d) bandwidth allocation for transmission, and (e) encryption at different levels. An efficient and flexible access control model can be developed using the capability model of the Walnut operating system [15], so that access to the SAHN resources can be granted and revoked in real time. However, resource access control models of both Bluetooth and Nokia RoofTop seem to be less fine-grained compared to that of the SAHN. In Bluetooh, there are three types of resources [16]: (a) services that require authentication and encryption, (b) services that only require authentication and (c) open services that do not require authentication or encryption. Nodes in Nokia RoofTop are unaware of different types of resources. A node, once authenticated, can transmit any type of data with restricted upstream and downstream bandwidth. [4]

The motivation to adopt a hybrid routing protocol with certain quality of service metrics and resource access control capabilities, is to eliminate the shortcomings of any individual protocol. The performance analyses of [17] and [6] reveal that both DSR and AODV behave poorly under certain network loads, network sizes and network topologies. This is due to delays in route discovery and data transmission and the inefficient use of network capacity. Though the new improved variants[9, 10, 18] of DSR and AODV are efficient under many conditions, they are not entirely free of shortcomings. [11, 12, 13, 14] have investigated the benefits of considering QoS metrics for route selection over best effort ad-hoc routing protocols. Makalic has done preliminary investigations of SAHN routing [4] to adopt a hybrid approach. We have outlined the SAHN routing scheme in the next section taking into account all considerations discussed above.

3 SAHN Routing Protocol

Generally the SAHN routing protocol has the following major responsibilities:

3.1 Neighbor Discovery

Neighbor discovery is a one-off procedure required when a node wishes to join the SAHN. The authentication procedure and negotiation of the shared key between a neighboring pair are performed in this stage. The SAHN routing protocol implements this neighbor discovery procedure with the help of 'Hello' and 'Hello reply' packets. To minimize the network traffic overhead, these packets are kept as small as possible. QoS values (available bandwidth, error rate and delay) of the neighboring nodes are also exchanged with these 'HELLO' and 'Hello Reply packets'.

3.2 Route Discovery

A node tries to discover routes to a destination if no route is found in its routing table or existing routes are unable to provide the required QoS. The process of on-demand route discovery is accomplished with the help of route request (RREQ) and route reply (RREP) packets. A table called the 'routing table' (RT) is maintained to keep track of all valid paths to different destinations and their associated QoS values.

At each intermediate node, its address and local QoS information (available bandwidth, error rate) are appended in the RIL (Route Information list) of the RREQ packets. Each entry in a RIL can hold a node address, its available bandwidth and error rate. Before forwarding a RREQ packet, each intermediate node retrieves new routes and their QoS values from the RIL.

A RREP packet is generated whenever an intermediate node has one or more routes to the destination, or is the destination node itself. If the node is not the destination node but has a route to the destination, the RREP is constructed by joining RIL of the RREQ with the RIL of the route to the destination.

When an intermediate node receives a RREP, the node updates its routing table with previously unknown routes and QoS values contained in the RIL. If the initiating source of the RREQ receives the RREP, route discovery is deemed successful. The source node then updates its routing table with the unknown routes and corresponding QoS values from the RIL of the RREP.

3.3 Data Transmission

Whenever a source node wishes to send data packets to its destination node, it first checks the cache of the neighboring nodes. If the destination node belongs to one of the neighboring nodes with sufficient QoS value, the data packet is unicast to it.

If the destination is other than any of the neighboring nodes, routes with sufficient QoS are selected to transmit data. It should be noted that, data is transmitted along all feasible routes rather than one feasible route. The first data packet of any session contains complete route address list to the destination. When any intermediate node receives the first data packet of a particular session, it creates a row in its forwarding cache with the destination and next node address. Any subsequent data packet of that session no longer needs to carry the route address list. Fast forwarding is accomplished at each intermediate node by retrieving the next node address from its forwarding cache indexed by the destination address field of any data packet.

3.4 Route Maintenance

A SAHN node may not receive acknowledgement within a certain period of time for the transmitted packet to its neighboring node since neighboring node may have disappeared. Sometimes it may receive a packet intended for a destination and the corresponding row is no longer in the routing table as that row has been deleted for being idle for a long time. In any of these cases a SAHN node generates RERR packets. When an intermediate SAHN node receives a RERR packet, it deletes the entries from the routing table and the cache corresponding to the values of 'Unreachable Node Address' and 'Global Destination Address'. When the RERR packet reaches the global source, it updates its routing table and the cache in the same way as the intermediate node. Then it tries to re-transmit the data using an alternative route contained in the routing table. If such route does not exist, it initiates a new route discovery sequence as described earlier.

Apart from updating the routing table and cache while processing a RERR packet, the route maintenance procedure periodically checks them for stale entries. If any entry is not used for an allowable maximum period of time, it is considered to be invalid and hence is removed from the routing table. The associated fields in the cache are also deleted.

The route maintenance module also keeps its local QoS information database up-to-

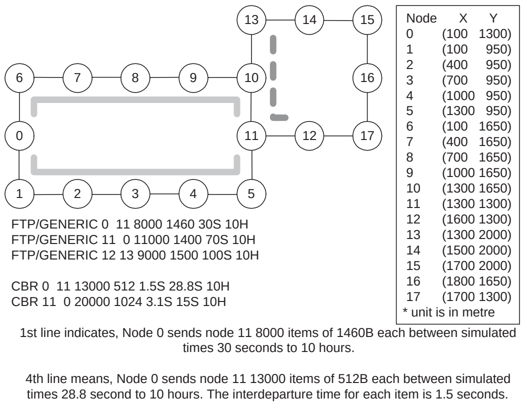


Figure 1: Node placements for simulation

date. Parameters of QoS, such as available bandwidth and error rate along each neighbors, are periodically measured and updated.

Should QoS information of any route become old, RMNT packets are generated and transmitted along corresponding routes to get the up-to-date QoS values. Each RMNT packet contains a RIL similar to the RREQ packet. Initially it contains all node addresses along a known route. QoS information in the RIL is updated by the respective nodes as soon as they receive the RMNT packet.

4 Simulation Results

We have simulated our algorithm with GLOMOSIM (version 2.03). Our aim is to see how well a hybrid routing strategy performs rather than considering any traditional solutions. At this stage, the security scheme and the load balancing using multiple routes at the same time have not been incorporated.

In this simulation, we had a physical terrain of 3 square kilometres. The nodes were placed as shown in Figure 1. There were three FTP clients (node 0, node 11, node 12) for three FTP servers (node 0, node 11, node 13). We had also introduced a pair of CBR or constant bit rate clients (node 0 and node 11) for a pair of CBR servers (node 11 and node 0 respectively). Common routes and sub-routes are indicated with thick lines in Figure 1.

The first set of comparisons (Figures 2(a), 2(c), 3(a)) were conducted in normal condition assuming the nodes were switched on for all times. However, any node was allowed to disappear due to poor signal strength. A second set of comparisons (Figures 2(b), 2(d), 3(b)) were done forcing one node to switch on and off periodically.

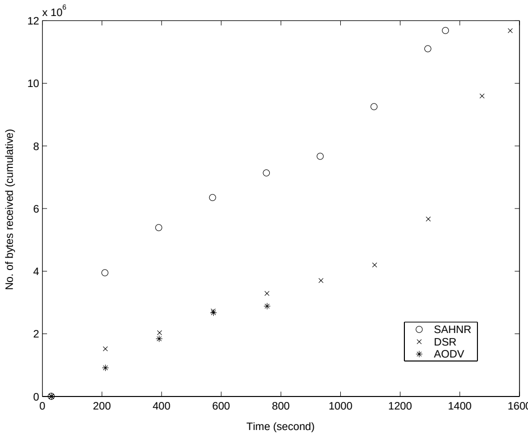
Simulation results showed that the duration of any session was less (Figure 2) while the SAHNR was employed instead of DSR or AODV. The SAHNR had 22% (16% for second set of comparisons) more throughput than DSR on an average. This is because, routes were used concurrently more in DSR than in the SAHNR. In all cases, AODV was unable to complete the FTP sessions created between FTP node 0 and node 11. Moreover, it had a lower rate of data transmission and reception than both the DSR and the SAHNR. In terms of control packet generation and transmission, the SAHNR imposed less stress on the network than DSR and AODV (Figure 3).

5 Conclusion

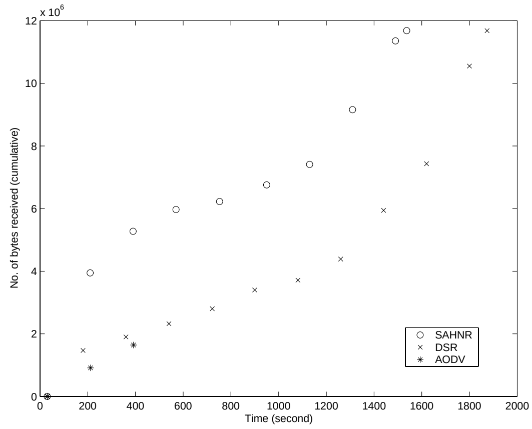
We are developing and testing our routing protocol using GLOMOSIM (version 2.03). There is a testbed with twenty desktop PCs to test our work in a real environment. Each PC acts as a SAHN node with its own routing modules as proposed in Section 3. Though we believe that more changes may be required during prototype implementation and testing, the proposed solution can be adopted to many ad-hoc community networks.

Acknowledgements

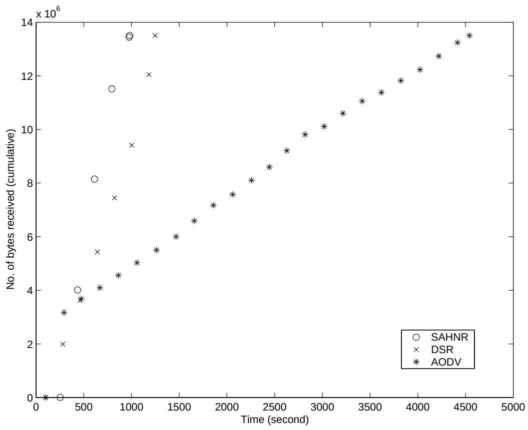
Initial definition of the SAHN architecture was carried out by Adrian Bickerstaffe, Enes Makalic and Slavisa Garic in their computer science honours projects in 2001 at Monash University. They also implemented the testbed. The current project builds on their excellent work.



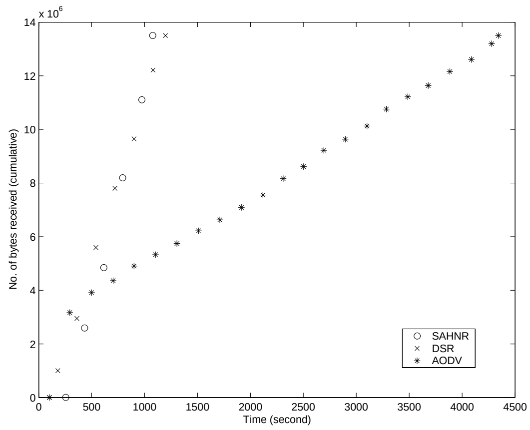
(a) FTP server/node 11 (normal condition)



(b) FTP server/node 11 (a node occasionally switches on and off)

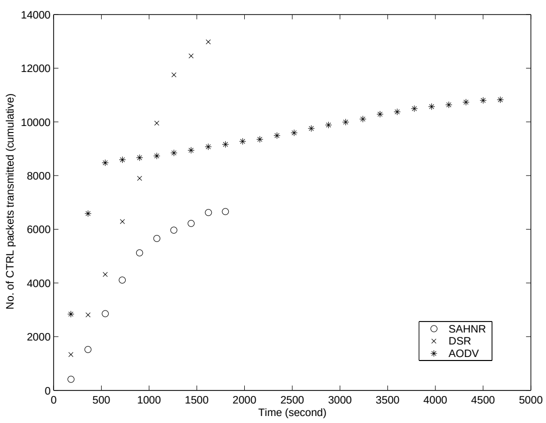


(c) FTP server/node 13 (normal condition)

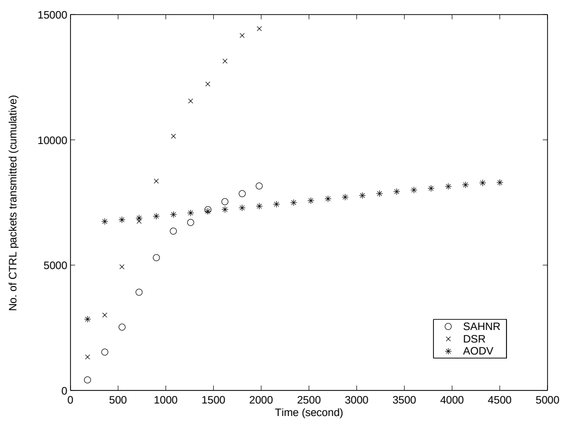


(d) FTP server/node 13 (a node occasionally switches on and off)

Figure 2: Comparing data reception rates



(a) normal condition



(b) a node occasionally switches on and off

Figure 3: Comparing load of CTRL packets in the network

References

[1] R. Pose and C. Kopp. Bypassing the home computing bottleneck: The suburban area network. *3rd Australasian Comp. Architecture Conf. (ACAC)*, pages 87–100, Feb 1998.

[2] 24/01/2003. http://www.wirelessanarchy.com.

[3] D.B. Johnson. Routing in ad-hoc networks of mobile hosts. Technical report, IEEE Workshop on Mobile Computing systems and Applications, Dec. 1994.

[4] E. Makalic A. Bickerstaffe and S. Garic. CS honours theses, Monash Uni, 2001. www.csse.monash.edu.au/~rdp/SAN/.

[5] Royer E.M. Perkins C.E. and Das S.R. Adhoc on demand distance vector (AODV) routing. IETF Internet Draft, Nov. 2000. http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-07.txt.

[6] Hong Jiang and Garcia-Luna-Aceves J.J. Performance comparison of three routing protocols for ad hoc networks. *10th Intl. Conf. on Computer Comms. and Networks*, 2001.

[7] Perkins C. and Bhagwat P. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. *SIGCOMM'94 Conf. on Comms. Architectures Protocols and Applications*, pages 234–244, Aug. 1994.

[8] Garcia-Luna-Aceves J.J. and Spohn M. Source-tree routing in wireless networks. *7th Intl. Conf. on Network Protocols*, 1999.

[9] Shu Y.T. Dong M. Wang L., Zhang L.F. and Yang W.W. Adaptive multipath source routing in wireless ad hoc networks. *IEEE Intl. Conf. on Comms.*, June 2001.

[10] Yantai Shu Lei Wang Lianfang Zhang, Zenghua Zhao and Yang O.W.W. Load balancing of multipath source routing in ad hoc networks. *IEEE Intl. Conf. on Comms.*, 5:3197–3201, 2002.

[11] K. Al Agha A. Munaretto, H. Badis and G. G. Pujolle. A link-state QoS routing protocol for ad hoc networks. *4th Intl. Workshop on Mobile and Wireless Comms. Network*, pages 222–226, 2002.

[12] A. Das H. Kaiyuan L. Gang R. Ravindran, K. Thulasiraman and X. Guoliang. Quality of service routing: heuristics and approximation schemes with a comparative evaluation. *IEEE Intl. Symposium on Circuits and Systems (ISCAS 2002)*, 3:775–778, 2002.

[13] K. Seung-Hoon H. Jong-Joon Hong and L. Kyoon-Ha. QoS routing schemes for supporting load balancing. *5th IEEE Intl. Conf. on High Speed Networks and Multimedia Comms.*, pages 351–355, 2002.

[14] Hongyi Wu S. De, S.K. Das and Chunming Qiao. A resource efficient rt-qos routing protocol for mobile ad hoc networks. *The 5th Int. Symp. on Wireless Personal Multimedia Comms.*, 1:257–261, 2002.

[15] M. D. Castro. The Walnut Kernel : a password-capability based operating system, 1996. Ph.D. Thesis, Monash University, Clayton, Australia.

[16] Bluetooth Security Architecture (Whitepaper). www.bluetooth.com.

[17] Perkins C.E. Das S.R. and Royer E.M. Performance comparison of two on-demand routing protocols for ad hoc networks. *INFOCOM 2000, 19th Annual Joint Conf. of the IEEE Computer and Comms. Societies*, 1:3–12, Aug. 2000.

[18] Marina M.K. and Das S.R. On-demand multipath distance vector routing in ad hoc networks. *9th Intl. Conf. on ICNP*, pages 14–23, 2001.