Performance Analysis of Data Aggregation and Security in WSN-Satellite Integrated Networks

S. Verma, P. Pillai and Y. F. Hu
School of Engineering, Design and Technology
University of Bradford, Bradford, UK

Abstract—Recently there has been an exponential rise in the use of Wireless Sensor Networks (WSNs) in various applications. While WSNs have been primarily used as independent networks, researchers are now looking into ways of integrating them with other existing networks. One such network is the satellite network which provides a reliable communication backbone to remote areas that lack appropriate terrestrial infrastructure. However, due to the integration of the two networks with different transmission and operational characteristics interoperability and security become major concerns. This paper presents an ns-2 based simulation framework of a WSN-satellite integrated network that is used to evaluate the effects of data aggregation and security mechanisms on overall network performance. The average end-to-end packet delay, overall energy consumption and aggregation efficiency are considered for this analysis. This paper also looks into the effects of implementing hop-by-hop security and end-to-end security and justifies the need for end-to-end security in the WSN-satellite integrated networks.

Index Terms—wireless sensor networks, satellite networks, data aggregation, security, integrated networks.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are currently in high demand due to advancements in wireless technology and digital electronics that have enabled the development of low-cost, low-power, multifunctional sensor nodes which communicate over short distances [1]. With the rapid increase in different types of technology and growing number of applications, integration of different technologies is gaining popularity as it enables the efficient utilisation of bandwidth. WSNs are generally used for remote monitoring applications where sensor data is collected and then transmitted to a remote destination. This exchange of sensor data can be done in several ways depending on the network architecture, network size, location of the destination node and the energy requirements. Due to several restrictions of WSNs [2] such as limited power, memory, computational capability, and transmission distance they rely on other existing communication technologies to bridge the communication gap between the source and the remote destination. Thus, they require to be integrated with other long-range fixed-line communications technologies like XDSL, fibre optics or wireless communications technologies 3G/4G, WiMax or even satellites. Over the years, satellites have been used to provide many services, such as satellite television, broadband internet services, GPS and geographical study. It is envisaged that in the future, satellites will be integrated with terrestrial WSNs to further strengthen the employment of WSNs for various applications. The addition of a back-haul satellite to existing terrestrial WSNs ensures that the communication gap is bridged between the sensor source and remote destination, thereby allowing WSN data to be remotely monitored over long distances and overcoming the short transmission range restriction of WSNs. Thus, satellites play an important role in the integration with WSNs wherein they are able to cover a large number of WSNs to provide remote monitoring of inaccessible areas that lack the appropriate terrestrial infrastructure for data transmission. However, in order to efficiently integrate these two networks, it is essential that mechanisms to support optimum and secure use the communication resources are considered.

In-processing techniques like data aggregation are implemented in WSNs in order to minimize the number of data transmissions within the network, thereby conserving nodal energy [3]. Data aggregation is generally implemented on the aggregator node, whose primary function is to receive data from other sensor nodes and aggregate the data (i.e. calculate sum, mean, find min/max, etc.) and forward the aggregated data towards the destination. From a security perspective, end-to-end data confidentiality is usually not supported when data aggregation is employed, since the aggregator node requires access to the plaintext sensor data. Hence, a hop-by-hop encryption is employed along with data aggregation, wherein the encrypted sensor data is first decrypted by the aggregator and then aggregation is performed on the plaintext sensor data and finally the aggregated data is encrypted prior to transmission over the satellite link.

Since data confidentiality is a vital security requirement for a secure sensor-satellite integrated network, this paper analyses the possible effects on the performance of the integrated network when data aggregation techniques and security mechanisms are implemented together.

For this, a WSN-satellite integrated network was designed using Network Simulator 2 (ns-2). The packet loss rate, average end-to-end packet delay, and average energy costs of the nodes were used to analyse the effects on the network performance. The effect of varying dissemination intervals of sensor and aggregator nodes with respect to the packet loss rate at the aggregator node is also analysed.

The rest of the paper is organized as follows. Section II discusses some of the related work on WSN-satellite integrated networks. Section III highlights the network architecture and Section IV outlines some of the security requirements of WSN-satellite integrated networks. Section IV presents the simulation model along with the performance
metrics, the simulation scenarios and the simulation results. Finally the conclusions are presented in Section VI.

II. RELATED WORK

WSNs are most commonly integrated with existing terrestrial infrastructure such as the Internet [4] wherein data from the sensor nodes are transmitted via the Internet backbone to the end user. Some of the popular commercial WSN-satellite integrated networks include the Argos system [5] and the GIS system [6] which primarily monitor and collect data that is then transmitted over the satellite link. Also, the Environmental Monitoring System (EMS) [7] and the Sensor Processing and Acquisition Network (SPAN) [8] have been developed in the research stages to route sensor data over a satellite backbone effectively. The authors of [9] present an architecture iCAAS designed to collect, store, manage and provide heterogeneous WSN data to users depending on their specific interests. However, end-to-end security has not been considered for any of these WSN-satellite integrated networks and only independent security protocols have been used individually by the WSN and satellite network, thus having a hop-by-hop security. The SatNEx-III project [10] mainly focused on the interoperability and integration of WSN and satellite networks and discussed the potential security issues, challenges and threats on such WSN-satellite integrated networks. Thus, in the absence of a security framework particularly catered towards WSN-satellite integrated networks, there is a scope for research in security implementations for WSN-satellite integrated networks along with the implementations of WSN processing techniques such as data aggregation.

III. NETWORK ARCHITECTURE

The network architecture of the WSN-satellite integrated network is adopted from [11] which proposes a cluster-based node layout scheme for the integrated network. The network architecture for the WSN-satellite integrated network used in this paper to study the effects on the overall network performance when security and data aggregation are implemented is shown in Fig. 1 where the WSN is a cluster-based network with each cluster having a cluster head node and a satellite gateway node. For simplicity, it is assumed that the cluster head node is placed at the centre of the WSN cluster, wherein the sensor nodes are arranged in an NxN grid-like manner. The dynamic selection of cluster heads is not considered in this paper. The primary function of the cluster head node is to receive sensor data from sensor nodes within its cluster, aggregate the sensor data, perform data encryption/decryption, and transmit the aggregated data to the gateway node. The main function of the satellite gateway node is to provide the satellite transmission capabilities in order for the transmission of the aggregated data to the remote monitoring station (RMS). There are two ways in which data confidentiality can be achieved in such a WSN-satellite integrated network:

• **Hop-by-Hop Data Encryption**, wherein the sensor nodes transmit the encrypted sensor data to the cluster head node which decrypts the sensor data packet, performs data aggregation, and encrypts the aggregated data packet finally decrypted only at the RMS.

• **End-to-End Data Encryption** wherein the sensor nodes transmit the encrypted sensor data which is decrypted at the RMS.

Since the cluster head node, being a sensor node itself, is responsible for multiple tasks such as transmission/reception, aggregation, encryption/decryption, etc., it is important to perform an evaluation in terms of the energy consumption of the cluster head node since the depletion of a cluster head node could render the whole cluster inactive.

IV. SECURITY REQUIREMENTS OF THE WSN-SATELLITE INTEGRATED NETWORKS

The general security requirements for a WSN-satellite integrated network are as follows:

• **Device Authentication**: Sensor nodes, cluster head nodes and the gateway nodes must authenticate themselves prior to any data transmission since an attacker can pose to be a legitimate sensor, cluster head or a gateway node and transmit erroneous data over the network, redirect or block data. The gateway node also has to authenticate itself with the RMS over the satellite link prior to routing sensor data.

• **Authorisation and Access Control**: Authorisation and access control services of the user may be required at the RMS only to analyse the received sensor data or to transmit any control signals to the sensor nodes, gateway or any other component in the integrated network from the remote monitoring station. Authorisation and access control are important since upon gaining access to the integrated network, an adversary may eavesdrop, modify data or transmit incorrect control signals to the sensors, which may disrupt the entire network.

• **Data Confidentiality**: Two forms of data confidentiality can be achieved in the WSN-satellite integrated network which are mentioned above; hop-by-hop and end-to-end confidentiality. Data confidentiality can be achieved by employing strong data encryption algorithms over the WSNs and the satellite network.

• **Data Integrity**: Data integrity checks are generally performed at the receiver where the receiver checks if the data obtained is same as the data sent. However, in the case...
of the integrated network, data integrity checks may be performed at the cluster head node or at the RMS. The integrated nature of the network provides some challenging issues with respect to security mechanisms since it requires different security algorithms to be applied for each network, key management, and protocol adaptations. Some of the key issues with respect to security are as follows:

- It is difficult to implement both data aggregation and end-to-end confidentiality since the aggregation function may require access to the plaintext sensor data [3].
- It is difficult to implement end-to-end confidentiality and hop-by-hop data integrity, since at each hop the plaintext sensor data may be required for the integrity check.

It is envisaged that a WSN-satellite integrated network should implement data aggregation techniques to minimise the number of data transmissions over the satellite link, end-to-end confidentiality to provide strong security services where only the RMS can decrypt the data, and finally hop-by-hop integrity to avoid the long satellite propagation delays in cases when the integrity check fails at the RMS. This paper focuses mainly on the simultaneous use of data aggregation and data encryption.

V. SIMULATION PARAMETERS & SCENARIOS

The analysis in the paper was conducted using the Mannasim Framework. The Mannasim framework is based on Network Simulator (ns-2) to simulate a wireless sensor network which introduces new modules for the design, development and analysis of various WSN applications. The Mannasim Framework, with respect to the WSN-satellite integrated network, has the following advantages for simulation: provision of modules to handle data aggregation functions such as min/max and average, sensor data generation and provision of node clustering within the network. The simulation parameters used in ns-2 are as shown in Table II.

<table>
<thead>
<tr>
<th>Table II</th>
<th>NS-2 SIMULATION PARAMETERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSN Standard</td>
<td>802.15.4</td>
</tr>
<tr>
<td>WSN Operational Frequency</td>
<td>2.4 GHz</td>
</tr>
<tr>
<td>WSN Operational Data Rate</td>
<td>250 Kbps</td>
</tr>
<tr>
<td>Transmission Distance</td>
<td>~100m</td>
</tr>
<tr>
<td>Sensor Packet Size</td>
<td>1024 bits</td>
</tr>
<tr>
<td>Sensor Transmission Power</td>
<td>0.05 W/packet</td>
</tr>
<tr>
<td>Gateway Transmission Power</td>
<td>4 W/packet</td>
</tr>
<tr>
<td>Sensor Dissemination Interval</td>
<td>1 s</td>
</tr>
<tr>
<td>Gateway Dissemination Interval</td>
<td>1.5 s</td>
</tr>
<tr>
<td>Routing Protocol</td>
<td>LEACH</td>
</tr>
<tr>
<td>Satellite Type</td>
<td>GEO</td>
</tr>
<tr>
<td>Simulation Period</td>
<td>300 seconds</td>
</tr>
<tr>
<td>Topology Area</td>
<td>1000 x 1000 m²</td>
</tr>
<tr>
<td>Agent/Traffic</td>
<td>UDP/CBR</td>
</tr>
<tr>
<td>Sensor Nodes</td>
<td>9-144</td>
</tr>
<tr>
<td>Node Layout Scheme</td>
<td>Cluster-based</td>
</tr>
<tr>
<td>Cluster Head Buffer Size</td>
<td>50 packets</td>
</tr>
</tbody>
</table>

Due to the functionality of data aggregation at the cluster head node and the requirement of a cluster-based node layout scheme, the LEACH protocol has been implemented in the ns-2 framework for routing data within the WSN. Also, with respect to the cluster head node and data aggregation, a dissemination interval is required at the cluster head node which determines the time interval between successive transmissions of aggregated data. The main aim of this paper is to analyse the possible effects of implementation of data aggregation techniques and security mechanisms on the overall network performance of the integrated network. In order to study the effects on network performance, the following scenarios were simulated:

- **Scenario 1**: No implementation of data encryption and data aggregation techniques.
- **Scenario 2**: Implementation of only data aggregation techniques and no data encryption implementation.
- **Scenario 3**: Implementation of both data encryption and data aggregation techniques.

The following performance metrics were used to determine the overall network performance for the sensor-satellite integrated network in accordance with the above mentioned network scenarios:

- **Average Packet Delay (APD)**: It is the average time that a packet takes to travel from the source node to the destination node, measured in milliseconds (ms). This performance metric considers the propagation, transmission, queuing and processing delays of data packets in the network.
- **Packet Loss Rate (PLR)**: It is defined as the percentage ratio of the packets dropped to the packets sent at a particular node such as the cluster head node.
- **Aggregation Efficiency (AE)**: It is defined as the percentage ratio of the packets used by the aggregation function to the packets received by the aggregator node. Within a certain period of time the aggregator node processes a certain number of packets received to calculate the aggregated data. When this time period elapses the aggregated data is disseminated to the gateway node. The aggregation efficiency is used to determine whether there are any received packets at the aggregator node which have not been used by the aggregation function. The higher the aggregation efficiency the lesser the number of received packets that have been dropped by the aggregation function.
- **Total Energy Consumption**: It is the total energy consumption during the simulation period of the cluster head node, measured in Joules (J), i.e. energy consumption for data aggregation, encryption and transmission.

A. Average Packet Delay:

The average packet delay, as shown in Fig. 2, was calculated for all three scenarios with varying number of wireless sensor nodes within a cluster. Fig. 2 shows that by increasing the number of sensor nodes under a single cluster head node, the average packet delay increases due to additional processing. In scenario 2, with the implementation of only data aggregation, it is observed that the additional processing delay due to the aggregation of various sensor data packets produces a higher average packet delay compared to
scenario 1 ranging from 305-325ms, at least a 2% to 5% increase in delay. In Scenario 3, with the implementation of both data aggregation and security, it is observed that the average packet delay is significantly higher compared to the other 2 scenarios. This is mainly due to the additional processing delays induced by the sensor nodes implementing Advanced Encryption Standard (AES) to encrypt sensor data (17ms) and decrypt (13ms) individual sensor packets prior to data aggregation at the aggregator node; aggregation function delay (varies according to the number of packets used for aggregation); and encryption and decryption of the final aggregated data (30ms).

The packet loss rate for the various scenarios is shown in Fig. 3 wherein scenario 1 has the highest PLR since the number of data transmissions is not reduced resulting in a buffer overflow and packet collision. The 18-21% increase in the average packet delay of Scenario 3 results in an increase of 58% for the PLR as compared with Scenario 2 for a maximum of around 150 sensor nodes under a single cluster head node.

B. Aggregation Efficiency:

Wireless sensor nodes have a set dissemination interval, i.e. the sensor node is disseminated towards the cluster head node at a set periodic interval of time. Similarly, the gateway node also has a dissemination interval which is the periodic time interval set for the dissemination of aggregated data towards the receiver over the satellite link. As the dissemination interval of the cluster head node increases the number of data transmissions towards the gateway decreases and the end-to-end delay increases as shown in Fig. 4. For dissemination intervals 1.5s and 2.0s the number of sensor nodes that can be efficiently used under a single cluster head is around 50 nodes. However, for dissemination intervals 2.5s and 3.0s the number of sensor nodes is almost 50% lower, i.e. around 25 sensor nodes can be efficiently used under a single cluster head node.

Fig. 4. Varying aggregation efficiency for different dissemination intervals

From Fig. 4 and Fig. 5 it is observed that with the increase in the number of sensor nodes within a cluster, the aggregation efficiency decreases for different cluster head dissemination intervals, mainly due to the buffer overflow at the aggregating node. It is observed that when the aggregation efficiency starts to drop the energy consumption of the cluster head node starts to attain a constant value mainly since the number of received packets used by the aggregation function decreases resulting in a lesser consumption of energy for data aggregation. Also, for smaller dissemination intervals the aggregation efficiency is high and but the energy consumption for the corresponding dissemination interval is also high, reducing the lifetime of the WSN. Thus from Fig. 4 and Fig. 5 it is evident that there is a trade-off between the aggregation efficiency and the energy consumption of the cluster head and an appropriate dissemination interval should be negotiated prior to data transmission in order to accommodate data processing time and ensure that the number of data transmissions over the satellite link is minimized to meet the energy requirements of the integrated network.
C. Cluster Head Energy Consumption

The total energy consumption of the cluster head node was calculated for various scenarios with varying number of wireless sensor nodes in each cluster, as shown in Fig. 6. The energy required to encrypt/decrypt a single byte of data using the AES-128 security protocol is 1.62 \( \mu J \) [12]. Data aggregation energy of 5 nJ/bit is used to determine the amount of energy spent in aggregating \( N \) sensor data packets of 1024 bits each [13]. The energy required to transmit a single sensor data packet of 1024 bits from the cluster head node to the gateway node is 204.8 \( \mu J \) [11].

It is interesting to note from Fig. 6 that the energy spent by the cluster head node with the implementation of data aggregation and security is almost the same as that of the scenario without the implementation of data aggregation and security. Despite the implementation of data aggregation to further reduce the energy expenditure by minimizing the data transmissions from the cluster head node, a significant amount of energy is spent in decrypting the sensor data packet and encryption of the aggregated packet, when hop-by-hop security mechanism is implemented. Hence, using hop-by-hop security negates the advantages of reduced energy usage due to data aggregation and increases the energy expenditure by 85% compared to end-to-end security for a maximum of 150 nodes under a single cluster head node.

VI. CONCLUSION

From the analysis provided there is a significant difference in the amount of energy consumed by the cluster head node when hop-by-hop security is employed and end-to-end security is employed along with data aggregation. It is observed that the energy saved when end-to-end security is implemented with data aggregation is 88% which increases the life time of the cluster head node. The single cluster analysis can be further extended to study the performance metrics for a multi-cluster scenario for the future work of this paper. It is anticipated that the multi-cluster scenario will reduce the processing load and energy consumption of the cluster head and thus a larger number of sensors can be deployed within the sensing region. However, the main drawback of this approach is additional hardware and self-organizing of the sensor nodes. From the perspective of the gateway which communicates with the satellite, there is future scope for implementation of data fusion techniques which will further reduce the number of data transmissions over the satellite by encapsulating multiple aggregated packets into an IP packet and conserve valuable bandwidth and energy of the gateway node. The analysis concludes that the implementation of hop-by-hop encryption in WSN-satellite integrated networks consumes around 5% to 10% more energy compared to no implementation of either security or data aggregation. Hence this paper justifies the need for end-to-end data encryption along with the implementation of data aggregation and projects the expected energy conservation and the average end-to-end delay.

ACKNOWLEDGEMENT

This work has been partially supported by the European Space Agency contract 23089/10/NL/CLP - SatNEx Network of Experts Call of Order 2.

REFERENCES