Airborne Surveillance Networks with Directional Antennas

William Huba, Nirmala Shenoy
Networking Security and Systems Administration Department,
Rochester Institute of Technology, Rochester NY 14623, USA
nxsvks@rit.edu

Abstract— **Surveillance using unmanned aerial vehicles (UAVs) is an important application in tactical networks. Such networks are challenged by the highly dynamic network topologies, which result in frequent link and route breaks. This requires robust routing algorithms and protocols. Depending on the coverage area, several UAVs may be deployed thus requiring solutions that are scalable. The use of directional antennas mitigates the challenges due to limited bandwidth, but requires a scheduling algorithm to provide conflict free schedules to transmitting nodes. In this article we introduce a new approach, which uses a single algorithm 1) that facilitates multi hop overlapped cluster formations to address scalability and data aggregation; 2) provides robust multiple routes from data generating nodes to data aggregation node and; 3) aids in performing distributed scheduling using a Time Division Multiple Access protocol. The integrated solution was modeled using Opnet and evaluated for success rate in packet delivery and average end to end packet delivery latency primarily. The notably high success rates important for surveillance purposes coupled with low latencies validate the use of the proposed solution in critical surveillance applications.**

Keywords-airborne surveillance; network of unmanned aerial vehicles; directional antennas; TDMA

I. INTRODUCTION

Surveillance networks comprising of airborne nodes such as unmanned aerial vehicles (UAVs) are a category of mobile ad hoc networks (MANETs), where the nodes are travelling at speeds of 300 to 400 Kmph. Surveillance requires aggregation of data captured by all nodes in the network at few nodes, from where the data is then sent to a center for further action. Due to high mobility of nodes and varying wireless environment, the topology in surveillance networks is subject to frequent and sporadic changes. Such MANETs thus face severe challenges when forwarding data from node to node, which is the task of the medium access control (MAC) protocol and also in discovering and maintaining routes between source and destination nodes, which is the task of the routing protocols. Another challenge faced is the scalability of the protocols to increasing number of nodes which can be addressed partly through clustering which can also aid in data aggregation

In this article, a unique solution for surveillance networks comprising of UAVs, equipped with directional antennas is investigated. The solution *uses a single algorithm* for several operations such as 1) multi-hop overlapped cluster formation, 2) routing of data from cluster clients to cluster head to aid in data aggregation, and 3) scheduling time slots to transmitting nodes using a Time Division Multiple Access (TDMA) based MAC protocol, which avails the directional antenna capabilities. To best leverage the strengths of this approach, the MAC, clustering and routing functions were implemented as processes operating using a single address that collaboratively address the challenges faced in surveillance networks. Due to the critical nature of the application such a unified or integrated approach is justified. This is vetted by the performance tests conducted in networks with twenty, fifty and seventy five UAVs. The performance metrics of primary interest were success in packet delivery and packet delivery latency which are very important in surveillance applications.

The proposed solution with its various components was modeled using Opnet. Surveillance applications require low packet loss and low information or packet delivery latencies. The unique approach introduced in this article achieves these performance goals. However due to lack of similar published work and the availability of models for such application scenarios, this presentation is limited to result from simulations of the proposed solution.

The rest of the paper is organized as follows. Section II describes related work in the area of TDMA MAC, routing in large MANETs and clustering techniques. The benefits of the integrated approach are highlighted in the light of these discussions. Section III describes the *meshed tree* algorithm - the single algorithm, which is able to support all three operations while allowing them to interact efficiently. Section IV describes the link assignment strategy. Section V provides the performance analysis conducted using Opnet. Conclusions are provided in Section VI.

II. RELATED WORK

The solution in this work targets an integrated approach, facilitated also by the use of a single algorithm. To the best of our knowledge there is no published work that integrates different operations such clustering, scheduling at MAC and routing using a single algorithm and a single address for large surveillance MANETs. In this section, we thus present some related work conducted separately in the areas of TDMA based MAC and scheduling, routing protocols for large MANETs and clustering techniques and conclude by highlighting the advantages of an integrated approach.

TDMA based MAC: To achieve higher capacity and better delay guarantees in networks that use directional antennas, *Spatial reuse Time Division Multiple Access* (STDMA) MAC can be employed. In STDMA, multiple transmissions can be scheduled in a way to avoid packet

ISBN: 978-1-61208-186-1

interference [1]. STDMA thus takes advantage of the spatial separation between nodes to reuse time slots. Such schemes require strict time synchronization among participating nodes. In addition, if the nodes are mobile, periodic changes in the network topology require regular and timely updates to the schedules. The most challenging task is generating conflict free schedules to aid multiple nodes to transmit simultaneously in a time slot. Several algorithms [1-3] have been investigated for the purpose. Some adopt a centralized approach requiring information about all links at the centralized scheduler. Distributed scheduling eases this requirement but at the expense of higher complexity.

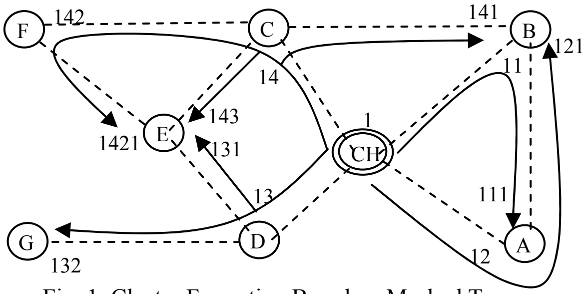

Fig. 1. Cluster Formation Based on Meshed Trees

Literature is rich with work conducted in the area of routing and clustering for MANETs in general. The related work presented here is limited to those routing protocols that are zone limited and multi hop clustering.

Clustering or zoning can be efficiently employed for the type of convergecast traffic encountered in surveillance networks, were the primary traffic flow is from cluster clients (CC) to cluster head (CH) [4, 5]. In such cases proactive routing approaches are recommended as the routing is limited to the cluster or zone and will also reduce stale routes. However proactive routing algorithms require the dissemination of link state information to all routers in the network or zone, which can introduce latency in realizing or breaking a route, and high overhead. In the *Zone Routing Protocol* (ZRP) [6] each node pre-defines a zone centered at itself. ZRP proposes a framework, where any proactive routing protocol can be adopted within the zone and any reactive routing protocol can be adopted to communicate outside of the zone. *Multi path distance vector zone* routing protocol [6] is an implementation of ZRP that uses multi path *Destination Sequence Distance Vector* [7] for proactive routing. *LANMAR* [6] routing protocol defines logical groups to address scalability where landmark nodes keep track of the groups. A local scope routing based on *Fisheye State Routing* is used in the group.

Multi Hop clustering techniques such as the d-hop or k-hop clustering [8] algorithms can offer flexibility in terms of controlling the cluster size and cluster diameter, but are often complex to implement.

Advantages of the Single Algorithm Approach: From the above discussions it would be clear that clustering, routing and scheduling are different operations and hence normally are based on different algorithms. When combining the different operations, it becomes essential to define an interworking mechanism for the different algorithms. This adds processing complexity. It also results in added overhead for the operation of the combined functions. If all these operations can be based off a single algorithm the complexity and overhead can be reduced.

Advantages of Interacting Modules: If the above approach were possible, and if the MAC, routing, clustering and scheduling can use a single address for their operation (unlike our current protocol stack, where MAC protocol uses 48 bit MAC addresses for its operation and routing protocols use 32 bit IP addresses (or 128 bits If IPv6)), we can achieve a solution, where the processes can closely interact and also avoid issues and overhead due to protocol layering, handling different headers and complex cross layered techniques. This would also make the solution compact and efficient and foster close interworking among the different operations. Such an approach would be ideal for critical tactical surveillance networks.

III. THE INTEGRATED APPROACH

The multi meshed tree (MMT) algorithm [10-12] is the one proposed to support the integrated approach and will be briefly explained first. Cluster formations, proactive routing and TDMA scheduling based on this algorithm will be explained subsequently.

A. The Multi Meshed Tree Algorithm

The formation of a single *meshed tree* based on the MMT algorithm is described with the aid of Fig. 1. The dotted lines connect nodes that are in communication range with one another at the physical layer. The node designated as CH is the root of the meshed tree. For ease in explanation, the meshed tree formation is kept simple and restricted to nodes that are connected to the CH by a maximum of 3 hops. At each node several values or IDs have been noted. These are the virtual IDs (VIDs) assigned to the node when it joins one of the tree branches in the meshed tree. Without loss of generality, assume that the CH has a VID '1'. All nodes connected to this CH will have '1' as the first digit in their VIDs. Extending the above logic, a node gets a VID, which will inherit as its prefix the VID of the node upstream in the tree branch (the parent node), followed by a single (or multiple) digit(s) which indicates the child number under that parent. In the presented work the child number is restricted to a single integer - validated by the fact that having more than nine children under a single parent node could cause bottleneck issues during traffic aggregation. In Fig. 1, each arrow from CH is a tree branch that connects the nodes to the root.

Flexible Multi-hop Cluster Formation: Except for the CH, each node in Fig. 1 is a CC that will send the captured surveillance data to the CH. The size of the tree branch can be limited by limiting the length of the VID, which in turn allows control of the diameter of the cluster. Each node that joins the cluster has to register with the CH, by forwarding a registration request (reg_req) along the branch of the VID.

This confirms the path defined by the VID and also allows the CH to accept /reject a joining node to control the cluster size. The number of VIDs allowed for a node can control the amount of meshing in the tree branches of the cluster.

Multiple Dynamic Proactive Paths: The branches of the meshed tree provide the *route* to send and receive data and control packets between the CCs and the CH. The branch denoted by VIDs 14, 142 and 1421 connects nodes C (via VID 14), F (via VID 142) and E (via VID 1421), respectively, to the CH. Consider packet forwarding based on VIDs in which the CH has a packet to send to node E. If the CH decided to use E's VID 1421, it will include this as the destination address and broadcast the packet. En route nodes C and F will pick up the packet and forward to E. This is possible as the VIDs for nodes C and F are contained in E's VID. The VID of a node thus provides a virtual path vector from the CH to itself. Note that the CH could have also used VIDs 143 or 131 for node E, in which case the path taken by the packet would have been CH-C-E or CH-D-E respectively. Thus, between the CH and node E there are multiple routes as identified by the multiple VIDs. The support for multiple proactive routes through the multiple VIDs allows for robust and ***dynamic route adaptability*** to topology changes in the cluster, as the nodes request for new VIDs and joins different branches as their neighbors change. This keeps the routes non-stale.

B. *Scheduling*

The VIDs carry link information between a pair of nodes that share a parent-child relationship. Thus a link assignment strategy was adopted in this work. The structure of the VIDs, also allows each node in a cluster to be aware of its neighbors due to the parent-child relationship defined by the VIDs. This allows a node to schedule time slots with its neighbors (parent or child) taking into consideration its current committed time slots to its other neighbors.

C. *Scalability*

A surveillance network can comprise of several tens of nodes; hence the solutions for surveillance networks have to be scalable to that many nodes. We assume that several 'data aggregation nodes (i.e., CHs)' are uniformly distributed among the non-data aggregation nodes during deployment of the surveillance network. Meshed tree clusters can be formed around each of the data aggregation nodes by assuming them to be roots of the meshed trees. Nodes bordering two or more clusters are allowed to join the different meshed trees and thus reside in the branches originating from different CHs. Such border nodes will inform their CHs about their multiple VIDs under the different clusters. When a node moves away from one cluster, it can still be connected to other clusters, and thus the surveillance data collected by that node is not lost. Also, by allowing nodes to belong to multiple clusters, the single meshed tree cluster based data collection can be extended to *multiple* overlapping *meshed tree* (MMT) clusters that can collect data from several tens of nodes deployed over a wider area with a very low probability of losing any of the captured data. This addresses the *scalability* requirements in surveillance networks.

D. *Interworking of Modules*

It is important to understand the interworking of the modules and their interaction with the directional antenna system. Hence, the directional antenna system is first described followed by the interactions among the modules and their use of the directional antenna systems.

Directional Antenna System: All nodes in the surveillance network are assumed to be equipped with four phased array antennas capable of forming two beam widths. One beam width is focused with an angle of 10^o and the other is defocused with an angle of 90^o. The defocused beams are used for sending broadcast packets, while the focused beams are used for unicast or directed packets. Each antenna array covers a quadrant (90^o) and is independently steerable to focus in a particular direction within that quadrant in the focused beam mode.

We also assume that each node is equipped with a Global Positioning System (GPS) which is used for time synchronization and to provide node position. The latter information is used in a tracking algorithm to estimate the location of a receiver node, so transmitting nodes can direct their beams to the destination node.

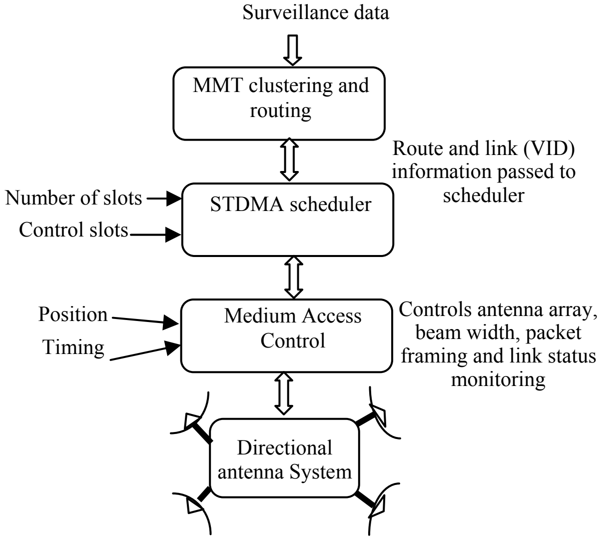

Fig. 2. Scheduler Operations with other Modules

Interworking Principles: The surveillance data collected by the nodes is passed to the MMT clustering and routing module, which decides the route or VID to use to forward the data to the CH. Once the route has been decided, the node knows the address of the next hop node which will forward the packet. This information will be used by the STDMA scheduler to schedule slots, taking as input the number of slots, slot time and control slots. This information is then passed to the MAC to create the frame and forward to the next node. Before forwarding, the MAC, locates the destination node position and controls the antenna array to transmit the packet using a directed beam.

Scheduler Operations: The scheduling algorithm has to schedule time slots for (1) cluster formation after deployment of the UAV nodes, (2) subsequent cluster and route maintenance, and (3) data aggregation. It should also send updated schedules in a timely manner as network topology changes. For all of these operations different categories of time slots as described below were used.

- *Broadcast Slots:* Some slots are preselected as broadcast slots in which they announce their VIDs, location, and current schedule, in a *configuration* (conf) packet, so neighboring nodes can listen and decide to join the cluster.
- *Directed Slots:* All other slots are used in a directed mode, where one node is transmitting using the directed beam to its listening neighbor. Directed slots can be *assigned* slots or *temp* (unassigned) slots.
- *Temp Slots* are used by nodes to negotiate for a common time slot for data transfer.
- *Assigned Slots:* Temp slots become assigned slots after a mutual negotiation by a pair of nodes. In the assigned slots control information for cluster and route maintenance, link maintenance (*lnk_ mnt*) control packet generated by the MAC and data packets are sent and received. Assigned slots are unidirectional and are used either for transmitting (data-tx) or receiving (data-rx). If there are data packets to be sent in such slots slot, the control packets are sent first, followed by the data packets. When there are no data packets to send, the MAC sends lnk-mnt packets to monitor the link status.

IV. LINK ASSIGNMENT

The approval of a new node by the CH is an indication that the CC has both a physical and logical path towards the CH. Scheduling slots for the new node starts subsequent to its acceptance into a cluster by the CH. Nodes individually schedule data slots in a distributed manner with their one-hop neighbors making the scheme truly distributed. The end to end information is carried by the VIDs. Time slots are scheduled for as long as at least one VID remains between a node pair. The process of mutual scheduling is explained with the aid of Fig. 3 below.

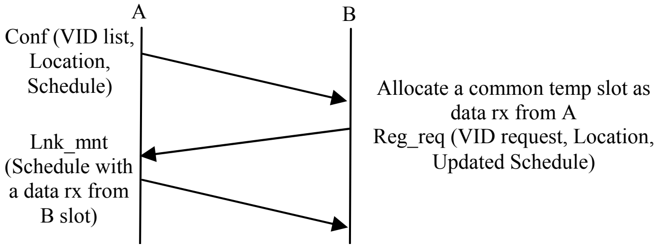

Fig. 3. Distributed Scheduling Across Neighbors

Details about cluster formation, VID acquisition and control packets are covered in [10-12]. When node A advertises its VIDs via a *conf* packet it attaches its current schedule and GPS coordinates. Node B receives the packet and decides to request a VID under one of the advertised VIDs. Node B will then reserve a data-rx slot from one of the temp slots advertised by the parent that matches with its own temp slot and respond with a registration request (reg_req), and the updated schedule to node A. Node A in turn assigns another temp slot that is common to the pair as a data-rx slot for receiving packets from node B. It then forwards the registration request from node B towards the CH. During the next frame, node A will send a *lnk_mnt* packet to node B with the updated schedule. Thus a set of slots for transmitting and receiving between nodes A and B are decided. No other node's schedule is taken into account unless it directly affects the current link between two negotiating nodes.

The process of allowing a new requesting node a VID to reserve a data_rx slot in which the parent node can transmit allows the parent node to resolve conflicts in case the suggested data_rx slot is not available. The parent node does this by sending a lnk_mnt packet on a data-rx slot reserved by the child, requesting that it change its data-rx slot.

A. On Demand Slot Allocation

The above negotiation can be tuned to traffic demands at a node. For example if node A's buffer indicates packet (to be sent to node B) accumulation beyond a threshold value, then in the next lnk-mnt packet, A can request node B to set aside *x* data-rx slots, where the value x is capped to avoid one node taking up all available slots. Node B will respond with the updated schedule by setting aside the *x* slots provided it has no such similar demands from its other neighbors. If there are similar demands, it will allocate slots proportional to the demands of tis neighbors. The on demand allocation can result in increased number of data-rx slots at B (to receive from node A) though the single data-tx towards node A will be maintained unless changed by a demand. The tuning of the on-demand slots is executed every frame.

V. SIMULATIONS

The performance evaluations of the surveillance network using the proposed solution was carried out using Opnet (version 14.5) simulation tool. All the processes explained above were modeled in Opnet. For surveillance data, each CC generated a 1 MByte file, which was then sent to the CH for aggregation. Normally UAVs travel in elliptical trajectories for surveillance purposes. In the models, we used circular orbits, to introduce more route breaks and thus stress test the solution. These circular orbits had a diameter of 20 Km (which defines the areas for each scenario), while the maximum transmission range was limited to 15 Km. the overlap between trajectories is seen in Fig. 4. A maximum of 5 UAVs were allowed in one circular trajectory, thus the UAVs were deployed over a wider area, which was covered with several trajectories. For example, in the 20 node scenario, there were four circular trajectories with slight overlap in their trajectories, to avoid physical network segmentation as shown in Fig 4. In the trajectories, the speed of the UAVs varied between 300 to 400 Kmph; hence, the different colors for the trajectories.

The physical layer parameters were maintained invariant. Packets with 1 bit error rate were dropped and no *Forward Error Correction* was implemented. In the focused beam mode the data rate is 50 Mbps and in the defocused mode the data rate is 1.5 Mbps. A single frame had 50 timeslots each of 4 ms duration and 0.5 ms guard time. These values were optimized based on our prior work [4, 5].

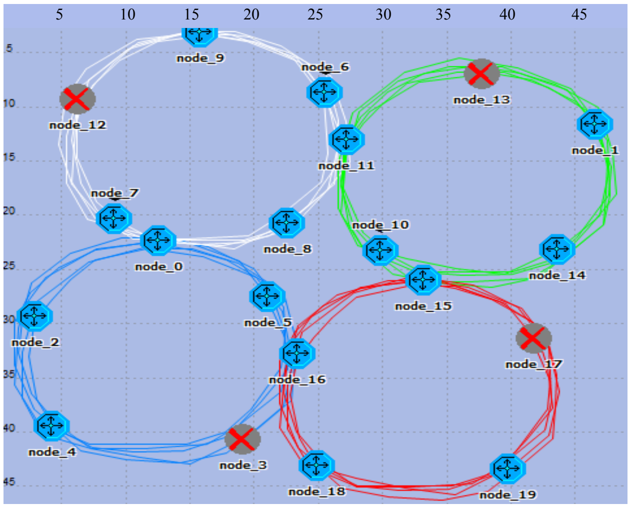

Fig. 4. Typical Deployment and UAVs

Due to the lack of similar published work and comparable models in Opnet the performance of the presented solution is analyzed with respect to the performance goals we had stated for surveillance networks earlier namely success in packet delivery, and latency in packet and file deliveries. Included in the performance graphs are the overhead incurred by the MAC and routing protocols, and the average hops encountered during packet delivery, which is useful in explaining some results

Overhead is the % of control traffic as a ratio of all traffic i.e., including data traffic in the network. Packet latency recorded was the end to end latency i.e. from the time the packet was sent by a sender node till it was received by the CH. File delivery latency was calculated similarly.

In each of the test scenarios, a certain number of nodes were randomly selected to send a 1 MByte file to the CH. These selected nodes sent the files simultaneously, thus stress testing the solution. Furthermore the number of sending nodes was increased to include all of the nodes except the data aggregation nodes, which is a highly stressful test scenario. Each test scenario was repeated with 20 different seeds (high prime numbers) and the results averaged over these seeds. The simulations were limited 20 runs in each case due to the stable outcomes noticed with different seeds.

A. 20 Nodes Scenario

Figures 5A to 5C are the plots for the twenty UAV scenario with 4 clusters. The x axis in all plots shows the number of nodes that are simultaneously sending aggregation traffic, i.e., 1 MByte file to the 4 CHs. The number of sending nodes was varied from 4 to 16. In the last case all 16 CCs were sending a 1 MByte file simultaneously to the CHs.

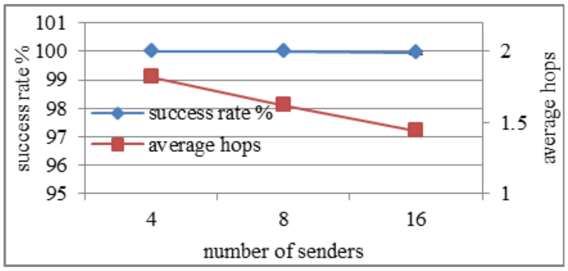

Fig. 5A. Success rate % and Avg hops vs senders

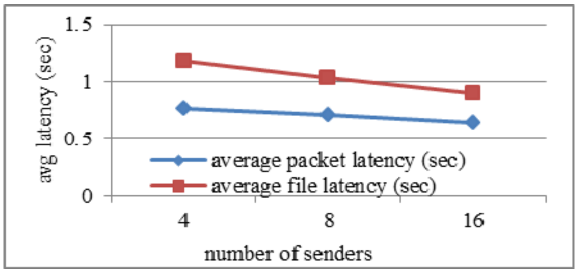

Fig. 5B. Average packet and file latency vs senders

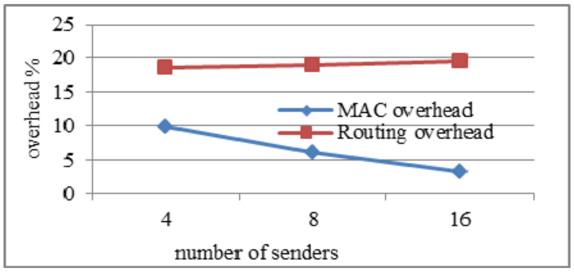

Fig. 5C. Control overhead vs senders

With increasing number of senders, the success rate hardly dropped below 100%. This shows the efficiency of the scheduler to successfully schedule all the packets that are arriving simultaneously. The average hops recorded in graph 1 however shows a decrease when the number of sending nodes was increased. When 20 nodes were selected to send traffic they encountered an average hop distance of 1.8 hops; which dropped to 1.4 hops when all 16 nodes were sending traffic. This is because of the random way in which the sending nodes were selected. The average hops graph can be interpreted thus – the first four nodes that were selected were farther away from the CHs, but as more nodes were randomly picked they were closer to the CH. The impact of this is noticeable in the packet and file latencies recorded in graph B, which shows a decrease with increasing number of senders.

In Fig. 5B, the average packet latency recorded was less than 0.8 seconds. Acceptability of packets arriving at this latency depends on the criticality of the surveillance application. If an upper limit was specified then that could be used as a cut off to drop packets arriving late. The file delivery latency is only slightly higher at around 1.2 seconds, which shows that all packets in the 1 MByte file were transported from the data collection node to the aggregation nodes, i.e., the CH within the time.

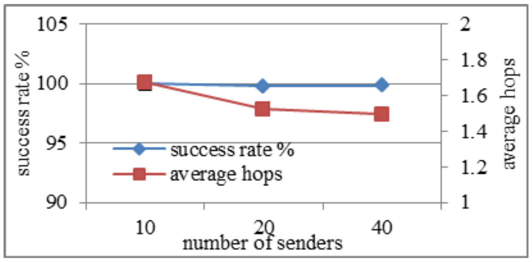

Fig. 6A. Success rate % and Avg hops vs senders

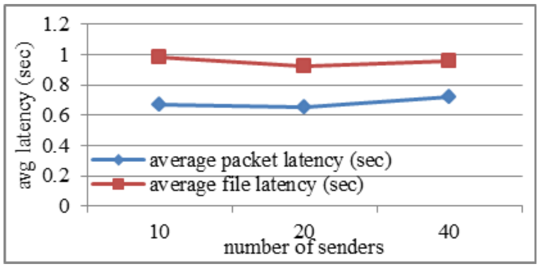

Fig. 6B. Average packet and file latency vs senders

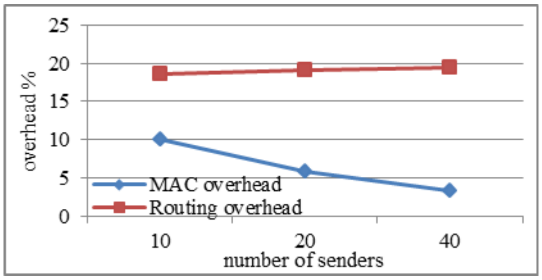

Fig. 6C. Control overhead vs senders

Fig. 5C is the plot of a very important parameter as it shows the channel bandwidth used by the control traffic both by the MMT based routing protocol as well as the MAC protocol. The MAC and routing overhead were recorded to show the ratio of messages used for control purposes by two operations.

The MMT routing overhead was below 20% while the MAC overhead reduced from 10% when there were 4 sending nodes to less than 5% when there were 16 sending nodes. It should be noted that the MMT routing traffic also includes the cluster formation control traffic.

The MAC overhead shows a decrease with increasing number of senders, because when there are fewer data packets to send (with less senders) the MAC still sends maintenance packets, thus the ratio of control bits to the total bits that travelled the network, shows a decrease when there are more data packets in the network. The routing overhead records a very slight increase (around 1%) with increasing senders, which can be attributed to more route maintenance which will be triggered to correctly route the high amount traffic generated.

B. 50 Nodes Scenario

Figures 6A to 6C are the plots for the 50 UAV scenario with 10 clusters. The number of UAVs sending 1 MByte file simultaneously was varied from 10, 20 to 40. Thus in the case of the 40 senders, all CCs were sending 1 MByte files to the CHs simultaneously.

The success rate in graph A shows a slight drop to around 99.7 % as the senders increased, which shows the reliability in data transfer of the proposed solution and its scalability as the number of surveillance nodes and data sending nodes increased. The average hops which is plotted along with success rate graph does not show a linear decrease as in Fig 5 graph A. This is again attributed to the random selection in sending nodes. The first 10 senders were on an average of 1.7 hops from the CH, the added 10 senders for the 20 node case reduced the average hops to slightly above 1.5, and the last 20 senders brought the average hops to 1.5.

Figure 6B reflects the impact of the average hops in the packet and file delivery latency. There is drop when the senders increase from 10 to 20, this is because the average hops has a steep decrease from 1.7 to 1.5. However the average hops drops very slightly when senders are increased from 20 to 40 nodes, this and the fact that there is more traffic and more buffering by the nodes, the packet and file latency increase with increase in senders from 20 to 40.

The MAC and routing overhead in Fig 6C show a similar trend as observed in Fig 5. Though the number of nodes has increases, control traffic is calculated as a ratio of control traffic to total traffic in the network during the time that the files are being delivered.

C. 75 Nodes Scenario

Figures 7A, 7B and 7C are the performance plots for the test scenario with a total of 75 UAVs and 15 clusters, the number of sending nodes was varied from 15, 30 to 60. Hence again when 60 nodes are sending 1 Mbyte file it is the case of all CCs sending traffic to the CHs. The success rate dropped to around 98.7% with increasing number of senders – reflecting the robustness of the proposed solution and its scalability to increasing UAVs and increasing number of senders. The plot of the average hops again shows a decrease from 1.55 to 1.47 as the number of senders selected randomly to send the traffic to the CH was increased.

Figure 7B is the plot for the packet and file latency. The plot shows an increase because the change in the average hops was 0.06 as the number of senders was increased. The latency trends reflect the average hops trend. Figure 7C which is the plot of the MAC and routing overhead has a similar trend as noted for the 20 and 50 node scenarios.

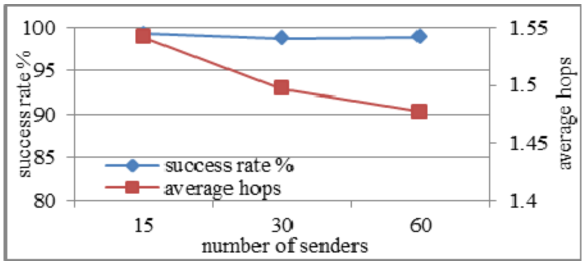

Fig. 7A. Success rate % and Avg hops vs senders

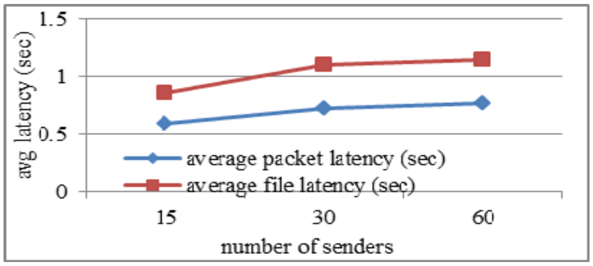

Fig. 7B. Average packet and file latency vs senders

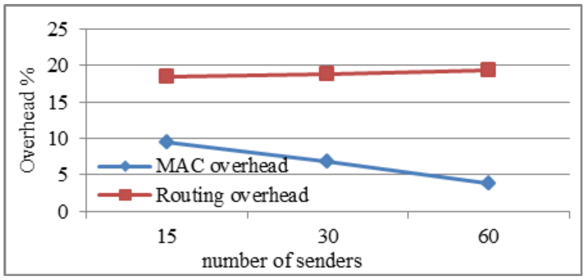

Fig. 7C. Control overhead vs senders

Summarizing, the performance graphs indicate the high robustness of the proposed solutions to highly mobile and stressful MANET conditions. The continually high value of success rate despite the increase in the network size and the increase in the number of sending nodes indicate the reliability of the proposed solutions and its scalability. The packet and file latencies never exceeded 0.8 seconds and 1.2 seconds respectively in the three network setups. This indicates the robustness of the scheduling algorithm.

The overheads noted have similar trends and show very little difference as they were calculated as a ratio of the traffic in the network. The senders in each case were a quarter of the CCs, half of the CCS and the rest of the CCs. The control traffic increases with the increase in the number of nodes in a scenario, but as it is expressed as a ratio of all the traffic in the network including the data traffic, and due to the ratio of senders being consistent in all scenarios, this value can be noticed to be very close in all scenarios.

VI. CONLUSION

Surveillance networks are critical tactical applications, and hence require special consideration during solution design. The primary goal in surveillance networks of UAVs is to collect the captured data reliably at few nodes, and with low latencies. In this work we presented a solution that uses an integrated approach where MAC, routing and scheduling are based off a single algorithm and use a single address - the VIDs for their operations. This results in a low complexity yet robust and scalable solution.

The solution was evaluated in a UAV surveillance network of varying sizes of 20, 50 and 75 nodes. In each case the numbers of simultaneous 1 MByte file senders were increased from one quarter to one half to all of the remaining nodes besides the aggregation nodes. This was a highly stressful test case. The results achieved under such stress situations were very good. The drop in reliable and timely delivery was very low as the numbers of senders were increased. These results thus validate the use of the solution to such critical tactical applications.

ACKNOWLEDGMENT

This work was partly by funded by AFRL, Rome NY under contract no. 30822, and partly from ONR.

REFERENCES

[1] Fernandez S. G., "On the performance of STDMA Link Scheduling and Switched Beamforming Antennas in Wireless Mesh Networks", Master's thesis, King's College London United Kingdom, 2009.

[2] Grönkvist J. and Hansson A., "Comparison between graph-based and interference-based STDMA scheduling," in *MobiHoc*, 2001 pp 255-258

[3] Grönkvist J., "Assignment methods for spatial reuse TDMA, in", First Annual Workshop on Mobile and Ad Hoc Networking and Computing, 2000, pp. 119–124.

[4] Gerla M. and Tsai J., "Multicluster, mobile, multimedia radio network," *Wirel. Netw.*, vol. 1, pp. 255-265, 1995

[5] Lian, J.; Agnew, G.B. and Naik, S., "A variable degree based clustering algorithm for networks," *Computer Communications and Networks, 2003. ICCCN 2003. Proceedings. The 12th International Conference on* , vol., no., pp. 465-470, 20-22 Oct. 2003

[6] Hong X., Xu K., and Gerla M., "Scalable Routing Protocols for Mobile Ad Hoc Networks", *IEEE Network Journal,* July/Aug 2002, Vol 16, issue 4, pp 11-2.

[7] Abolhasan M., Wysocki T. and Dutkiewicz E., "A review of routing protocols for mobile ad hoc networks", *Journal of ad hoc networks,* Elsevier publications, 2004

[8] Orakwue C., Al-Mousa Y., Martin N. and Shenoy N., "Cluster Based Time Division Multiple Access Scheme for Surveillance Networks using Directional Antennas" *ICSPCS, Brisbane Australia* Dec 2010.

[9] Amis, A. D., Prakash, R., Vuong, T.H.P. and Huynh, D.T., "Max-min d-cluster formation in wireless ad hoc networks," INFOCOM 2000. vol.1, no., pp.32-41 vol.1.

[10] Huba W., Martin N., Al-Mousa Y., Orakwue C. and Shenoy N., "A Distributed Scheduler for Airborne Backbone Networks with Directional Antennas", *ComsNets,* Bangalore India 2011

[11] Martin N., Al-Mousa Y. and Shenoy N., "An Integrated Routing and Medium Access Control Framework for Surveillance Networks of Mobile Devices" *12th ICDCN 2011*, Springer Verlag, pp 315-323.

[12] Daniel L., "A comprehensive overview about selected Ad hoc networking routing protocols", *Technical Report, Department of Computer Science,* Munich Technical University, Germany