Tiered Wireless Sensor Network Architecture for Military Surveillance Applications

Louise Lamont, Mylène Toulgoat, Mathieu Déziel
Communications Research Centre
Ottawa, Canada
Email:{louise.lamont, mylene.toulgoat, mathieu.deziel}@crc.gc.ca

Glenn Patterson
Newtrax Technologies Inc.
Montreal, Canada
email: gpatterson@newtrax.com

***Abstract*—This paper presents a novel tiered sensor networking architecture that employs advanced Wireless Sensor Network (WSN) technologies for military operations. This architecture results in an agile surveillance system with a focus on improved operational flexibility and usability. Performance measurements using an in-house simulator are provided using two different scenarios to demonstrate the system's great agility and expandability, operating from possibly a small-scaled single cluster to a network of many chained hop-to-hop connections offering a large coverage area.**

Keywords: ***Tiered Network Architecture; Scalability; deployments; field trial.***

I. INTRODUCTION

The military areas of operation are becoming less contiguous, creating broad surveillance areas that are increasingly more difficult to monitor. The security and force protection of observation posts, for instance, face particular challenges especially when relocation may not be an option due to the requirements of the mission. In addition, the more urban deployment locations of modern military operations include buildings and other man-made structures that block lines of sight creating challenges for reconnaissance systems.

To meet the needs of contemporary deployments, the military requires a sensor system that can detect, classify, and localize hostile forces 24 hours a day in all weather conditions. This system must enhance the surveillance of both critical terrain and nomadic installations to support the monitoring of cease-fire lines, demilitarized zones, encampments, and other high-value assets. As such, the sensor system should be able to reduce the operators' workload while providing greater persistence, thereby freeing up troops for other tasks.

Conventional platform-based military sensor surveillance systems are usually large and expensive, requiring substantial manpower to operate and monitor [1]-[4]. These wireless systems have the ability to sense phenomena from their surrounding environment and communicate the gathered data to a base unit or gateway where the information is sent via long-haul communication to a command and control unit. The deployment requires that the sensors be placed strategically at a certain distance to the gateway to ensure that the sensor nodes are in line-of-sight (LOS) to the gateway or the base station. This deployment configuration results in limited coverage and single point of failures when deployed in complex terrain. Sharing detections and validation of events between sensor nodes is non-existent, which can result in high-levels of false alarms. The application of these systems is limited to predefined and fixed monitoring tasks. For fast and effective deployment, the usability of such systems is very constrained.

Wireless Sensor Networks (WSN) have gained popularity particularly with the proliferation in Micro Electro-Mechanical Systems (MEMS) which have made possible the use of large networks of small wireless sensors that are inexpensive compared to the traditional sensors. Through distributed coordination, WSN are envisioned to enhance situational awareness and improve the effectiveness of military operations. This new generation of WSNs consists of collaborative sensing nodes that are equipped with many transducers, a processor, memory, batteries, and a radio that supports the formation of an ad hoc network for extended communication coverage [5]-[7]. Sensor nodes communicate in a multi-hop fashion to reach a gateway. This type of architecture can be referred to as a planar wireless sensor network. The gateway provides wireless long-haul connectivity between the sensor nodes and the backend command and control station. The gateway bridges the sensed data and alarms to a remote user using beyond line-of-sight (BLOS) communication. The advantages of having the sensor nodes communicate in an ad hoc fashion are that the network is more robust, link redundancy increases system reliability, and sensor nodes can be deployed more rapidly. Additionally, the sensor nodes can perform cross-cueing to validate events before sending the information to the gateway, hence reducing the number of false alarms. The drawback of transmitting the sensory data in a multi-hop fashion is that the throughput per node falls asymptotically with the number of nodes N as $O\sqrt{(1/N)}$. Hence, when large areas need to be monitored, the number of sensor nodes as well as the number of hops to reach the gateway increases resulting in a decreased communication throughput and an increased delay.

A tiered networking architecture can be used to facilitate scalability and address this problem. A number of gateways

The work described herein was funded by Defence Research and Development Canada (DRDC.)

ISBN: 978-1-61208-144-1

can be deployed and the sensor nodes can associate with the closest gateway to form clusters [8-10]. The gateways form the second level of the hierarchy and also form an ad hoc network. When using clustering techniques, one can reduce the number of hops required to reach the gateways and decrease the bottleneck around the gateway. Based on this motivation, we designed and implemented a tiered embedded WSN that exhibits a hierarchical networking architecture that we called Self-healing Autonomous Sensor Network (SASNet).

The SASNet system tackles the fundamental requirements of deployment effectiveness, usability, scalability, reliability, robustness and offers an agile surveillance system with a focus on improved operational flexibility and usability for military applications. SASNet aims at providing a holistic solution that facilitates rapid network deployment and concept of operations.

The remainder of this paper is organized as follows: Section 2 gives an overview of the SASNet network architecture. Section 3 covers the deployment effectiveness and usability. In section 4, the performance of the tiered network is discussed as well the limitations of the network architecture. Section 5 provides the conclusion.

II. SASNET ARCHITECTURE

SASNet is a tiered embedded wireless sensor network that exhibits a hierarchical networking architecture, containing: low cost disposable sensors, the sensor nodes, for extended monitoring coverage; resource-rich specialized nodes, the fusion nodes, for aggregation, database and application processing; and a management node for the command and control by a remote operator.

A. SASNet Hardware

The sensor nodes form the level 1 tier of the network. A sensor node is composed of a transducer board for sensing, an ultrasound board for localization, and a Newtrax WN-200 board [11] for communication as shown in Figure 1. The sensor nodes communicate with each other on a non-IP network in non-standard frequency bands anywhere between 300MHz and $1,100$MHz. They use also this band to communicate with the fusion node belonging to their cluster. The communication board supports data rates in the order of kbps.

The fusion nodes form the level 2 tier of the network. The fusion node hardware is shown in Figure 2. The fusion node consists of a TS7800 ARM embedded computer, a BU-353 GPS receiver, and three radios:

- The first radio operates within the tier-1 network to communicate with the sensor nodes in the lower UHF band.
- The second radio is a more capable radio (in term of data rate) using IEEE 802.11b. It is used to communicate using IP with other fusion nodes at the level 2 tier network in the higher UHF band at a maximum rate of 11Mbps.
- The third radio is a WiMax link between the fusion nodes and the management node. It supports data rates in the order of tens of Mbps.

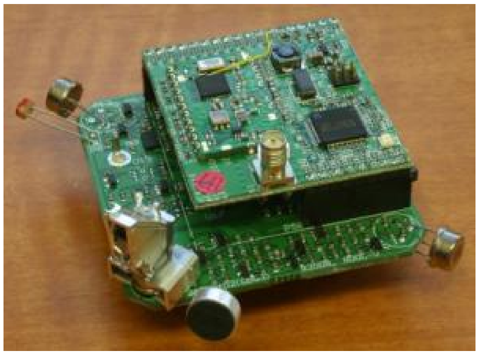


Figure 1. Sensor Node casing.

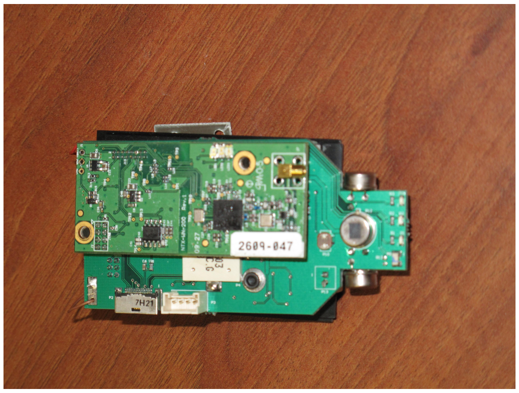


Figure 2. Fusion Node Hardware.

The TS7800 ARM holds the database software, the fusion node application software, and the level 2 tier routing software. The database is contained in the flash memory.

The management node is at the level 3 tier of the network. The management node hardware consists of a laptop computer and a WiMax radio operating in the 5.8GHz band. The laptop holds the Graphical User Interface (GUI) software.

B. SASNet Networking Archirecture

The SASNet hierarchical networking architecture is depicted in Figure 3. The sensor nodes lie at the first level (tier-1) of the hierarchy, where they perform basic operations and provide extended monitoring coverage. Sensor nodes are equipped with on board transducers such as acoustic, seismic, passive infra-red (PIR), magnetic and piezo-electric. They can detect the event of interest, validate the detection by performing cross-cueing, and facilitate classification. Each sensor node in the network acts as a router, forwarding data packets for its neighbor nodes. They form an ad hoc network on the fly and support a single radio interface for

ISBN: 978-1-61208-144-1

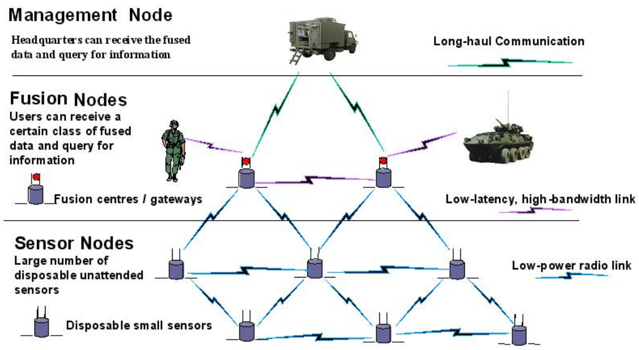

Management Node
Headquarters can receive the fused data and query for information
Long-haul Communication
Fusion Nodes
Users can receive a certain class of fused data and query for information
Fusion centres / gateways
Low-latency, high-bandwidth link
Sensor Nodes
Large number of disposable unattended sensors
Low-power radio link
Disposable small sensors

Figure 3. SASNet Operational Architecture Overview.

bi-directional communication between the sensor nodes and the fusion node.

At the second level (tier-2) of the hierarchy, the fusion nodes provide a more comprehensive function such as database synchronization, cluster formation, application logic formation, and commanding. The fusion nodes receive information requests from users, keep track of command/response queries, task the sensor nodes, aggregate information, and store history of events that have occurred in the area covered by the fusion node. The fusion nodes can also act as actuators in the network, for example, to trigger an onboard or nearby camera to obtain near real time imagery. Unlike the typical WSN, fusion nodes at the second level of the hierarchy also form an ad hoc network enabling extended coverage for larger deployment support. They are equipped with multiple radio interfaces for communication with the sensor nodes and other fusion nodes and for long-range data communications to reach the BLOS management node. The sensor nodes and fusion nodes form clusters that interconnect through capable fusion nodes to construct an unattended ground sensor system.

The management node (MN) at the third level provides the global view of the system for application, for operational control, and for system management. The fusion node uses a long-haul communication link to communicate with the management node. Authorized users can flexibly access the system from the fusion nodes at level 2 or from the management node at level 3. Using a handheld device, a laptop or a station PC, a user with proper authorization can query and subscribe to events, receive the alerts, and view histories of the system activities.

III. DEPLOYMENT EFFECTIVENESS AND USABILITY

SASNet employs the concept of a sensor toolbox allowing for the assigned users to rapidly deploy the system. The sensor toolbox is a lightweight piece of equipment in which the soldier finds necessary tools to instrument an area of interest where remote surveillance tasks are conducted. The toolbox typically contains:

- Multiple sensing nodes supporting multiple sensors per unit (motion, vibration, sound, magnetic field, etc) and a communication module.
- One or multiple ”fusion nodes” that manage the clusters, each consisting of a group of sensor nodes in an area of interest performing one common or multiple sensing tasks.
- One advanced sensor node per cluster, for example an EO sensor, capable of local image analysis.
- Handheld device unit(s) (HHD) used for deploying the network, tasking a cluster, and monitoring activities.

During the deployment, the fusion nodes are placed first and the user must ensure that they communicate with the management node. The fusion nodes are equipped with a GPS receiver and send their position to the management node and the hand-held device. The fusion nodes can be connected directly to the management node using long-haul communication or to another fusion node using ad hoc routing technology when long-haul communication is not available on all fusion nodes. Once the fusion nodes have been deployed successfully, the sensor nodes are deployed and associate with the nearest fusion node to form clusters.

During the deployment, the hand-held device user needs to quickly establish and verify the desired network communication coverage and effectiveness. As the nodes are being deployed, LEDs on the sensor nodes indicate if a network connection has been established to the fusion node or to another sensor node. Network formation is done autonomously. Once the sensor nodes in the system have calculated their position, completed auto-configuration and formed the network, users that are authorized to configure the system view the sensor nodes and the network status on their monitoring interface. Once all sensor nodes in a cluster have been deployed, the network formation of the cluster is verified by the user by tasking the system. After the nodes placement and tasking from the hand-held device have been completed, the task is sent to the management node using the database synchronization scheme. The operator can then add additional tasks if necessary. The hand-held device user can retreat to a covered area that may be a distance away from the monitored area.

Authorized users can formulate the query and/or the event subscription with desired contextual information such as period of time, geographical area, type of event to trigger on and an action to perform. An event subscription sets up the actions following a detection trigger, including further detection and confirmation of the event, sending an alarm for the event trigger, etc. A query can retrieve the past activity reports in the system. Users and operators can be at a distance of a few hundred meters to up to 1 km, or in some cases to up to 10 km from the instrumented area.

ISBN: 978-1-61208-144-1

The user interface on the hand-held device allows navigation through the system information and quick setup of event subscription, tasking, and queries. The user can easily select the geographical area of interest, a period of interest in time, a pre-configured type of event and action such as classification of detected vehicle and alarm with event image reporting.

The operator at the command and control station has more time and can formulate more complex tasks that can be dispatched to the right area and nodes in the network. The useful basic patterns may include as examples, motion pattern detection such as stop, turning direction, and detection contextual information setup such as time, location, and count.

Event subscriptions and associated tasks can be flexibly modified during the operation to monitor new events or to obtain different contextual information of the monitored events. Upon the subscribed event triggering, the network performs the actions as assigned in the corresponding task to collect, coordinate, aggregate the detection information and to send report/alarm to the required destination device(s).

After completion of the SASNet operation for a certain mission, the system is decommissioned and reusable equipments are collected and placed back into the SASNet toolbox.

IV. PERFORMANCE MEASURES OF THE NETWORK

In this section, we use a simulation environment to evaluate the performance of the SASNet system in two different topologies.

The simulation environment is based on the discrete-event model using the OmNet++ architecture and runs the same protocol stack firmware as run on the nodes to simulate a wireless mesh network. The simulator can be easily configured via configuration scripts and results are obtained in the form of reports and detailed event lists. It is also possible to visualize the network topology at any time using Matlab/Octave.

The performance of the network was analyzed using simulation results for two deployment scenarios, namely a single-hop cluster and a multi-hop linear network. We considered the following performance metrics: average one-hop latency, average single node throughput, average rate of packet loss.

A. Scenario 1: Single-Hop Cluster Network

The first scenario represents a cluster of sensor nodes that connect directly to a fusion node in a single hop. We deployed clusters of sizes $N = \{5, 6, 7, 8, 9, 10, 12, 14, 15\}$ nodes in a star-topology where the fusion node is placed at the centre of a circle of radius 35m and the sensor nodes are placed at equal distances along the perimeter of the circle. This represents a worst-case congestion scenario as all nodes are in RF range of one another and therefore can experience interference from any other node in the network.

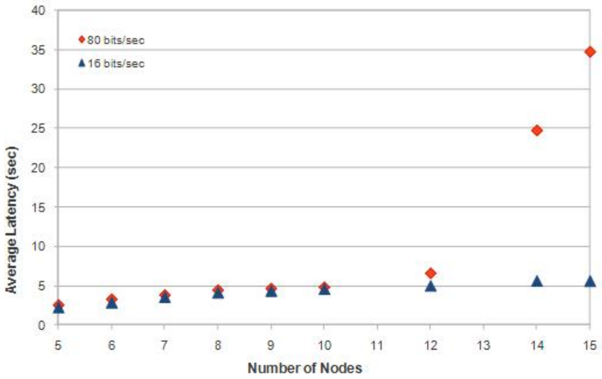


Figure 4. Average Latency for one-hop cluster networks where each sensor node sends data at 16bits/sec and 80bits/sec respectively.

Once the cluster networks form in the simulator, we send 10 byte packets from every sensor at the same instants at two different rates: every second and every five seconds. This gives a packet rate of 16 bits/second and 80 bits/second from each sensor node respectively. We transmit packets continuously over a 4500 second interval.

In Figure 4, we show the average packet latency of the single-hop cluster networks of varying size at both packet rates. We see that when the sensor nodes transmit packets every 5 seconds, the latency per packet is between 2 and 6 seconds as the cluster size increases. For cluster sizes less than ten nodes when we send packets every second, the latency on a typical node is the same as when we send packets every five seconds. However for cluster sizes larger than 12 nodes, we see that the congestion in the network at 80 bits/second causes the latency to sharply increase.

In Figure 5, we show the average packet loss ratio for both sensor node traffic rates. Here we see that for clusters of less than 8 nodes and packet generation every 5 seconds (16 bits/sec) we get very low packet loss. However as the cluster size increases, the congestion of the medium sharply pushes the loss rate above 20%. For packets generated every second (80 bits/sec), the packet loss rate increases linearly above 10% for clusters of size 6 and greater. Sensor networks are known to exhibit severe packet losses due to congestion of a shared medium when supporting high data rates and this is often referred to as the Data Implosion Problem when many nodes simultaneously transmit to a centralized fusion node. This problem is especially exacerbated here because all nodes are in interfering RF range with each other and were forced to connect directly to the fusion node to create a worst-case scenario. The performance could be improved by deploying several fusion nodes to effectively share the network load.

ISBN: 978-1-61208-144-1

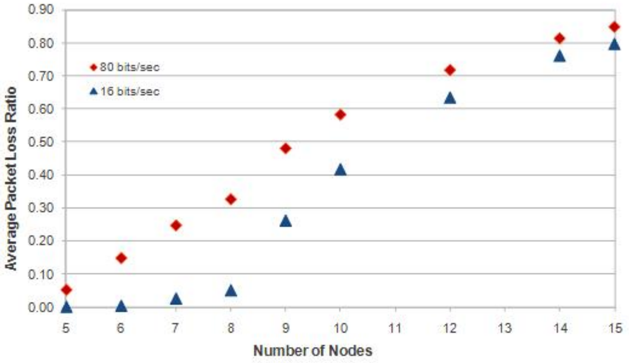


Figure 5. Average Packet Loss Ratio for one-hop cluster networks where sensor nodes send data at 16bits/sec and 80bits/sec respectively.

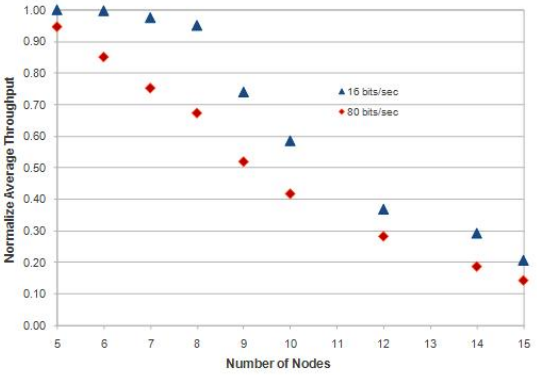


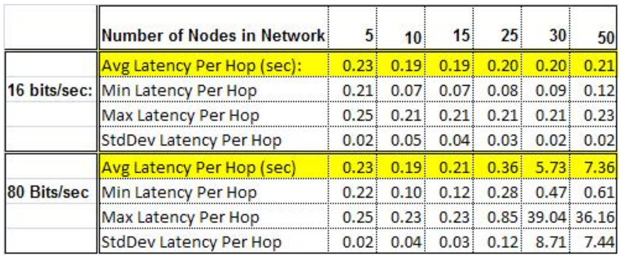
Figure 6. Average node throughput for one-hop cluster networks where nodes send data at 16 bits/second and 80 bits/second respectively normalized by that packet generation rate.

In Figure 6, we show the effective average throughput of a node in the cluster networks for the two different packet generation rates. To compare the results between the two packet rates, we have normalized each curve by the packet generation rates. For packets generated every 5 seconds, the throughput stays very close to the maximum achievable (16 bits/second) for cluster sizes below 9 nodes and then quickly decreases as the cluster size is increased towards 15 nodes. When packets are generated every second, the throughput drops off for all cluster sizes above 5 nodes in a linear manner.

B. *Scenario* 2*: Multi-Hop Linear Network*

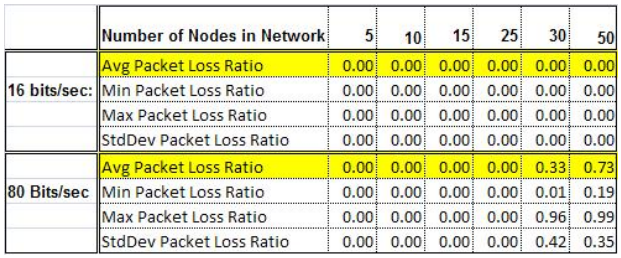
The next set of scenarios studied were multi-hop linear networks of fixed distance between consecutive nodes with the fusion node at the head of the network. In all scenarios, the fixed inter-node distance was 70m between all nodes. At 15dBm transmission power, this creates a network such that any node is only in RF range of its two adjacent neighbors. We experimented with network lengths of $N = \{5, 10, 15, 25, 30, 50\}$ nodes ($N-1$ sensor nodes and 1 fusion node).

Table I
LATENCY STATISTICS FOR MULTI-HOP LINEAR NETWORKS OF VARIOUS LENGTHS AT DATA RATES OF 16 BITS/SEC AND 80 BITS/SEC.



	Number of Nodes in Network	5	10	15	25	30	50
16 bits/sec:	Avg Latency Per Hop (sec):	0.23	0.19	0.19	0.20	0.20	0.21
	Min Latency Per Hop	0.21	0.07	0.07	0.08	0.09	0.12
	Max Latency Per Hop	0.25	0.21	0.21	0.21	0.21	0.23
	StdDev Latency Per Hop	0.02	0.05	0.04	0.03	0.02	0.02
80 Bits/sec	Avg Latency Per Hop (sec)	0.23	0.19	0.21	0.36	5.73	7.36
	Min Latency Per Hop	0.22	0.10	0.12	0.28	0.47	0.61
	Max Latency Per Hop	0.25	0.23	0.23	0.85	39.04	36.16
	StdDev Latency Per Hop	0.02	0.04	0.03	0.12	8.71	7.44

Table II
PACKET-LOSS STATISTICS FOR MULTI-HOP LINEAR NETWORKS OF VARIOUS LENGTHS AT DATA RATES OF 16 BITS/SEC AND 80 BITS/SEC.



	Number of Nodes in Network	5	10	15	25	30	50
16 bits/sec:	Avg Packet Loss Ratio	0.00	0.00	0.00	0.00	0.00	0.00
	Min Packet Loss Ratio	0.00	0.00	0.00	0.00	0.00	0.00
	Max Packet Loss Ratio	0.00	0.00	0.00	0.00	0.00	0.00
	StdDev Packet Loss Ratio	0.00	0.00	0.00	0.00	0.00	0.00
80 Bits/sec	Avg Packet Loss Ratio	0.00	0.00	0.00	0.00	0.33	0.73
	Min Packet Loss Ratio	0.00	0.00	0.00	0.00	0.01	0.19
	Max Packet Loss Ratio	0.00	0.00	0.00	0.00	0.96	0.99
	StdDev Packet Loss Ratio	0.00	0.00	0.00	0.00	0.42	0.35

For each N, we studied the performance of the linear network by sending one 10 byte packet from every sensor at the same instants at two different rates: every second and every five seconds. This gives a packet rate of 16 bits/second and 80 bits/second from each sensor node respectively. We transmit packets continuously over a 4500 second interval.

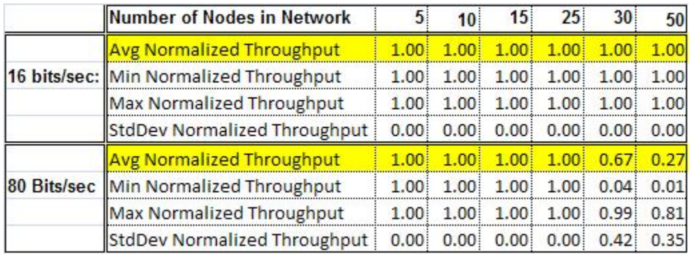
Compared to the star-topology, the linear network where each node is only in RF range of two adjacent neighbors will experience much less congestion of the RF medium. However as we shall discuss later, linear networks have their own congestion problems. In Tables I, II, and III we show the statistics for the latency, packet-loss, and normalized throughput for both data rates with linear networks of various number of nodes.

If we look at the performance at 16 bits/sec data rate, we see that we can successfully deliver all packets generated with optimal latency (about 0.2 sec/hop). When the data rate is increased to 80 bits/sec, for $N \leq 25$ we can deliver all packets with optimal or near optimal latency (0.356 sec/hop in a 25 node network). However for $N \geq 25$ nodes, we see that the performance begins to degrade. In particular, we see nodes close to the fusion node with latencies near 40 seconds for both 30 and 50 node linear networks with corresponding packet-loss rates of 95% and 99.5% respectively.

Unlike the star-topology network previously examined, the performance degradation as the length of the linear

ISBN: 978-1-61208-144-1

Table III
THROUGHPUT (NORMALIZED BY THE DATA RATE) STATISTICS FOR MULTI-HOP LINEAR NETWORKS OF VARIOUS LENGTHS AT DATA RATES OF 16 BITS/SEC AND 80 BITS/SEC.



	Number of Nodes in Network	5	10	15	25	30	50
16 bits/sec:	Avg Normalized Throughput	1.00	1.00	1.00	1.00	1.00	1.00
	Min Normalized Throughput	1.00	1.00	1.00	1.00	1.00	1.00
	Max Normalized Throughput	1.00	1.00	1.00	1.00	1.00	1.00
	StdDev Normalized Throughput	0.00	0.00	0.00	0.00	0.00	0.00
80 Bits/sec	Avg Normalized Throughput	1.00	1.00	1.00	1.00	0.67	0.27
	Min Normalized Throughput	1.00	1.00	1.00	1.00	0.04	0.01
	Max Normalized Throughput	1.00	1.00	1.00	1.00	0.99	0.81
	StdDev Normalized Throughput	0.00	0.00	0.00	0.00	0.42	0.35

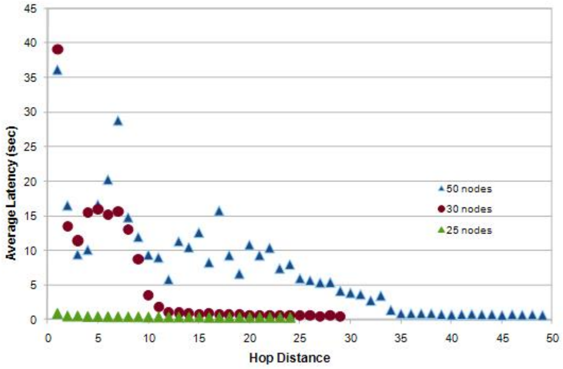


Figure 7. The Average Latency for a multi-hop linear network plotted as a function of hop distance to the fusion node for linear networks of length 25, 30, 50 nodes. Data packets are generated at each node at a rate of 80 bits/sec.

network increases is the result of buffers being filled at down stream nodes close to the fusion node. Basically, the nodes closer to the fusion node must route all the traffic generated further upstream and over an extended period of time, their buffers become full and they will drop packets when this happens. Again, this is a manifestation of the data implosion problem of large-scale sensor networks.

In fact, for $N \geq 30$ the average values in Tables I, II and III are somewhat statistically misleading on account of this data implosion. We see in these tables, that for more than 30 hops in the network, the variance on the latency, packet-drop, and throughput is on the same order of magnitude as the average value. In Figure 7, 8 and 9 we plot the average latency, packet-drop, and throughput of each node in a linear network to illustrate the relationship between the hop-distance to the fusion node and the node performance for $N = \{25, 30, 50\}$ nodes.

Figure 7 demonstrates well the rapidly increasing per-hop latency as packets from downstream nodes get congested in the buffers of nodes closer to the fusion node. For $N = 30$ nodes, the latency starts to increase around the 11^{th} node and gets rapidly worse as we approach the fusion node, and thus about $1/3$ of nodes experience latencies far from the optimal value of about 0.2 sec/hop. For $N = 50$ nodes, the latency starts to increase around the 34^{th} node and gets rapidly worse as we approach the fusion node and so about $2/3$ of the nodes experience latencies far from the optimal value.

Looking at Figure 8, we see that as expected the packet-loss is much higher for the nodes closer to the fusion node. In fact for 50 node networks, the packet-loss is actually relatively low for hop-distances greater than 35 hops. At hop 34, the packet loss sharply swings to almost 100%. This same phenomenon happens at the 10^{th} hop for a 30 node linear network. However, we should note here that if the network were allowed to run for a longer interval and continue to generate packets every second, we could expect that these down-stream sensor nodes farther from the fusion node would one-by-one begin to experience exponentially increasing congestion and at this point there would be essentially no throughput in the network. Also note that contrary to our intuition, the node closest to the fusion node does not have the highest packet-loss rate. For example when we have a 50 node linear network, there is a region of about 30 nodes starting at the 5^{th} node that has almost 100% packet-loss rates. The first 4 nodes after the fusion node have packet-loss rates between 75% and 90%. This phenomenon can be explained as follows. At first, congestion affects the nodes closest to the fusion node. However, as their buffers fill up and they drop packets this phenomenon spreads one node at a time down the network towards the last node in the network. After a certain point, there is so much congestion due to packet transmissions and retries that the packets from the last $1/3$ of the network no longer even reach the nodes closest to the fusion nodes and so the load on these nodes is slightly less than the nodes in the middle of the network and they can successfully route more packets.

We also note here that the degradation of linear network performance at 80 bits/sec data rate is also a function of the time-window over which the packets are generated. For shorter windows, the linear network can successfully handle all the packets. For example, with a linear network of 50 nodes we can generate packets for 78 seconds (a relatively short window) continuously before the nodes close to the fusion node begin to experience buffer congestion and the resulting high packet-loss. For a 30 node network, we can support the 80 bit/sec packet rate for about 300 seconds before buffer congestion and the resulting high packet-loss. Indeed, we can imagine many sensor network applications where there is a large but short-lived burst of data (for example a vehicle moving quickly by all the sensor nodes) and so our networks could support the data generated in these cases. The durations we have tested in our simulations are really meant to give a worst-case and long-term picture of the network performance.

ISBN: 978-1-61208-144-1

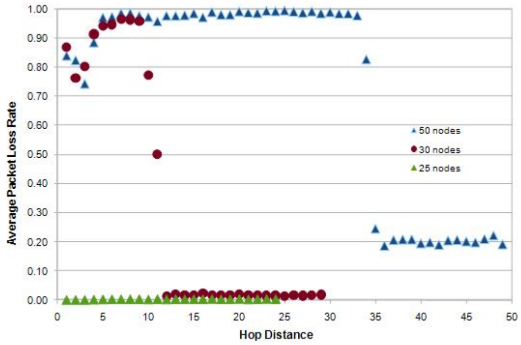


Figure 8. Average Packet Loss as a function of hop-distance to the fusion node for linear networks of length 25, 30, 50 nodes. Data packets are generated at each node at a rate of 80 bits/sec.

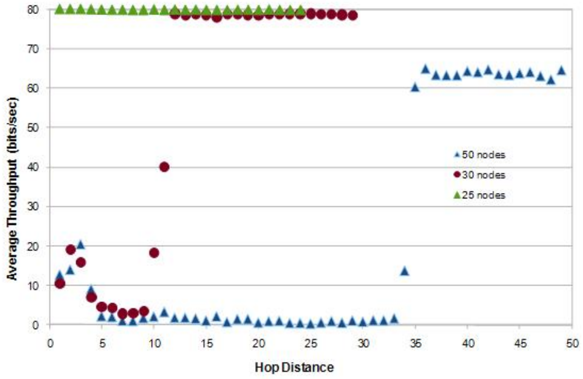


Figure 9. Average Throughput as a function of hop-distance to the fusion node for linear networks of length 25, 30, 50 nodes. Data packets are generated at each node at a rate of 80 bits/sec.

V. CONCLUSION

In this paper we have presented a tiered network architecture that results in an agile surveillance system with a focus on improved operational flexibility and usability. It was shown that two topology families, pure star and pure linear, are special-cases of what we could reasonably expect to form in an actual deployment of sensors in the field. In many applications it is reasonable to expect that not all sensor nodes will be in range of the fusion node and there will be some leap frogging because some sensors will be in range of 3 or more devices and so a pure linear network will form. Thus, what might be expected to form in the field would be closer to a hierarchical tree topology which will alleviate the buffer congestion seen in long linear networks and the wireless medium congestion seen in larger star-topology networks.

REFERENCES

[1] http://defense-update.com/products/f/falcon-watch.htm

[2] http://defense-update.com/products/m/MIS.htm

[3] http://defense-update.com/products/s/SCOUT-UGS.htm

[4] http://defense-update.com/products/r/rembassII.htm

[5] http://www.selex-sas.com/SelexGalileo/EN/Business/Products/Advanced_Sensors/index.sdo

[6] http://www.sownet.nl/download/T-Node_product_sheet.pdf

[7] http://www.exensor.com/index.php?s=systems&k=products&ok=yes

[8] M. Zhang, J. Song, and Y. Zhang, 'Three-Tiered Sensor Networks Architecture for Traffic Information Monitoring and Processing," *Intelligent Robots and Systems (IROS 2005)*, 2005.

[9] Y. Ye, V. Hilaire, A. Koukam, and W. Cai, "A Cluster Based Hybrid Architecture for Wireless Sensor Networks," Information Science and Engineering (ISISE '08), 2008.

[10] O. Gnawali, B. Greenstein, K. Jang, A. Joki, and J. Paek, "The Tenet Architecture for Tiered Sensor Networks", *Proc. the 4th international conference on Embedded networked sensor systems*, 2006.

[11] http://www.newtrax.com/