Defence Research and Development Canada
Recherche et développement pour la défense Canada

DEFENCE R&D DÉFENSE

Data Dissemination in Wireless Sensor Networks

Requirements, Design Considerations and Research Recommendations

Yasser Gadallah

The work described in this document was sponsored by the Department of National Defence under Work Unit 12PA.

Defence R&D Canada – Ottawa

TECHNICAL MEMORANDUM
DRDC Ottawa TM 2006-134
April 2006

Communications Research Centre Canada

CRC REPORT
CRC-RP-2006-002
April 2006

Canada

Data Dissemination in Wireless Sensor Networks

Requirements, Design Considerations and Research Recommendations

Yasser Gadallah
Communications Research Centre Canada

The work described in this document was sponsored by the Department of National Defense under Work Unit 12PA

Defence R&D Canada – Ottawa

Technical Memorandum

DRDC Ottawa TM 2006-134
April 2006

Communications Research Centre Canada

CRC Report

CRC-RP-2006-002
April 2006

Abstract

Current military wireless sensor networks, such as Optical Acoustic SATCOM Integrated Sensor (OASIS) from Textron Systems, are composed of mini sensors that have the ability to sense phenomena from the surrounding environment and communicate the gathered data to a base unit where the information is sent via satellite to a command and control unit. These systems have limited coverage, require carefully planned deployments and have a single point of failure.

New wireless sensor networks are composed of sensors that collaborate in performing sensing tasks and improve detection and tracking performance through multiple observations, geometric diversity, extended detection range and faster response time. These sensors form an ad hoc network to deliver aggregate information from geographically diverse areas to their destinations. The sensors act as relays and can be randomly deployed, allowing for extended coverage.

Data routing in sensor networks has the main function of establishing and maintaining paths through which this data is transmitted from their sources to their destinations. In this report, we explore the design issues of data routing protocols in wireless sensor networks. Our main goal is to establish a solid starting point for research on routing protocols for military mission-critical wireless sensor networks. As such, we first discuss the characteristics of sensor networks in order to extract some requirements on the operation of routing protocols within these networks. Then, we discuss the non-routing components of the operation that have a direct impact on the routing function. We provide a brief description of these elements as well as establish the link between them in order to extract a list of the required features of the routing component. We then describe some of the routing algorithms that have either been developed specifically for wireless sensor networks or belong to the mobile ad hoc networks, MANET, family (the parent class of wireless sensor networks) and have good performance characteristics. Finally we conduct an experimental comparison study between four routing protocols, two of which were designed for wireless sensor networks and the other two belong to the MANET protocol family. Our experiments reveal that an on-demand MANET protocol outperforms the other protocols from core routing perspective. We therefore make our recommendations for future research which include extending the resulting best protocol to comply with the requirements that we established in this study.

Résumé

Les réseaux de capteurs sans fil militaires actuels, comme l'Optical Acoustic SATCOM Integrated Sensor (OASIS) de Textron Systems, sont composés de mini-capteurs capables de détecter des phénomènes environnants et de communiquer les données recueillies à une unité principale qui les retransmet, à son tour, par satellite à un système de commande et de contrôle. Ces systèmes ont une couverture limitée, exigent des déploiements soigneusement planifiés et possèdent un seul point de défaillance.

Les nouveaux réseaux de capteurs sans fil sont constitués de capteurs qui collaborent à l'exécution de tâches de détection et qui améliorent la performance de détection et de poursuite grâce à des observations multiples, à une diversité géométrique, à une portée de détection étendue et à un temps de réponse plus rapide. Ces capteurs forment un réseau ad hoc pour transmettre des renseignements provenant de régions géographiques diverses vers leurs destinations. Ils servent de relais et ils peuvent être déployés au hasard, ce qui permet d'accroître la couverture.

L'acheminement des données dans un réseau de capteurs permet principalement de créer et de maintenir des voies facilitant le déplacement de ces données entre leurs points de départ et d'arrivée. Dans le présent rapport, nous examinons les problèmes de conception de protocoles d'acheminement des données dans les réseaux de capteurs sans fil. Notre premier objectif est d'établir un point de départ solide pour la recherche sur les protocoles d'acheminement des réseaux de capteurs sans fil militaires qui sont essentiels à la mission. Par conséquent, nous analysons d'abord les caractéristiques des réseaux de capteurs pour cerner quelques exigences relatives au fonctionnement des protocoles d'acheminement dans ces réseaux. Ensuite, nous examinons les composants du fonctionnement qui ne sont pas reliés à l'acheminement, mais qui ont une incidence directe sur ce dernier. Nous fournissons une courte description de ces éléments et nous établissons les liens entre eux afin de dresser la liste des caractéristiques fondamentales du composant de l'acheminement. Puis, nous décrivons quelques-uns des algorithmes d'acheminement qui ont été conçus spécialement pour les réseaux de capteurs sans fil ou qui appartiennent à la catégorie des réseaux mobiles ad hoc (MANET) (catégorie de base des réseaux de capteurs sans fil) et offrent un rendement satisfaisant. Finalement, nous réalisons une étude comparative expérimentale sur les quatre protocoles d'acheminement, dont deux ont été conçus pour les réseaux de capteurs sans fil et les deux autres appartiennent à la catégorie des protocoles de MANET. Notre expérience révèle que le protocole de MANET sur demande est plus performant que les autres protocoles du point de vue de l'acheminement d'infrastructure. Nous formulons donc des recommandations pour les futures recherches, ce qui comprend l'utilisation accrue du meilleur protocole pour satisfaire aux exigences définies dans cette étude.

Executive Summary

Wireless sensor networks are increasingly becoming a key component of the solution for applications that require phenomena detection in a certain geographical area and transmitting the sensed data for processing and utilization in a different geographical area. The large advances in the microchip as well as wireless radio technologies have provided the possibility for utilizing a large number of very small disposable wireless devices in sensor networks. These networks devices can then be deployed to areas that can not be reached by humans due to, for example, environmental disasters. Human operators can communicate remotely with these networks' devices to obtain information about a certain phenomenon in that area. Applications of sensor networks may also involve automatic triggering of devices that are included in the sensor network system upon the occurrence of a certain event. In such a scheme, when a certain event is detected with some certainty by one or more of the network sensors, some devices (e.g. cameras) in another part of the network (or possibly outside the perimeter of the network) are activated to perform a certain action. The broad functional possibilities of sensor networks have made it possible to utilize this technology in many applications that have not been thought possible until recently. Example applications are disaster relief operations, environmental monitoring, wild life habitat monitoring, medical condition detection and monitoring, surveillance, early detection and tracking of enemy movement including response activation, etc.

Many of the wireless sensor network applications depend on deploying a large number of sensor devices (nodes) in a random fashion over a certain geographical area. These areas may be quite large, or not reachable due to a variety of reasons. Consequently, it may not be possible or practical for a human operator to physically access network nodes to perform any configuration or maintenance tasks after they have been deployed. Therefore, many technical challenges arise from such deployment. For example, network nodes will have to be able to self-configure to adjust to their new environment and surroundings. Since the radio range of these wireless devices is often limited, it is crucial that a node cooperates with other nodes within the network in order to be able to achieve the data communication goals behind their deployment. Neighbor discovery then becomes the first major task for these devices after their deployment. Other challenging tasks include unattended error recovery and self-healing, resource-conscious operation and robust data transmission all the way up to the intended data destinations.

In this report, we take a comprehensive look at the data routing function in wireless sensor networks. Our goal is to set a direction and a solid starting point for research in the area of data routing in heterogeneous mission-critical wireless sensor networks. We start by discussing the characteristics of the targeted wireless sensor networks in order to pave the way for discussing the required features of the routing protocols for these networks. We then discuss the factors on which the successful and robust operation of data routing depends. These factors include other functional components of the system such as the energy efficiency policy, node addressing techniques, node localization schemes and routing strategy. The impact of data routing on network operation is directly affected by these components in such a way that an issue with any of these items may render data

routing dysfunctional. We therefore need to keep these elements in mind while doing our design work for data routing techniques in order to ensure a smooth integration of the whole system and a subsequent successful operation for data routing. We conclude our discussion of the routing protocol design issues by extracting a list of requirements that should be considered while designing routing protocols for sensor networks. Due to the active research in this area, many routing protocols have been devised for sensor networks. The motivation being that proven routing protocols that have been developed for the sensor network parent class, the mobile ad hoc networks (MANET), are not suitable for the resource-constrained sensor networks. This claim has not been supported by experimental work, to the best of our knowledge. We therefore discuss the architecture and operation of some of the routing schemes that have been developed for sensor networks. We also describe two of the popular protocols that belong to the main MANET routing categories. We conclude our report by conducting a comparative study of the some of the routing protocols that we have discussed. We use scenarios that are potentially faced in the operation of sensor networks. The goal is to show the relative strength of the protocols under study in order to select the best resulting one for further research. Our study shows that, from core routing strategy perspective, AODV which is a MANET on-demand routing protocol performs best of all studied protocols. The protocols that were specifically designed for sensor networks have performed clearly worse than AODV to varying degrees, depending on the scenario at hand. Our conclusion is to extend AODV, or a similar MANET technique, to adapt to the missing requirements that we outlined earlier in the study. This approach is potentially more promising and cost effective than attempting to fix fundamental performance issues in the core strategy of the other protocols.

Sommaire

Les réseaux de capteurs sans fil deviennent de plus en plus nécessaires aux applications exigeant une détection des phénomènes dans une région géographique donnée et la transmission des données captées afin de les traiter et de les utiliser dans une autre région géographique. Les percées importantes dans les domaines des puces et des technologies radio sans fil permettent l'utilisation d'un grand nombre de très petits appareils sans fil jetables dans des réseaux de capteurs. Ces appareils réseau peuvent être déployés dans des régions inaccessibles aux êtres humains en raison, par exemple, de désastres écologiques. Les opérateurs humains peuvent communiquer à distance avec ces appareils réseau pour obtenir des renseignements sur un phénomène précis dans cette région. Les applications des réseaux de capteurs peuvent aussi comprendre le déclenchement automatique d'appareils présents dans le système de réseau sans fil lorsqu'un événement particulier se produit. Ainsi, quand un tel événement est détecté par au moins un capteur du réseau avec un certain degré de certitude, quelques appareils (p. ex. caméras) situés dans une autre partie du réseau (ou à l'extérieur du périmètre du réseau) sont activés pour exécuter une tâche précise. Les vastes possibilités fonctionnelles des réseaux de capteurs ont rendu possible l'utilisation de cette technologie dans de nombreuses applications qui étaient encore irréalisables tout récemment. Cela comprend, entre autres les applications relatives aux opérations de secours aux sinistrés, à la surveillance environnementale, à la surveillance des habitants fauniques, à la détection et au contrôle des troubles médicaux ainsi qu'à la détection rapide et à la surveillance des mouvements ennemis, dont l'activation de la réponse.

Beaucoup d'applications de réseau de capteurs sans fil dépendent du déploiement d'un grand nombre d'appareils de détection (nœuds) de manière aléatoire dans une région géographique donnée. Une telle région peut être très vaste ou inaccessible pour différentes raisons. C'est pourquoi il peut être difficile ou impossible pour un opérateur humain d'accéder physiquement aux nœuds du réseau en vue d'exécuter des tâches de configuration ou de maintenance après le déploiement. Par conséquent, un déploiement semblable engendre de nombreux problèmes techniques. Par exemple, les nœuds de réseaux doivent être capables de se configurer de manière autonome pour s'ajuster à leur nouvel environnement. Puisque la portée radio de ces appareils sans fil est souvent limitée, un nœud doit obligatoirement collaborer avec les autres nœuds du réseau pour pouvoir atteindre les objectifs de communication des données visés par le déploiement. La détection des nœuds voisins devient alors la première tâche importante de ces appareils après leur déploiement. Les autres défis sont, notamment, la reprise en cas d'erreur inattendue, l'autoregénération, le fonctionnement selon les ressources et la transmission soutenue des données jusqu'aux destinations prévues.

Dans le présent rapport, nous examinons en détail la fonction d'acheminement des données dans les réseaux de capteurs sans fil. Nous souhaitons définir une orientation et établir un point de départ solide pour la recherche sur l'acheminement des données dans les réseaux de capteurs sans fil hétérogènes qui sont essentiels à la mission. Nous

commençons par examiner les caractéristiques des réseaux de capteurs sans fil ciblés de manière à préparer l'analyse des caractéristiques requises par les protocoles d'acheminement de ces réseaux. Nous étudions ensuite les facteurs dont dépendent le fonctionnement soutenu et la réussite de l'acheminement des données. Ces facteurs comprennent d'autres composants du système tels que la politique d'efficacité énergétique, les techniques d'adressage des nœuds, les modèles de localisation des nœuds et la stratégie d'acheminement. L'incidence de l'acheminement des données sur le fonctionnement du réseau dépend directement de ces composants. En effet, l'existence d'un problème avec n'importe quel de ces composants peut perturber l'acheminement des données. Nous devons donc tenir compte de ces éléments lors de la conception des techniques d'acheminement des données pour favoriser l'intégration en douceur de l'ensemble du système et la réussite ultérieure de l'acheminement des données. Nous terminons notre examen des problèmes de conception des protocoles d'acheminement en dressant la liste des exigences à considérer lors de la conception des protocoles d'acheminement pour les réseaux de capteurs. La recherche active dans ce domaine a entraîné la conception de nombreux protocoles d'acheminement pour les réseaux de capteurs. Selon l'hypothèse formulée, les protocoles d'acheminement reconnus qui ont été conçus pour la catégorie de base des réseaux de capteurs, les réseaux mobiles ad hoc (MANET), ne conviennent pas aux réseaux de capteurs aux ressources limitées. À notre connaissance, cette affirmation n'avait jamais été soutenue par des expériences. Nous examinons donc l'architecture et le fonctionnement de quelques-uns des plans d'acheminement élaborés pour les réseaux de capteurs. Nous décrivons aussi deux des protocoles les plus populaires qui appartiennent aux principales catégories d'acheminement des MANET. Nous terminons notre rapport en réalisant une étude comparative sur certains protocoles d'acheminement étudiés. Nous utilisons de scénarios réalistes dans le cadre du fonctionnement de réseaux de capteurs. Le but est de montrer la force relative des protocoles à l'étude afin de sélectionner les meilleurs et de les examiner plus avant. Notre étude démontre que, du point de vue de la stratégie d'acheminement d'infrastructure, le meilleur de tous les protocoles à l'étude est AODV, un protocole d'acheminement sur demande des MANET. Les protocoles conçus spécialement pour les réseaux de capteurs ont obtenu un rendement nettement inférieur au protocole AODV à différents degrés selon le scénario utilisé. Par conséquent, nous recommandons d'accroître l'utilisation du protocole AODV ou d'une technique semblable des MANET pour s'adapter aux exigences manquantes que nous avons recensées précédemment dans l'étude. Cette approche semble plus prometteuse et économique qu'une tentative de résolution des problèmes de rendement fondamental de la stratégie d'infrastructure des autres protocoles.

Table of Contents

List of Figures

1. Introduction

Wireless sensor networks are composed, in general, of several devices of different capabilities and resources that can communicate via their wireless interfaces. Some of these devices are equipped with sensing capabilities that can sense some phenomena of interest and communicate this data to the user or owner of the network through a preconfigured communications paradigm. This communication protocol is included in the software that was installed on network nodes prior to their deployment. Recent technological advances have resulted in the creation of very small and cheap hardware sensing devices that can operate on limited energy resources for extended periods of time. This has opened the way for using this type of networks in many applications that would have otherwise been thought impossible. Networks composed of such devices can be used in situations where they are completely unattended and may not be physically accessible. This can be the case when they are deployed in dangerous or unfriendly environments. As such, the network is expected to be self-configuring and self-healing. Wireless sensor networks may consist of a large number of devices of different capabilities. Some of the devices can be so small that they only possess limited computational, storage and energy resources. Others may be more capable in the sense that they can perform more demanding computational and data analysis tasks and they may have longer communication ranges which enables them to communicate with remote command centers or internet access points. Therefore, we can generally divide network nodes into two main classes: simple nodes with sensing capabilities and limited resources, and nodes that are more capable from computational, storage, wireless range and energy points of view. The latter type of nodes will be called data sinks, or simply “sink nodes” throughout the rest of this report. Sink nodes maybe able to move. This can be the case when they are mounted on vehicles such as military or emergency vehicles.

There are numerous examples for applications that can utilize wireless sensor networks in both the civilian and military arenas. Examples of this can be in areas with environmental problems such as in the case of forest fires, or in disaster areas to aid search and rescue operations. It can also be in situations such as in a battle field where enemy movements need to be detected. In these examples, a large number of sensor devices (nodes) can be randomly deployed (in some applications they can be deployed at specific points of interest) throughout a geographical area of interest. These nodes then self-configure in the sense that they start discovering their neighboring nodes, instantiate their software and data structure etc. Then these nodes engage in the mission for which they have been deployed. When they sense some phenomenon of interest, they start communicating this to designated sink nodes or, depending on the way they have been preconfigured, keep the data for a certain period of time where it gets mined on-demand by data sinks. The communications between sensor nodes and data sinks can be direct or via other network nodes (multi-hop), depending on the proximity of a specific sensor node of interest from the data sink.

From the above discussion, we can infer the existence of several functional components that contribute to the operation of wireless sensor networks. Some of the main items that comprise these components include the radio transmission protocols, the sensing applications, the node addressing algorithm, node localization algorithm, data routing technique, energy efficiency strategy, the media access control protocol, the data transport protocol and the application that is responsible for aggregating and analyzing the data that are being collected from the environment and the data security algorithm.

In this report, we only cover the data routing aspect of the operation. We first discuss the nature of the sensor networks and their anticipated structure. Then we discuss the elements that affect the functionality of routing protocols. The requirements on routing protocols for proper functionality in wireless sensor networks are then outlined. We then describe the functionality of some of the popular routing protocols that can be used in sensor networks. We present the results of a study that compares some data routing protocols of different strategies. Finally, we offer some recommendations for further research on this front.

2. Wireless Sensor Networks: Structure and Operation

Wireless sensor network may consist of a large number of network nodes (can reach a few thousands of nodes). These nodes communicate with each other as needed through a certain preconfigured communication protocol. In most cases, network nodes are configured in the factory or lab and then deployed in the field ready for initialization and joining other nodes to form the network. As we mentioned earlier, the network may be heterogeneous in the sense that not all network nodes have the same capabilities. The entire network, as an entity, may also be connected to the external world, be it processing/command centers or the internet, via nodes of special capabilities that are sometimes termed “gateways”. Gateway nodes normally run the network protocols that are used for communications within the sensor network as well as those that are used by the external world (command centers, internet …etc). Figure 1 shows some examples of network nodes of different sizes, capabilities and functions. From this figure we can see that sensor nodes are already available in different sizes and capabilities for different applications and operational needs. For more examples of commercial sensor network products and their specs, see [23]. The current industry trend shows a tendency for developing very small and yet capable nodes which will expand the possibilities and potential uses of using these devices. Examples of this are the “smart dust” devices [18] which can be as small as one cubic millimeter in size. There is also a tendency for developing very powerful devices that are used as fusion centers (data sinks) and gateways. Also, devices that can carry and actuate equipment such as cameras are being revealed every day.

Figure 1: Examples of wireless sensor network nodes

Figure 2 illustrates an example of a sensor network's structure and relationship with other networks. External sources such as command centers can query data from sensor networks via gateways. Different sensor networks can also exchange data if their gateways are within range of one another. We now zoom further into the operation of the sensor network. For this purpose, we use an example of a sensor network aided military operation, see Figure 3.

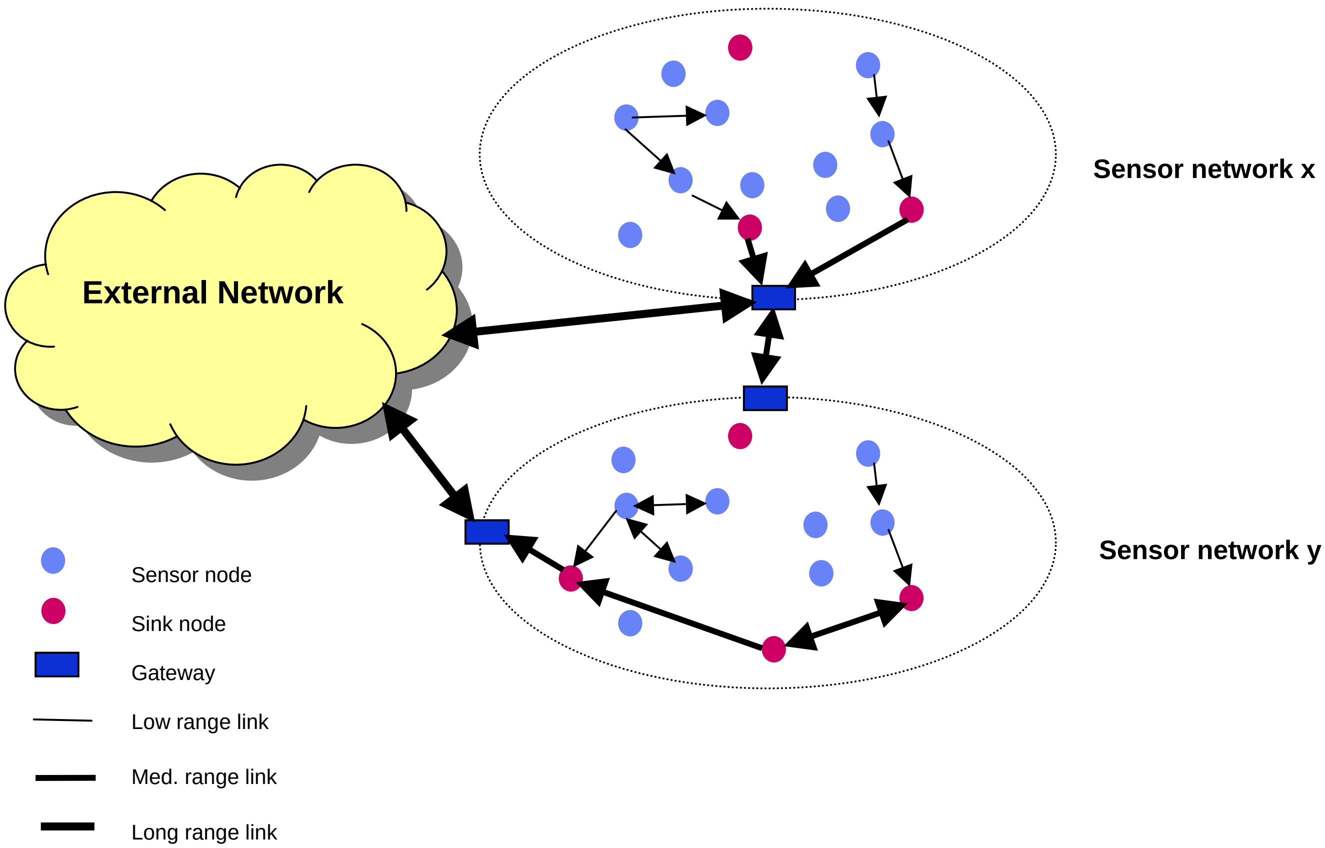

Figure 2: Example of sensor network structure

This example shows a potential realistic use of sensor networks for guiding military operations. Sensor nodes are deployed throughout a certain area of interest for military operations. Sink nodes gather data for aggregation and simple analysis and then make it available for consumers. Data consumers could be individual soldiers, military vehicles, or tactical command centers. Different classes of information are sent to the consumers based on the initial requests. It is worth mentioning that sink nodes can also be mounted on mobile military vehicles or even soldiers. In this case, these vehicles (or soldiers) would be able to query for data directly from sensor nodes (or other fixed fusion centers) to guide a specific operation that they are involved in. Tactical command centers, besides their normal function, can also act as gateways for transferring data to strategic centers for more processing, analysis and plan construction.

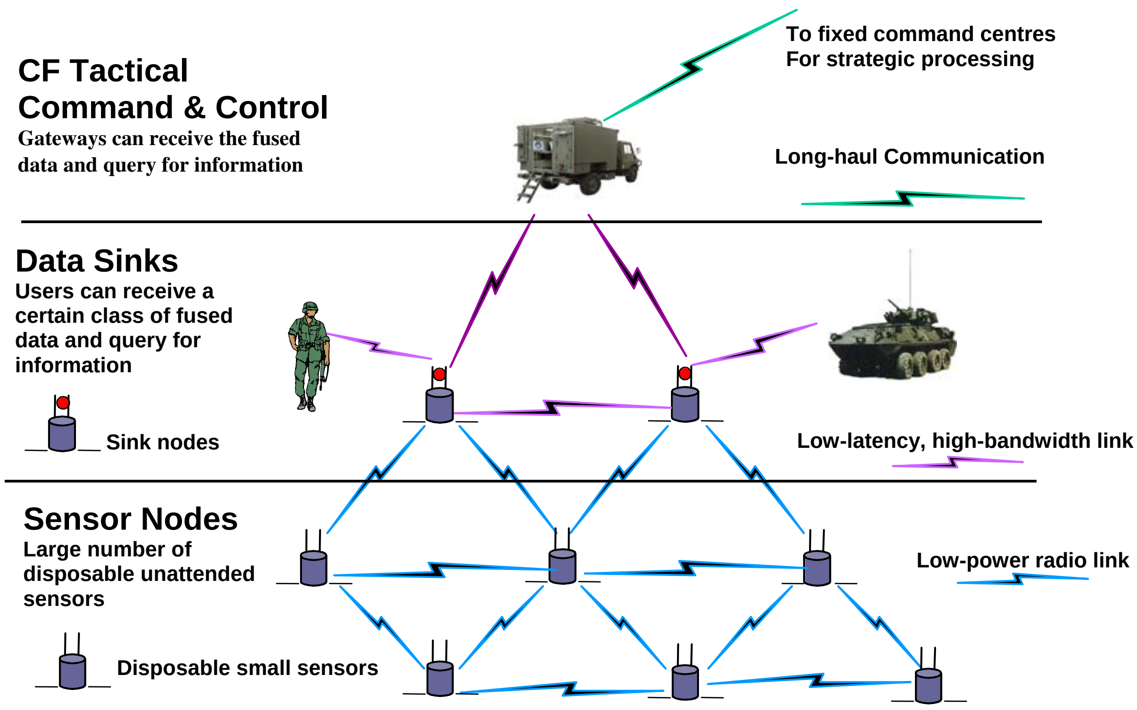

Figure 3: Sensor network usage in military applications

From the discussion so far, one can extract the following characteristics of the wireless sensor networks of interest:

- The network may be heterogeneous in nature. This means that its nodes may not necessarily have the same computational and storage capabilities as each other. This also includes mobility and therefore while sensor nodes are expected to be static, data collection (sink) nodes can be mobile. Some nodes may be carrying devices that extend their capabilities such as GPS's and cameras.
- Sensor nodes have limited resources. This includes energy resources (batteries), memory, storage, and processing capabilities.
- Wireless communication range for sensor nodes is generally limited.
- Network topology is expected to change with time, in general. This could be due to failed nodes, new nodes joining the network, or the mobility of some network nodes.
- Number of nodes within the network is generally large (from few hundreds to few thousands).
- In general, several types of target data are required to be collected by different sensors within the same network. The end point to which this data is sent could be one or more sink nodes.

- Sensor networks are expected to be data-oriented in nature, which means communications would normally target data of specific attributes, for example, as opposed to specific node addresses.

These characteristics pose important requirements on the algorithms that are used for networking within these networks, as we will discuss later in this report.

3. Data Routing in Sensor Networks: Design Considerations

The function of data routing in sensor networks is to establish and maintain data paths for transferring data from sensor nodes where they have been detected to data sinks where they get aggregated and prepared for further analysis or further transferred to their final consumers. Robustness of the techniques used for this function is crucial for the proper and successful operation of the entire network scheme and application. Even though this element of sensor network operation is in itself an area of research and development, it relies for its healthy operation on other elements. These elements can affect its operation significantly to the extent that we can consider routing to be tightly coupled to varying extents with these elements, depending on the requirements on the operation of the network at hand.

In the following, we briefly discuss the elements that affect the functionality of routing protocols as well as the overall requirements on the routing schemes which stem directly from the characteristics of the wireless sensor networks that we outlined earlier in this report.

3.1 Elements that support the routing function

The main elements that are very important to the proper and extended functionality of the routing technique are energy efficiency, addressing, localization and the routing strategy, see Figure 4. We will see, as we discuss the different routing schemes and their relative performance, that one or more of these elements will present an important factor that affects the functionality in some form. For example, in some applications, the accuracy of the localization and addressing techniques affects the operation of the routing algorithm significantly even when the routing scheme itself was built on a sound and robust strategy.

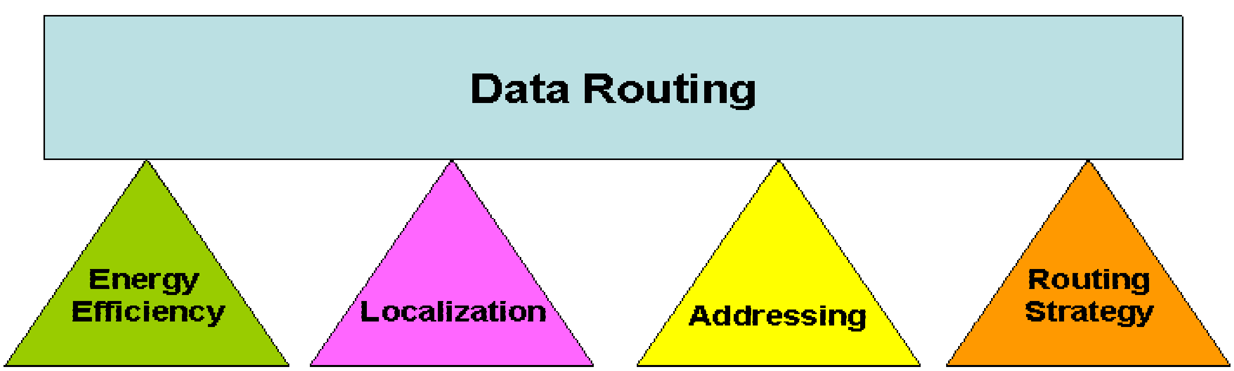

Figure 4: Supporting elements for routing in sensor networks

3.1.1 Energy Efficiency

In a wireless sensor network, a great deal of energy consumption occurs in the wireless interfaces of network nodes. Energy is consumed in send, receive, idle and sleep modes of operation of these interfaces. Idle energy consumption, which occurs when the wireless interfaces are idle, accounts for a considerable amount of energy consumption. Therefore, this wasteful energy consumption has to be reduced or eliminated to prolong the operation and lifetime of the sensor network. The most effective way to achieve this is to put the node interfaces to sleep when idle. There are many requirements on the technique that is to be used to achieve energy efficiency. For example, it has to be fair in order to ensure the extended lifetime of the network and to prevent quick network partitioning. It also has to be able to enable network nodes to determine with certainty the sleep state of their neighbors in order to prevent data losses or unnecessary flooding in search for new routes instead of the ones that are thought broken due to nodes being asleep. The underlying MAC protocol should also be able to support the requirements of the energy-efficient scheme in use. Many energy-efficient schemes that function in conjunction with routing protocols have been developed for MANET, see for example [3], [6], [19],[21]. There is a need to investigate the integration or customization of an energy-efficient strategy to the needs of wireless sensor networks. This will affect to some extent the routing strategy that is utilized in the network.

3.1.2 Localization

Localization is used to determine the location of different nodes within the sensor network. From a routing perspective, node locations are needed for one or more of the following purposes:

- Directing and processing location-based queries
- Supporting location-based routing
- Supporting location-based addressing

Therefore, localization techniques that are used in connection to routing need only provide location information that is accurate enough to carry out these duties. These techniques also have to have the minimum possible communication and computation overhead. This is to conserve the network bandwidth and also network node energies. The algorithms need also to be adaptable to the functionality of the utilized energy-efficient scheme. For example sensor network localization techniques see [2],[14],[15].

3.1.3 Addressing

In most sensor network applications, the process of searching for specific data does not usually depend on nodes with certain addresses, i.e. it is not an address-centric search process. It only depends on the attributes of the data in question. However, once the source of this data is located, a path needs to be established between data source(s) and the data requesting party. Communications would then switch from broadcast-style communication to some form of point-to-point communication. Once this stage is reached, node addressing becomes a basic requirement for establishing communication links. Addressing presents a major source of potential issues in sensor networks for the following main reasons:

- The potentially large number of network nodes
- The unattended mode of operation of many sensor networks which makes it quite difficult if not impossible to manually configure node addresses
- Limited node energies

The use of IP addressing in its regular form is not practical due to the overhead of communicating the IP headers of the regular IP scheme combined with the fact that operator-configured sensor nodes are not possible in many sensor networks applications. Addressing in sensor networks may not be global; rather it may only be neighbourhood and/or location dependent. In any case, addressing schemes should ensure that there are no duplicate addresses that are encountered by any network node. There are many addressing schemes that have been developed for sensor networks, see for example [7], [11], [16].

3.1.4 Routing Strategy

Routing strategy determines the methodology and semantics of the routing algorithm's operation. It is responsible for the reliability, robustness and impact of the routing algorithm on network's operation. The routing strategy can be divided along several lines. For example, we can classify the routing algorithms based on how it arranges network nodes; with the resulting algorithms being clustered versus distributed. Another arrangement would classify the algorithms based on their dependence on geographical information. Based on this, some algorithms would follow a geographical routing strategy while others are non-geographical based. A third classification would divide the algorithms into proactive versus reactive. Each routing strategy has its requirements and at the same time has its implications on network operation. For example, from a requirements perspective, geographical algorithms require network nodes to be location-aware. As an example of the implication of the routing strategy, using a proactive routing algorithm may add some extra overhead that can be costly in terms of the network bandwidth and node energies. On the other hand, it may be beneficial in reducing data delivery latency. Therefore, the routing strategy should be selected carefully in such a way that will make it both achievable (e.g. geographical routing cannot be used in networks whose nodes are not location aware) as well as cost effective (e.g. the benefit of using proactive approaches should justify their extra overhead).

3.2 Dynamics of Network Operation and Requirements on Routing Algorithms

From the above discussion we see that there are many elements that directly affect the correctness, robustness and continuity of the data routing function within sensor networks. Figure 5 shows the dynamics of network operation and the interaction of the different elements from a routing functionality perspective.

From the above discussion and the characteristics of wireless sensor networks that we discussed in the previous chapter, we can extract the following main requirements that have to be met by sensor network routing protocols for mission-critical operation:

- The overhead of the routing protocol specific traffic should not be significant to avoid overloading the bandwidth constrained network or affecting network throughput. Also, it should not impose heavy computational, storage or memory requirements on network nodes.
- The routing protocol should be able to scale with the size of the network population and traffic.
- The routing protocol should either be inherently energy-efficient, or be adaptable to integration with some algorithm that enables it to achieve this goal. Energy-efficient operation implies using node energies both wisely and fairly.
- The functionality of the routing protocol should be distributed, as opposed to centralized, for robustness. Therefore, the protocol should not be constantly dependent on a node or a subset of network nodes for its functionality.
- The routing protocol should be able to respond to changing network conditions and topology promptly and efficiently without imposing heavy traffic load on the network as a result.
- The routing protocol should be able to support multi-hop operation due to the limited sensor node wireless ranges.
- The routing algorithm should be able to support the data-oriented nature of sensor networks.

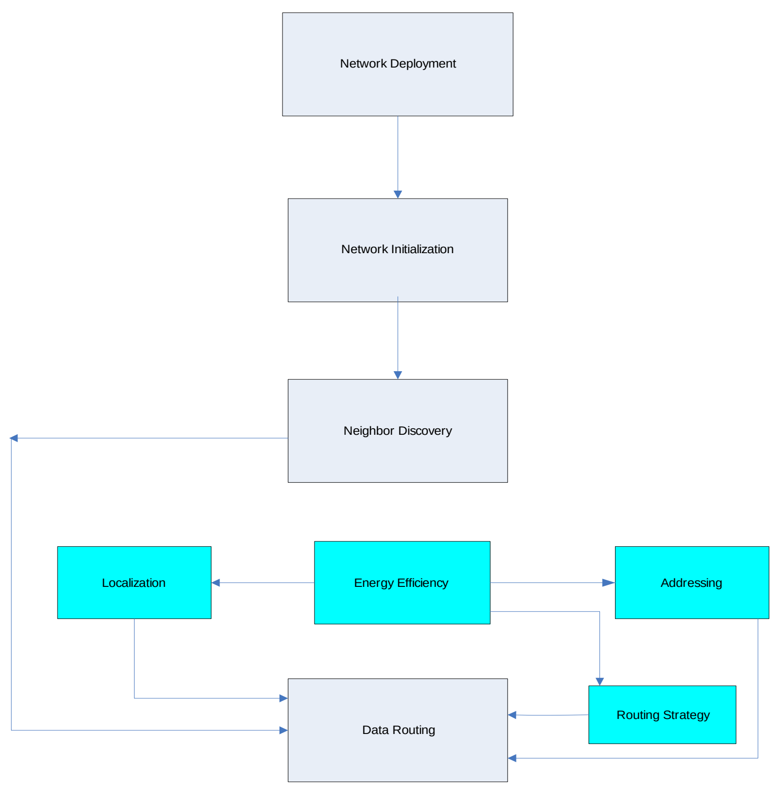

Figure 5: Network operation from data routing perspective

The task to locate a single algorithm that meets all the above requirements can prove challenging. Therefore, the search strategy will revolve around finding a “best fit” algorithm that meets the core requirements. Work will then be needed to modify the algorithm in order to make it compliant with the rest of the requirements, or most of them. One of the main selection criteria is ensuring that the modifications to be made will not affect or alter the core strategy of the chosen routing algorithm. Acceptable modifications should only deal with add-on functionality rather than major changes that affect the methodology by which the algorithm handles the routing function.

4. Data Routing Techniques in Wireless Sensor Networks

Many techniques have been created specifically for data transfer within sensor networks, see for example the survey in [1]. Despite the existence of well established routing techniques that have been developed and used successfully in mobile ad hoc network (MANET) applications, there have been some assertions (e.g. in [5]) that the special nature of wireless sensor networks makes the use of MANET algorithms impractical in sensor networks. Later in this document, we examine this claim and make some recommendations based on our findings. However, in this chapter we will include some of the popular MANET protocols in our discussion to pave the way for our subsequent comparison discussion.
As we mentioned earlier in this report, routing protocols can be classified along several lines. In this chapter, we divide these techniques into the following two classes:

- Clustered (or grid-based) protocols
- Non-clustered protocols

Routing protocols that belong to the same category may resort to using different techniques, e.g. some techniques may be based on geographical locations of network nodes while others may function independently of node locations, etc. Conversely, we may find that the same technique is utilized by routing protocols that belong to different categories.

In the following sections we describe each of the above categories together with some representative algorithms. We have selected the protocols that can potentially accommodate military applications such as the one that we illustrated in Figure 3 in this report. Furthermore, our subsequent evaluation work of these protocols will consider the elements of the scenarios of such applications, such as different node capabilities and mobile gateways or sink nodes.

4.1 Non-clustered Protocols

In this category, the topology is flat in such a way that it is not divided into groups of nodes for which one or more of the group nodes perform duties on behalf of other nodes within the group. Therefore, all nodes are considered to have the same weight or rank at any point in time with regard to the functionality of the algorithm. The differentiator between nodes would only be the suitability of the node's position or state for a certain route or path.

This class includes routing protocols that may follow different routing strategies. For example, shortest path MANET techniques that belong to both the proactive and reactive routing approaches can be considered members of this category. Also, distributed data-oriented techniques that have been developed specifically for wireless sensor networks such as directed diffusion are also members of this category. In the following, we describe three of the algorithms that belong to this category but use different techniques: the directed diffusion, AODV and OLSR algorithms.

4.1.1 Directed Diffusion

In the directed diffusion algorithm [8], communications between nodes is done on the basis of one-on-one communications. Therefore, no elaborate routing is done. Sink nodes decide on which data is needed and the intervals at which this data needs to be transmitted. The concept of the gradient, which mainly describes the data, its dissemination frequency and its flow direction, is used to handle data transfers. The process starts by a sink node broadcasting its need for certain data that is described by specific attributes. This request gets propagated through the network until it reaches a node that either possesses this data or knows where to get it. When several responses reach the requesting sink node, it accepts the first one and enforces the continuation of obtaining data from the neighbor from which the fastest response was obtained. This operation is shown in Figure 6. The rest of the neighbors continue to receive exploratory events, which are data packets at a reduced rate. Although the purpose of this strategy is to add robustness to the operation by making backup paths available, this can be a source of bandwidth overhead and energy consumption. When we consider the criteria that we discussed in the pervious chapter we note that directed diffusion does not possess inherent energy-efficiency features. Therefore its adaptability to integration with a complementary energy-efficient technique needs to be investigated.

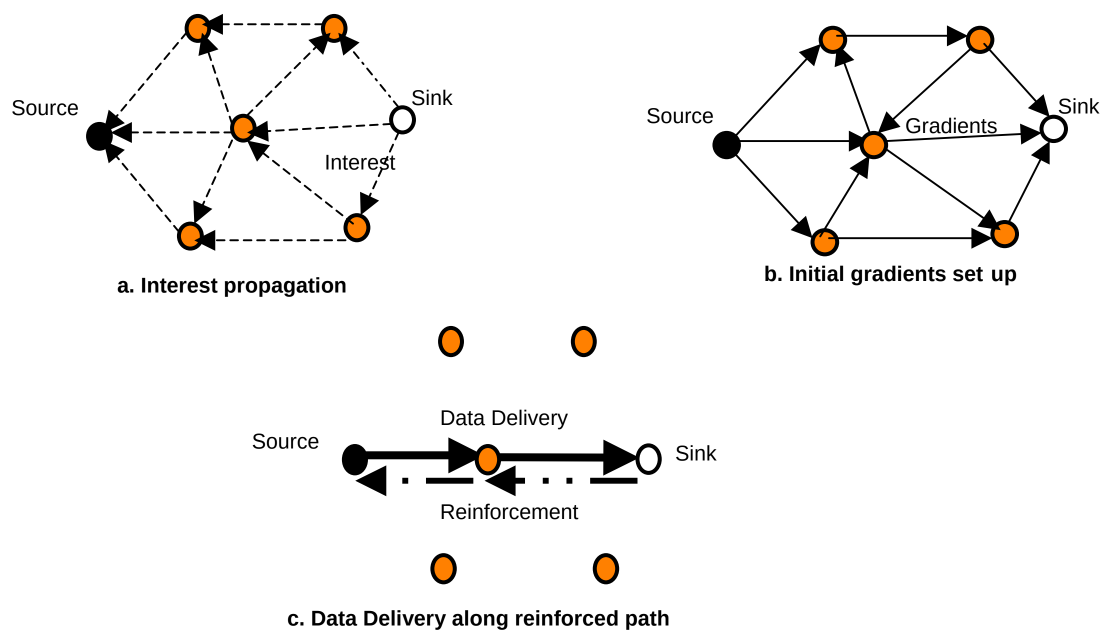

Figure 6: Path discovery in directed diffusion

4.1.2 AODV

The functionality of the AODV protocol [12] is based on maintaining a vector of paths (i.e. routing table) that lead to the different destinations at each node. Route establishment is done on demand. A given node does not have a full knowledge of any of the routes. It only knows the next node along any given route. Each node keeps only one route (the one that has the smallest number of hops, i.e. the shortest route) to any given destination. When a node needs to communicate with another node to which it does not have a route, it sends a route request to its neighbors. This request gets propagated via broadcast in the network until a node that knows a route is found. It then replies back informing that it knows a route. The classic AODV algorithm also uses periodic HELLO messages to keep neighbors aware of the other nodes in the neighborhood. In more recent versions of AODV, this is done via relying on the link state capabilities of the underlying MAC protocol. This procedure is used for route maintenance. AODV is not a data-oriented algorithm. This is an area that needs to be addressed to make it viable for use in many of the sensor network applications. Also, it does not have an inherent energy-efficiency strategy. However, it has been shown to integrate successfully with energy-efficient algorithms [6]. Also, its dependence on IP addressing can introduce unnecessary overhead to sensor network operations. To overcome this issue, a light IP implementation that is suitable for sensor networks can be used [4]. Alternatively, non-IP based versions of AODV can be used.

4.1.3 OLSR

The OLSR (Optimized Link State Routing) protocol [10] belongs to the proactive routing category in MANET. In this protocol, nodes exchange topology information on a regular basis. Selected multipoint relay (MPR) nodes announce this information periodically to the network. These nodes are also used in determining the route from any network node to a given destination. MPR node selection depends on periodical exchange of HELLO messages between nodes. Also, topology control messages are sent periodically (or upon MPR node changes) to maintain topology information throughout the network. With regard to the criteria discussed in section 2, the aspects that we discussed in the AODV case apply equally to OLSR. In addition, the overhead of the OLSR proactive approach in determining routes to all network nodes can result in unnecessary overhead to sensor network operation even though it can also have a positive impact in lowering packet delivery latency in some scenarios.

4.2 Clustered Protocols

Routing protocols that belong to this category usually organize the network into clusters or cells of network nodes, with each cluster having a specific node or nodes designated to act on behalf of the cluster nodes. These nodes are sometimes called the cluster heads. The designated nodes within a cluster are in general responsible for communicating the data of their cluster nodes or exclusively handling data forwarding to the destination or next hop in the structure. There are several possible criteria for selecting the cluster head. For example, it could be selected based on its remaining energy. Alternatively, the proximity to the sink node can be used as the selection criteria, and so on. Usually, the main goal of this category of algorithms is to achieve energy efficiency by decreasing the number of nodes that have to contribute to data transmissions to the sink. In the following, we describe two of the algorithms that belong to this category: the LEACH and the TTDD algorithms. These techniques use different techniques to carry out the routing duties as we will see shortly.

4.2.1 Leach

One of the main algorithms that belong to this category is the LEACH (Low-Energy Adaptive Clustering Hierarchy) algorithm [13]. In this algorithm, network nodes organize themselves into clusters. Each cluster has a cluster head. The cluster head, which will handle communications with the sink node on behalf of cluster nodes, gets selected based on a certain scheme that depends on determining a certain percentage of network nodes that would be acting as cluster heads at a given point of time. The cluster formation operation in LEACH is illustrated by Figure 7. Nodes that have not become cluster heads in the previous rounds are the candidates to become cluster heads in the upcoming rounds until all nodes are covered. After cluster heads have been selected, they advertise their new status. Network nodes then decide to which cluster they would belong based on the signal strength of the advertisement packets that reach them from the different cluster heads. In case of a tie, the cluster selection is done randomly by the node. Once clusters have been established, each cluster head establishes a TDMA schedule for its cluster nodes for sending their data to it and inform the nodes when they should transmit by broadcasting the schedule within their own cluster. The cluster heads perform local data fusion and send the information to the sinks (gateways). When it is the time slot for a certain node, it sends its data to its cluster head. Otherwise, it turns its radio interfaces off thus saving its energy. LEACH also uses CDMA coding to avoid communication interferences between adjacent clusters. LEACH attempts to handle communications with the sink via a single hop approach. Consequently, each cluster head communicates directly with the sink by adjusting its transmission power. In situations where the network is spread over a large area, this may not work. Also, with a single node handling communications for the whole cluster at any point of time, this may cause the communications from and to this cluster to be interrupted for a period of time if this node fails, until all nodes within the cluster wake up and decide to elect a new head to recover from this failure. Finally, the current implementation of LEACH assumes the existence of only one sink node which may limit the usefulness of the algorithm in many wireless sensor network applications.

4.2.2 Two-Tier Data Dissemination (TTDD)

The TTDD design [20] is built on the assumption that network sensor nodes are stationary and location-aware. A source node detects an event and proactively builds a grid structure throughout the sensor field and sets up the forwarding information only at the sensors closest to grid points (dissemination nodes). The cell size, α, is a critical parameter for the functionality of TTDD. Its choice, according to the TTDD authors is dependent on the application at hand. Data sinks need to flood their queries only within their local cells until a dissemination node is reached. Once the query reaches a local dissemination point, it is forwarded on the grid upstream towards the source. Each dissemination node along the path keeps information about the downstream node from which it got the query. Data is then sent back from the source to the requesting sink along the same path. A one source-one sink example of the TTDD operation is shown in Figure 8. TTDD handles sink

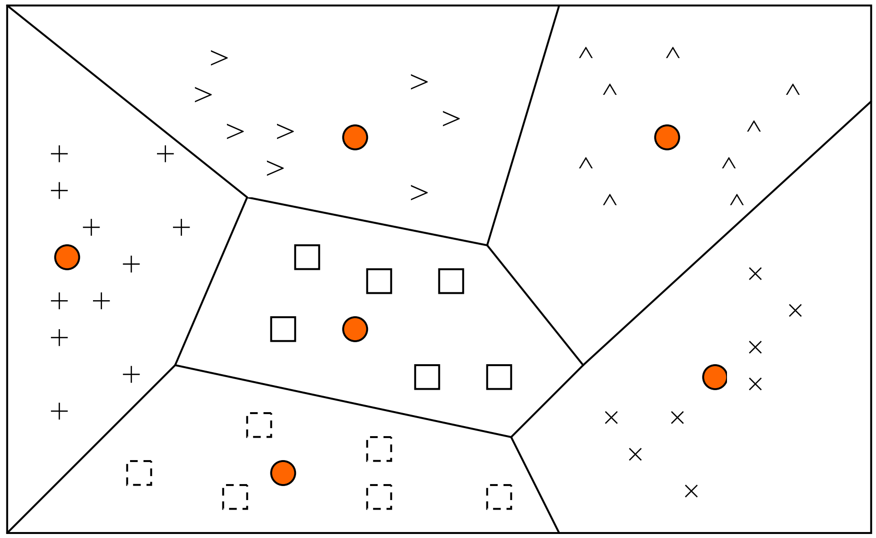

Figure 7: Cluster formation in LEACH. All nodes marked by a certain symbol belongs to the same cluster with cluster nodes marked by a colored dot

mobility via assigning changeable *primary* and *immediate* agents to each sink node. The primary agent takes care of communicating with dissemination nodes. It then sends the data to the immediate agent which in turn relays it to the sink. When a sink node starts moving out of range of its immediate agent, it acquires a new immediate agent and informs its primary agent. Similarly, the primary agent is replaced when the sink moves away from it. When we consider the criteria of section 2, we find that TTDD does not follow an energy-efficiency strategy. Its adaptability to integration with an energy-efficient scheme needs to be examined. It should also be noted that the dependence of TTDD on nodes at grid points only can lead to large energy imbalance. Also, the large communication overhead resulting from grid construction and maintenance can have a significant effect on energy consumption and network operation.

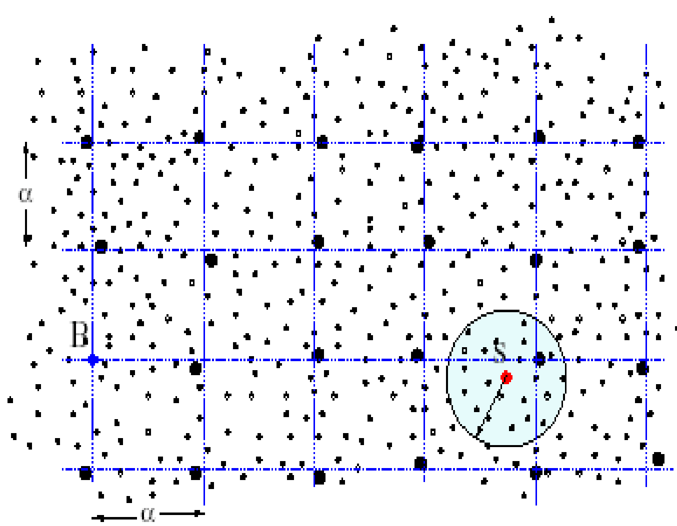

Figure 8: Grid formation in TTDD: one source B, and one sink S

5. An Experimental Comparison of Sensor Network Routing Techniques

5.1 Purpose

In this chapter, we perform an experimental comparison between routing protocols that can potentially be used in wireless sensor networks that are used in real-life applications, both civilian and military. For this purpose, we compare two of the algorithms that have been developed specifically for wireless sensor networks with two protocols that belong to the two main classes of MANET protocols. The reason behind this comparison strategy is two-fold. First, we aim at finding the best possible routing strategy that we can build on for inclusion in actual mission critical networks. Second, while we do this search we would like to examine the assertion that MANET protocols are not suitable for the operation of sensor networks due to several reasons the main of which is their heavy overhead. Since MANET protocols are well established and proven in many ad hoc network applications, we did not want to exclude them without performing some basic testing against some of their promising sensor network specific counterparts.

For this comparison, we have selected the Directed Diffusion and TTDD algorithms, which have been developed specifically for sensor networks, and AODV and OLSR, which are among some of the popular MANET protocols. The descriptions of these protocols have been already covered in Chapter 4.

5.2 Comparison Strategy

We perform our comparison experiments based on realistic scenarios that can be encountered in practical sensor network applications. This is to demonstrate the relative abilities and performance of the different algorithms under study in real life situations. For this purpose, we select a topology of specific dimensions and use randomly generated node deployment scenarios.

5.2.1 Comparison Scenarios

Our goal is to test the performance of each algorithm in situations where sensor nodes are deployed randomly in the field to collect data in a certain area of interest. Examples of this can be in areas with environmental problems such as in the case of forest fires, or in disaster areas to aid search and rescue operations. It can also be in situations such as in a battle field where enemy movements need to be detected. We simulate a heterogeneous network with two types of nodes. The first type is sensor nodes which have limited energy resources and are stationary (no movement). The second type is nodes that are more capable and have significantly more resources, and can be mobile. This is to simulate the situation of the interactions between sensor nodes that are deployed in the field, and resource-rich nodes which can be either the processing/command centers or gateways to these centers. In reality they can be mounted on tanks or battle vehicles that move around in the military field, or on the rescue vehicles that are used in the areas of natural disasters and can communicate with deployed sensors to collect data that can guide the operations. We will call this latter type of nodes “sink nodes” throughout the rest of this study.

We experiment with the following scenarios:

- Various network node populations: to test the ability of the algorithms to scale with increased network sizes
- Different sink mobility levels: to test the ability of the algorithms to cope with changing topologies
- Different numbers of sink and source (sensor nodes which detect and transmit phenomena data) nodes
- Different data rates (the data rate of sources increases with the increase in the activity of the monitored phenomena)

Throughout our simulations we will assume that all data sinks are interested in data detected by any source sensor. This means that connections need to be established for all source-sink combinations within the network. In reality, data sinks may be interested only in the information that is coming from sensors in a specific area of the network. This has to be detailed further within the scope of the SASNet architecture.

5.2.2 Metrics

We use both network operation performance metrics as well as sensor node energy performance metrics.

As far as network operation performance is concerned, we measure the following two aspects:

- Average data delivery ratio: This metric gives an indication of the ability of the algorithm to deliver the data that was detected at source sensors to data sinks. It is measured as the ratio of the number of data packets received at data sinks to the number of data packets detected at source nodes over all source-sink pairs. In our evaluations we will consider that the delivery ratio for a certain source-sink pair is zero for a certain algorithm if the algorithm was unable to enable the pair in question to establish a path and communicate.
- Average data delivery latency: This metric measures the average data delivery delay over all packets that were successfully delivered to data sinks.

As for the energy performance metrics of sensor nodes, we measure the following aspects:

- Average energy consumption: This metric measures the energy cost of a certain scenario. It is the average energy consumed calculated over all sensor nodes within the network. It gives an indication of the effect of the scenario on the lifetime of sensor nodes.
- Energy fairness: This metric is calculated as the standard deviation of remaining sensor node energies. It shows the relative utilization of sensor nodes in routing duties by the routing algorithm. This gives an indication of the effect of a certain scenario on network lifetime. The less fair the operation of a routing algorithm is, the more likely it is to cause full depletion of some critical nodes faster than others, which may lead to network partitioning.

5.2.3 Simulation Environment

We use the network simulator ns-2 [22] in our comparisons. The AODV and directed diffusion algorithms are already implemented and included in the regular ns-2 software. We use the INRIA implementation of OLSR [9]. We also use the TTDD code as implemented by the TTDD authors [17]. We run all our simulations in a simulation area of dimensions 1000 × 1000 square meters. Unless otherwise indicated in the discussion of a specific experiment, the simulations parameters default to the following values. We use a total number of network nodes of 100. We use 4 sink nodes, and 4 source nodes. Data are generated at each source node at a rate of 1 packet per second. The size of the data packet is 64 bytes. Sensor nodes are always stationary and data sink nodes are also static unless otherwise indicated. Each sensor node, including source nodes, starts the simulation with limited energy resources. Sink nodes, on the other hand, have plenty of energy resources to simulate a realistic difference between the normally resource restricted sensor nodes and the resource rich data sinks. Energy parameters are given in table 1. For TTDD, the cell size is an important parameter. Since there is no specific method in the original TTDD study to calculate it, we used a cell size of 300 meters based on taking the ratio between the simulation area size of [20] and that of our study. Each result is an average of ten simulation runs; each of which with a different random node deployment scenario. Each simulation experiment runs for 600 seconds.

Table 1: Simulation energy parameters

Initial Sensor Node Energy (J)	200
Rx Sensor Node Power Consumption (W)	0.395
Tx Sensor Node Power Consumption (W)	0.66
Idle Sensor Node Power Consumption (W)	0.035
Rx Sink Node Power Consumption (W)	1.0
Tx Sink Node Power Consumption (W)	1.4
Idle Sink Node Power Consumption (W)	0.83

5.3 Results

In this section, we present the results of each of our simulation experiments together with an explanation of the resulting trends.

5.3.1 Performance with Increasing Network Population

In this experiment, we examine the performance of the different routing algorithms when increasing the number of network nodes. In reality, it is expected that many sensor network applications will require deploying a large number of sensor nodes randomly over a certain geographical area of interest. We ran simulation experiments with the default simulation parameters as in Section 5.2.3 but with varying the number of network nodes (50, 100, 150, 200 and 250 nodes) to check the effect of increasing the network size on protocol performance. Figure 9 shows the effect on packet delivery ratio. We notice from this figure that the packet delivery ratio for AODV remains almost unchanged as the network population increases and is almost 100% for these simulation conditions. Considering directed diffusion, we find that the delivery ratio is comparable to that of

AODV at lower node numbers and starts to drop significantly at about 150 nodes. As the number of nodes increases, the number of possible paths between a source-sink pair increases which causes a significant increase in exploratory messages within the network. This in turn leads to increased collisions and packet loss. The same trend is also seen with OLSR but with a higher ratio decline than with directed diffusion. The proactive nature of the OLSR algorithm in trying to establish routes to all network destinations affects its performance with the increase of network nodes due to increased congestion and hence collisions. This causes loss in both topology information and data. As for TTDD, we find that the delivery ratio is lower than the other algorithms even at a lower number of nodes due to the fact that some source-sink connections could not be established in some node deployment scenarios hence affecting the overall average. The decline in the case of TTDD as the number of network nodes increases is also significantly steeper than the other cases. The high communication overhead involved in constructing and maintaining the grids in TTDD and the resulting congestion around some critical nodes seems to affect its ability to establish robust source-sink connections as the number of network nodes grows.

Considering packet delivery latency, we find that the AODV and TTDD algorithms perform best in this regard, see Figure 10. Nevertheless, we have to keep in mind the sharp decline of packet delivery with the increase of the number of nodes in the TTDD case. The increase in the latency in case of directed diffusion as the number of nodes increases is attributed to the increase in the retransmissions due to the relatively higher congestion with the increased routing and the associated exploratory events overhead with increased path possibilities as we mentioned earlier. In case of OLSR, retransmissions due to the congestion resulting from the topology maintenance overhead cause packet delivery delays as the number of network nodes increase.

When we consider the energy performance of sensor nodes, we find that AODV consumes the least amount of energy in all protocols under comparison, see Figure 11. The amount of consumed energy stays almost the same as the number of network nodes increases. This is due to the reactive routing strategy that it follows which is based on establishing one route per connection and only when needed. The relatively low communication overhead of AODV also helps conserve energy. The TTDD algorithm consumes less energy than directed diffusion and OLSR and performs somewhat close to AODV with small number of network nodes. This changes as the number of nodes increases with the sharp increase in protocol overhead. OLSR also sees large increase in energy consumption with the increase in network population due to the increase in proactive route maintenance overhead as well as the cost of retransmissions. Figure 12 shows how the different algorithms compare when it comes to energy fairness as the network size increases. The figure shows that the standard deviation of remaining sensor node energies, which is the measure for energy fairness, increases only slightly in case of AODV.
This means that energy imbalance increases with the increase of network nodes as the focus on specific routes causes some nodes to become more utilized relative to others within the network. In case of directed diffusion, energy imbalance between network nodes starts higher than that of AODV at smaller number of nodes. As the number of nodes increases the imbalance increases only slightly in most cases.

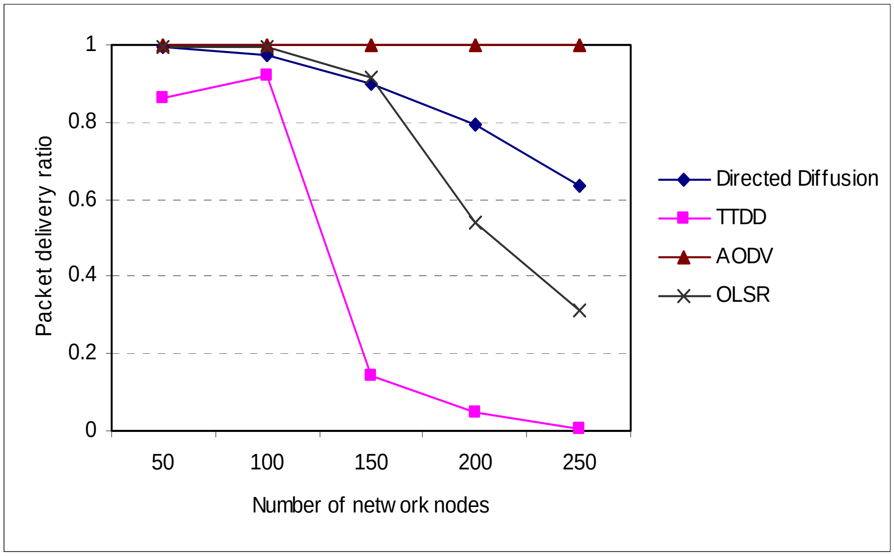

Figure 9: Effect of network population on packet delivery ratio of the different protocols

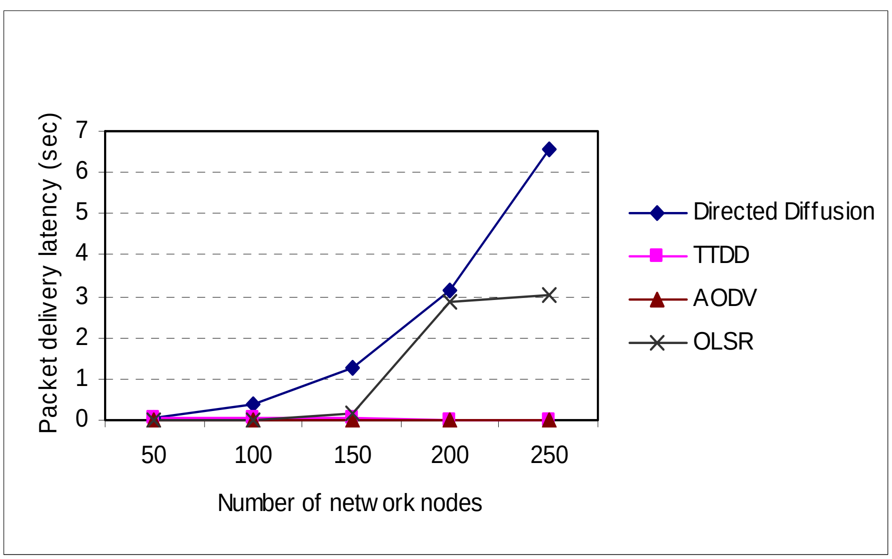

Figure 10: Effect of increasing network population on packet delivery latency

In case of TTDD, the imbalance starts at relatively low levels with smaller number of network nodes and increases sharply as the number of nodes increases due to the over utilization of dissemination nodes that perform more routing duties relative to other sensor nodes. At a number of nodes of 150, this trend is reversed and the level of imbalance starts decreasing as more nodes get more utilized through the flooding as the density increases per cell. The large drop in packet delivery at 150 nodes also contributes to this result. OLSR also follows a trend similar to that of TTDD but with lower level of increase in energy imbalance with the increase in network size. With the increase in the number of nodes beyond a certain number, the imbalance starts to decrease due to the sharp drop in data packet delivery which somewhat reduces the load on MPR nodes.

5.3.2 Performance with Sink Mobility

In this experiment, we explore the performance of the algorithms under different sink mobility levels. The conditions of this experiment can be encountered in situations such as military operations where military vehicles or soldiers subscribe to the sensor network to query network nodes for information related to enemy movements or battle field conditions. This could also be the case in rescue operations where emergency vehicles (data sinks) join the sensor network to get information from deployed sensor nodes about the conditions in a certain disaster area e.g. presence of live people who need to be rescued, etc. In our experiment, we use the default simulation parameters as described in Section 5.2.3 and vary the mobility conditions of the sinks by changing the pause time. We use pause times of 100, 200, 300, 400, 500 and 600 seconds. The sink stops for the pause time and then moves in a random direction at a speed that is uniformly distributed between 0 and 10 m/sec.

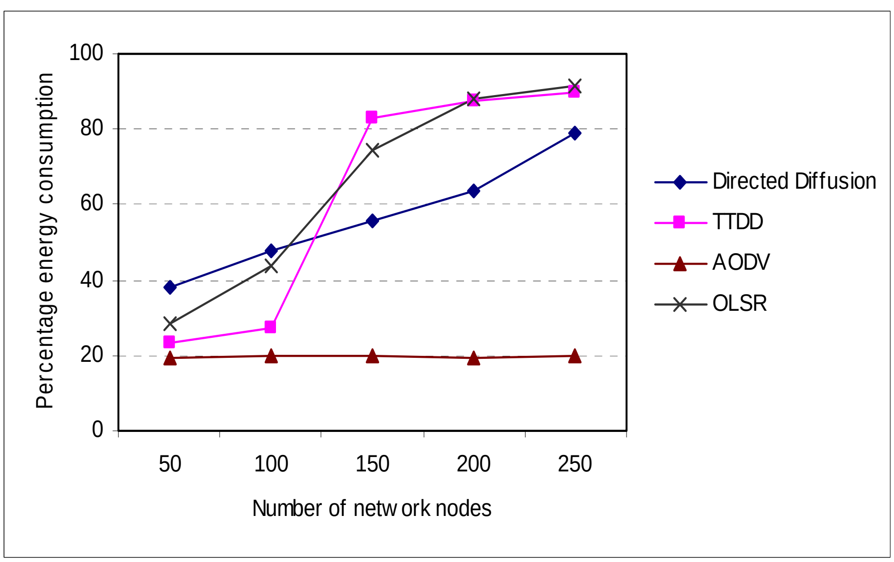

Figure 11: Effect of network size on energy consumption

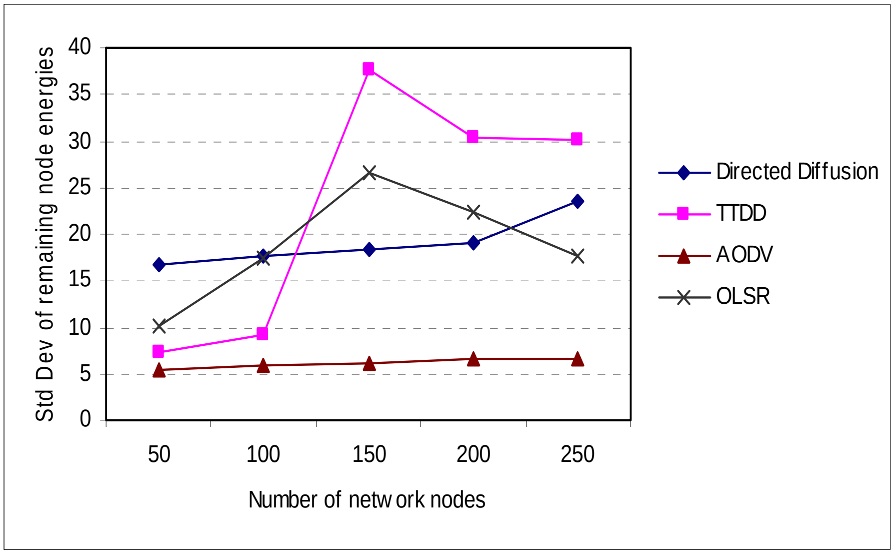

Figure 12: Effect of network size on energy fairness

Under these conditions, the packet delivery performance of the different algorithms is as shown in Figure 13. We notice from this figure that AODV consistently delivers data at a delivery rate of almost 100% regardless of the sink mobility conditions. It is followed closely by OLSR which performs comparably as far as this metric is concerned. Directed diffusion comes next in this regard followed by TTDD. They both have lower delivery ratios with higher mobility and this improves as sink mobility decreases (higher pause time). Average packet delivery latency, as shown by Figure 14, is consistently low with both AODV and OLSR which show comparable performances. TTDD shows a slightly higher latency than AODV and OLSR. Directed diffusion shows high delivery latency with high sink mobility. Path establishment between source-sink pairs seems to take longer time with mobility in directed diffusion than all other algorithms. In both the directed diffusion and TTDD cases, the latency decreases with the decrease of mobility as the routes become more stable resulting in faster packet delivery to sinks. As far as energy consumption is concerned, the behavior of the different algorithms in this experiment is shown in Figure 15. We notice from this figure that all algorithms, with the exception of TTDD, perform in a consistent manner with regard to average power consumption regardless of sink mobility conditions. AODV consumes the least amount of energy, while OLSR comes second followed closely by directed diffusion. TTDD, on the other hand, consumes comparable amount of energy to that of OLSR and directed diffusion at high mobility conditions. Its energy consumption decreases with the decrease of sink mobility due to the corresponding significant decrease of its routing overhead. Energy fairness, as shown by the standard deviation trends in Figure 16, is generally consistent regardless of mobility in the cases of directed diffusion, AODV and OLSR, with AODV being the fairest due to its relatively low routing overhead and hence moderate utilization of routing nodes. In TTDD, energy imbalance between sensor nodes is generally higher with higher sink mobility and it improves as the mobility decreases. This is attributed to the increased communication load that results from flooding that the sinks perform to establish new routes to sources in the neighborhoods where sinks move to. This increases the energy expenditure on the sensor nodes in the vicinity thus increasing the imbalance.

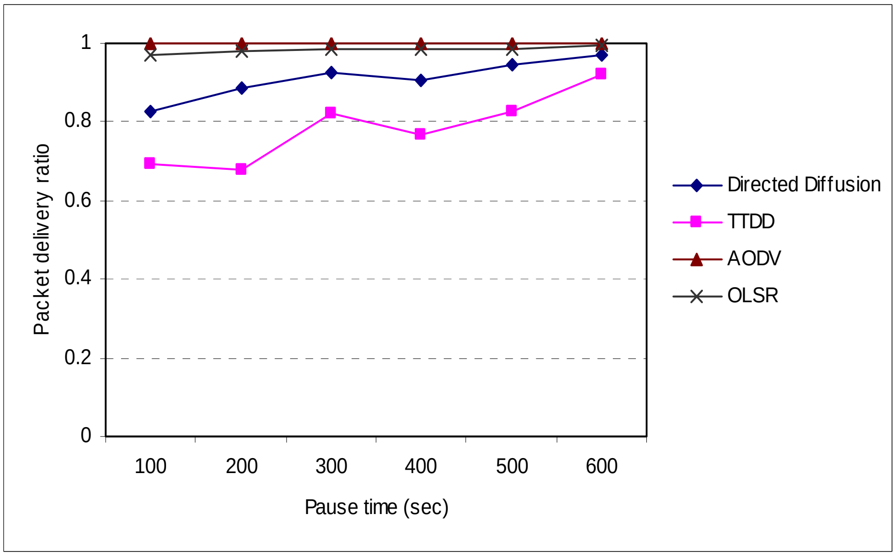

Figure 13: Effect of sink mobility on packet delivery ratio

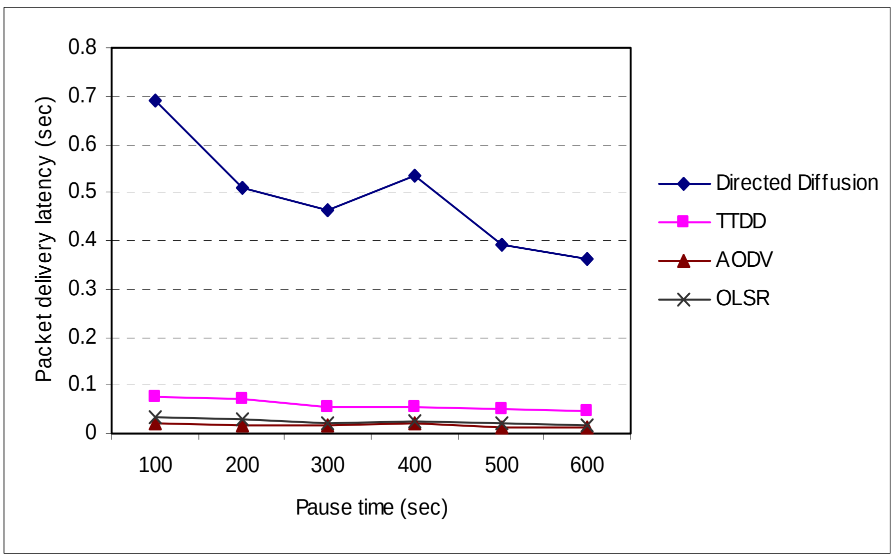

Figure 14: Effect of sink mobility on packet delivery latency

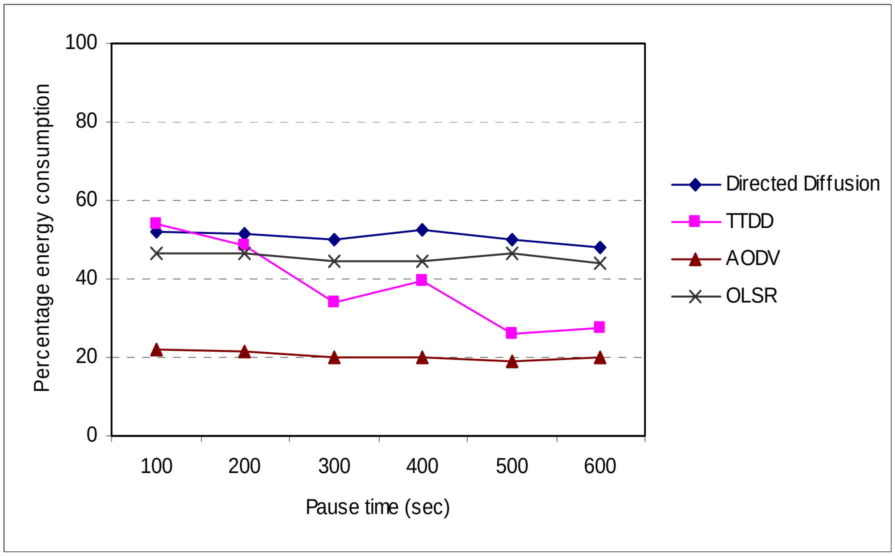

Figure 15: Effect of sink mobility on energy consumption

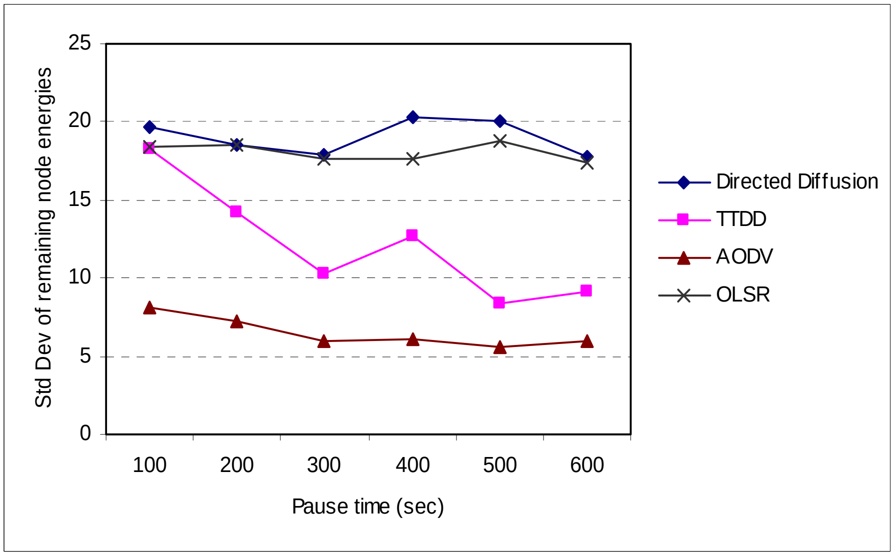

Figure 16: Effect of sink mobility on energy fairness

5.3.3 Performance with Different Numbers of Sources

In this experiment, we measure the effect of increasing the number of sources, and hence the overall data traffic, on the performance of the different algorithms. When monitoring some phenomenon, there will be times when several sensor nodes detect activities pertaining to this phenomenon at the same time. These sensor nodes will then transmit data simultaneously to interested sinks as per network configurations. It is important to investigate the effect of such an event on the performance of the different algorithms. For this purpose we keep the number of sink nodes at 4 and vary the number of sources to 1, 2, 3, 4, 5 and 6. Our goal is to establish a trend of the performance under increasing number of sources. Otherwise, the other simulation parameters are kept at default values as specified previously. Figure 17 shows the effect of changing the number of sources on the packet delivery ratio of the four algorithms. We notice from this figure that AODV and OLSR are almost unaffected by the change of the number of sources for the conditions of this experiment. Directed diffusion packet delivery ratio starts to suffer in a visible way as the number of sources reaches 5. The effect is not so severe, though. TTDD's packet delivery performance declines as the number of sources increases. This reaches high levels as the number of sources reaches 5. This is due to the increase in the grid forming and maintenance overhead with the increase of the number of sources. As for the packet delivery latency performance as shown in Figure 18, we notice that AODV, OLSR and TTDD show low values of latency whereas directed diffusion's delivery latency increases steadily and sharply with the increase of the number of sources. This could be due to the increased reliance on common nodes for different sink-source paths as the number of sources increase. This combined with the exploratory messaging overhead imposes extra delays on packet transmissions. The energy cost of the different algorithms with the increase of the number of sources is shown in Figure 19. In this figure we notice that energy consumption increases in all cases due to increased traffic. In the cases of AODV and OLSR the rate of increase is low even though the consumption in case of OLSR is much higher due to topology maintenance overhead as we explained in earlier cases. In case of TTDD the rate of increase becomes more visible at larger numbers of sources (starting 4 sources) due to the corresponding increase of protocol overhead. In the case of directed diffusion, the increase in consumption is almost linearly proportional to the increase in the number of sources and surpasses OLSR's consumption level at 4 sources. This shows that the cost of overhead in case of directed diffusion climbs steadily with the increase in the number of sources.

Energy fairness trend, as shown in Figure 20, shows a decrease in energy fairness in all protocols as the number of sources increases. The rate of increase is lowest in OLSR. This is due to the fact that it proactively searches routes for all destinations in all cases, and the increase is merely a reflection of the increase of the data transmission load on the MPR nodes. In case of other protocols, the increase of sources reflects the need of new routes and therefore requires an increase of routing overhead. This, together with the increase of data traffic, imposes an additional load on the nodes on the routes. In the case of AODV, since the overhead is moderate, the imbalance is the lowest in all algorithms. TTDD shows almost a similar trend like AODV until we reach 5 sources and then the additional overhead pushes the imbalance sharply higher. In the case of directed diffusion, the rate of increased energy imbalance is sharpest in all algorithms due to the increased overhead, and hence energy costs, in the neighborhoods of sink nodes with the increase of sources as sinks try to establish communications with these sources.

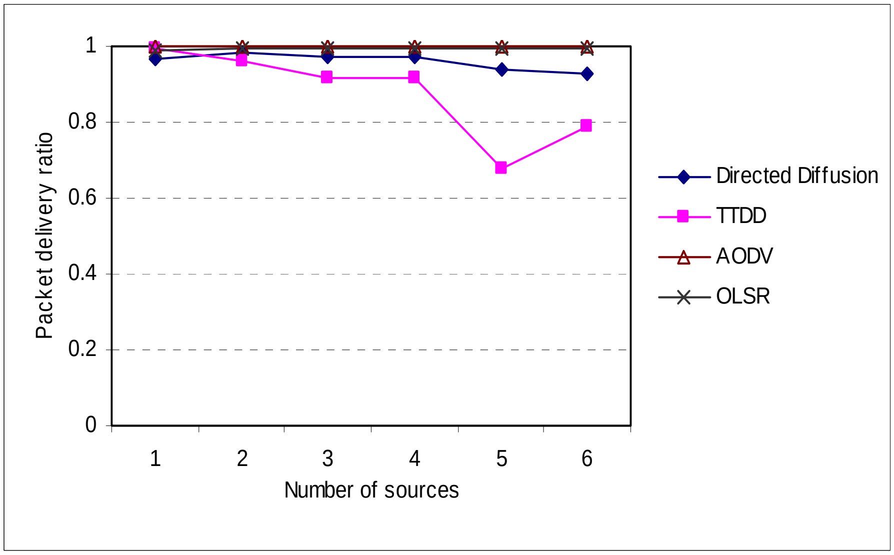

Figure 17: Effect of varying the number of sources on packet delivery ratio

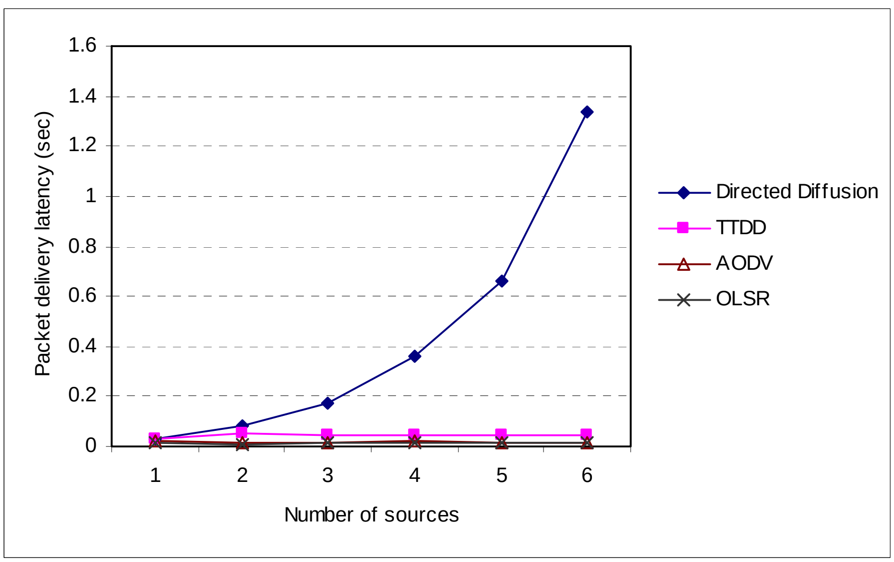

Figure 18: Effect of varying the number of sources on packet delivery latency

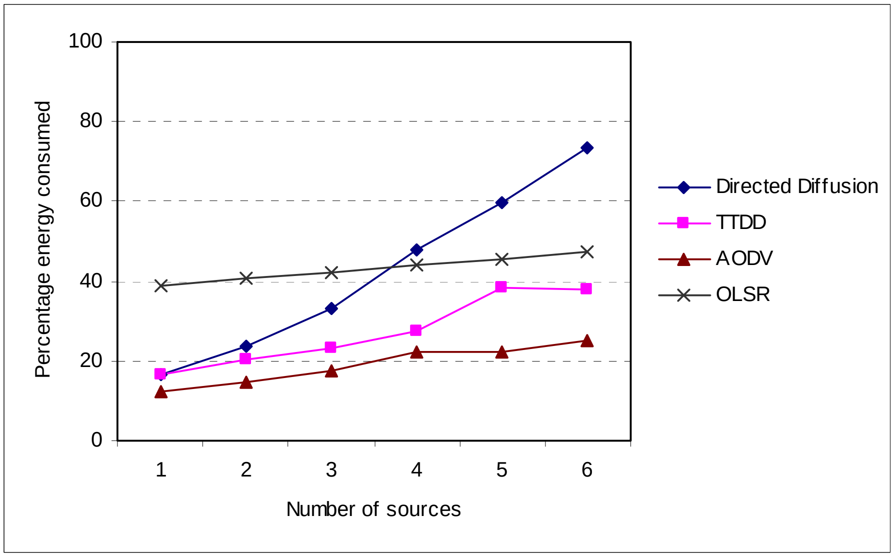

Figure 19: Effect of varying the number of sources on energy consumption

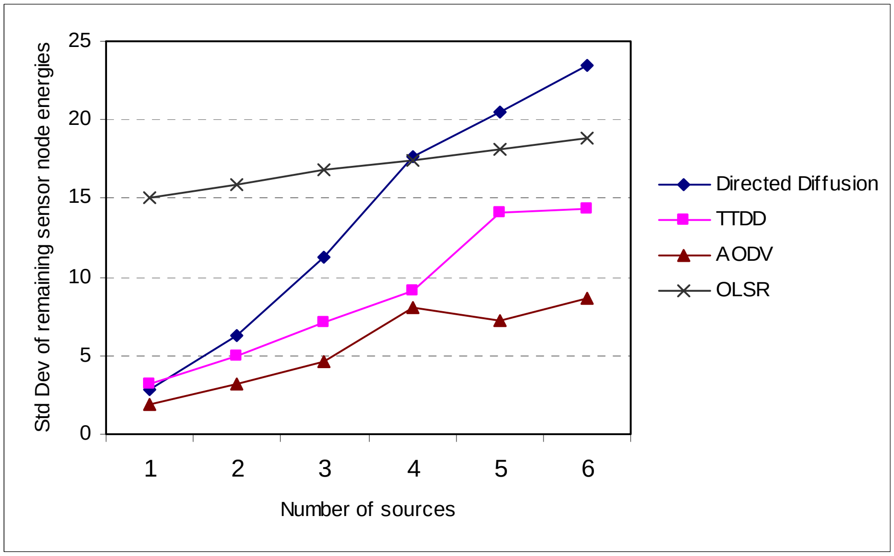

Figure 20: Effect of varying the number of sources on energy fairness

5.3.4 Performance with Different Numbers of Sinks

The number of sinks can increase in reality when the demand on a sensor network increases. Examples of this are in situations where new parties (soldiers, rescue workers, etc) subscribe to the network from different geographic locations upon the occurrence of certain events in order to obtain sensed data of specific phenomena. Therefore, we experimented with varying the number of sinks to test the effect on the performance of the algorithms. Figure 21 shows the packet delivery ratio performance of the different algorithms. We see from the figure that AODV and OLSR perform best regardless of the number of sinks. The directed diffusion performance is generally comparable even though it shows slightly less delivery ratio. TTDD's performance seems to be affected in the first place by the number of sources (4 in this experiment) and therefore it seems consistent until the number of sinks increases to 5 where it drops significantly. This is due to the increased effect of flooding around sinks on network congestion conditions. By examining the effect of sink numbers on data delivery latency we find that both AODV and OLSR show low latency trend that is consistent regardless of the number of sinks, see Figure 22. Latency is also relatively low with TTDD but is higher than AODV and OLSR. It also increases slightly as the number of sinks increase due to congestion caused by the additional flooding. Directed diffusion shows significantly higher latency that increases linearly with the increase of the number of sinks due to the increase of the overhead of exploratory messages. The effect on energy consumption is illustrated in Figure 23. We notice from this figure that the trend is quite similar to the case of varying the number of sources for similar reasons. Same can be said about energy fairness which is shown by Figure 24.

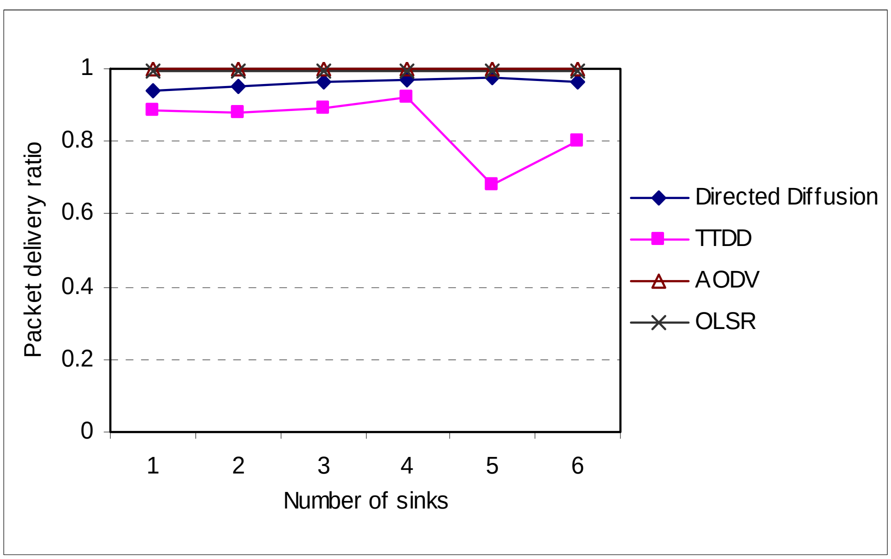

Figure 21: Effect of varying the number of sinks on packet delivery ratio

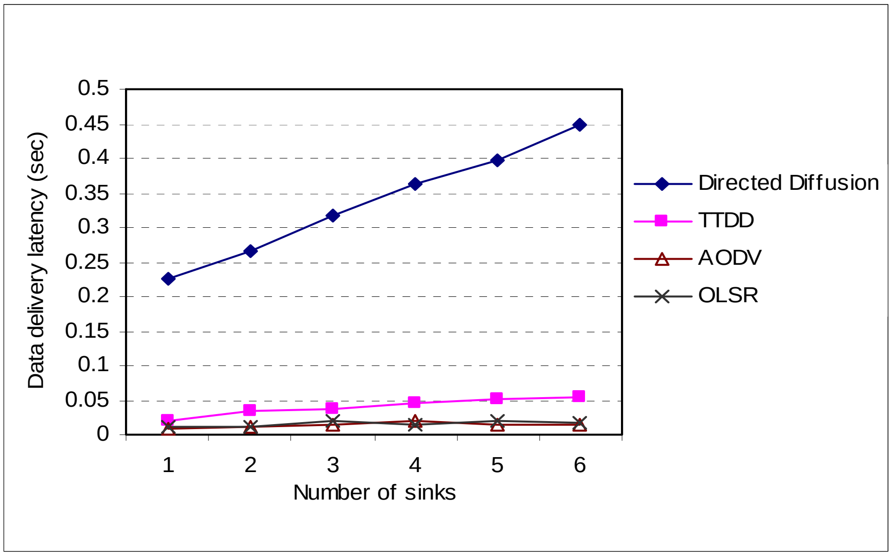

Figure 22: Effect of varying the number of sinks on packet delivery latency

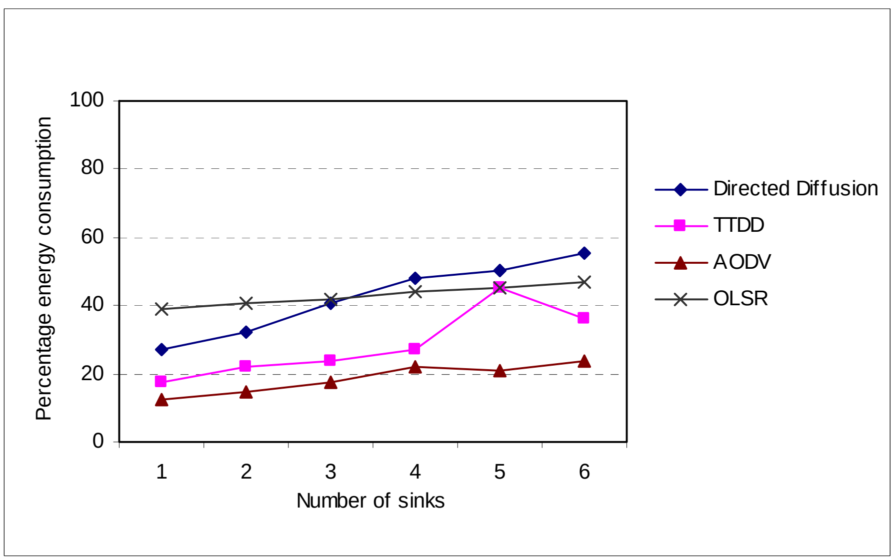

Figure 23: Effect of varying the number of sinks on energy consumption

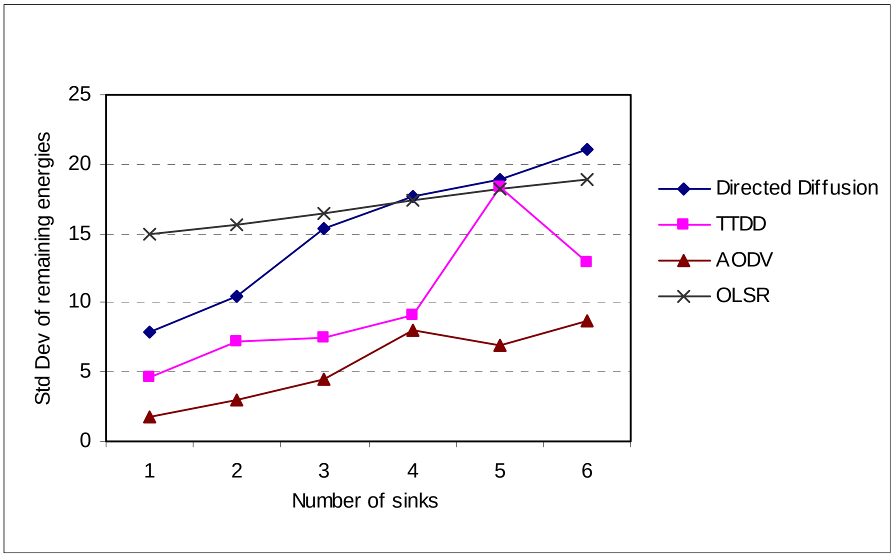

Figure 24: Effect of varying the number of sinks on energy fairness

5.3.5 Performance with Different Data Rates

Data transmission rates increase in reality when the activity of the monitored phenomena increases. This triggers sensor nodes to increase the rate of sending data to sinks in the cases where data transmission is triggered by events. In this experiment, we change the data rate for each of the sources to take the values of 1, 2, 3, 4 and 5 packets per second. The packet delivery ratio trends are given by Figure 25. From this figure we see that there is no visible effect on AODV with the increase in data transmission rate. The effect on OLSR starts to become visible at the relatively high rate of 4 packets/sec. Directed diffusion shows less delivery ratio earlier and it gets worse as the data rate increases. TTDD's delivery ratio drops more sharply than the rest of the algorithms at lower data rates. Considering packet delivery latency, we see from Figure 26 that all of AODV, OLSR and TTDD show low packet delivery latency in all the data rates that we experimented with. Directed diffusion, on the other hand, shows increased latency that is almost linear with the increase of the packet send rate. It seems that the increased data rate together with the directed diffusion exploratory message overhead affects the latency of packet delivery. The energy consumption trends, as seen in Figure 27, show that all algorithms experience an increase in energy consumption as the data rate increases. The increase is almost linear in case of AODV and OLSR, and is close to linear in case of directed diffusion. In case of TTDD, the increase is drastic as the rate increases from 1 packet per second up to 3 packets per second and then it becomes almost flat. This is due to the increased congestion with the increased send rate combined with TTDD protocol overhead which causes collisions and retransmission attempts which in turn causes additional energy waste. It then drops at 4 and 5 packets per second due to the large drop in data packet transmission rate as we discussed above. Energy fairness, as shown by Figure 28, seems to decrease (as indicated by the increase of the standard deviation of remaining energies) as the data traffic rate increases in the cases of AODV and OLSR. This is due to the increased utilization of the forwarding nodes with the increased data traffic since the routing is based on the shortest path

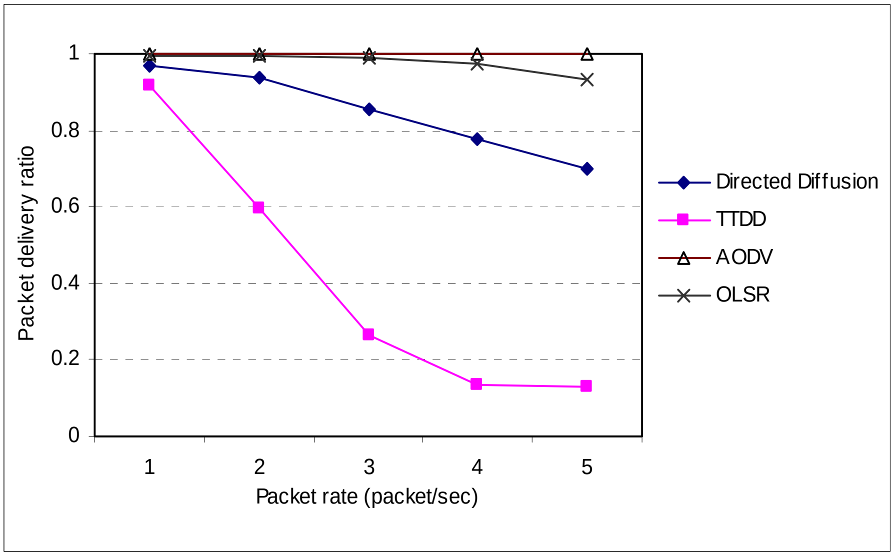

Figure 25: Effect of data rate on packet delivery ratio

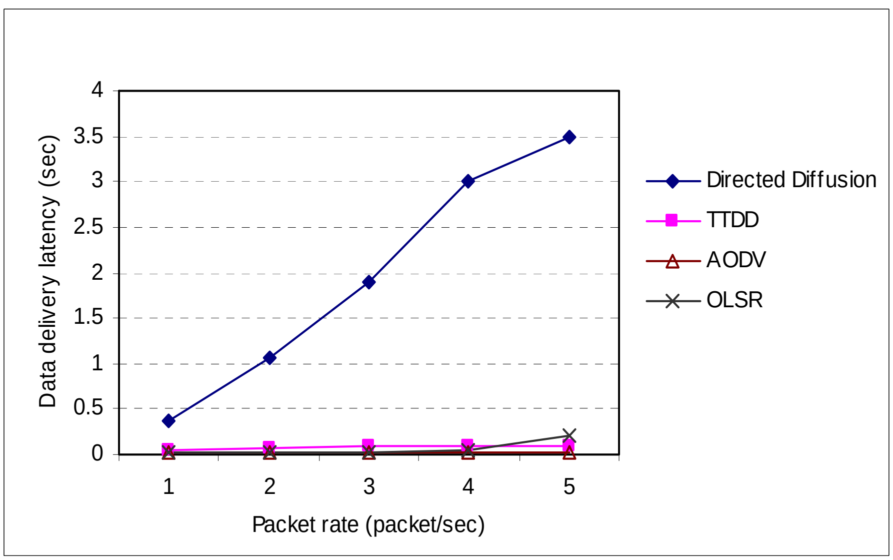

Figure 26: Effect of data rate on latency

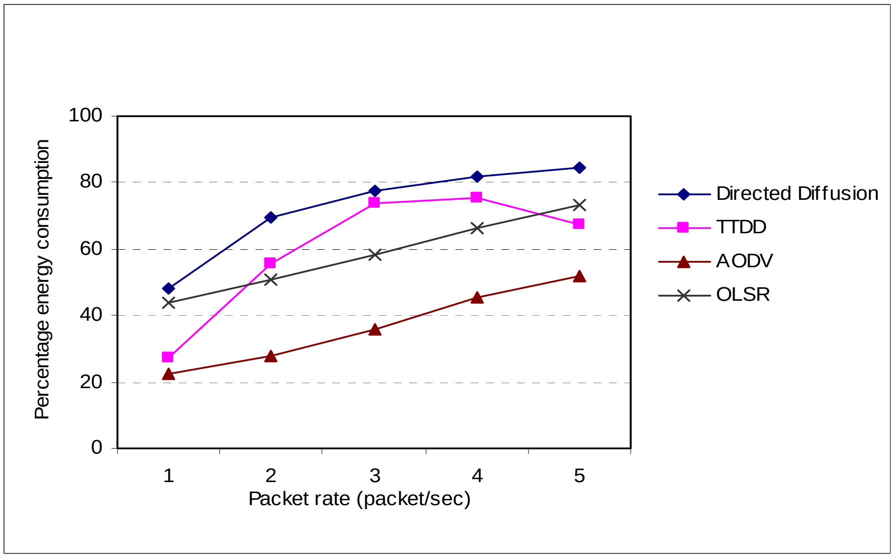

Figure 27: Effect of data rate on energy consumption

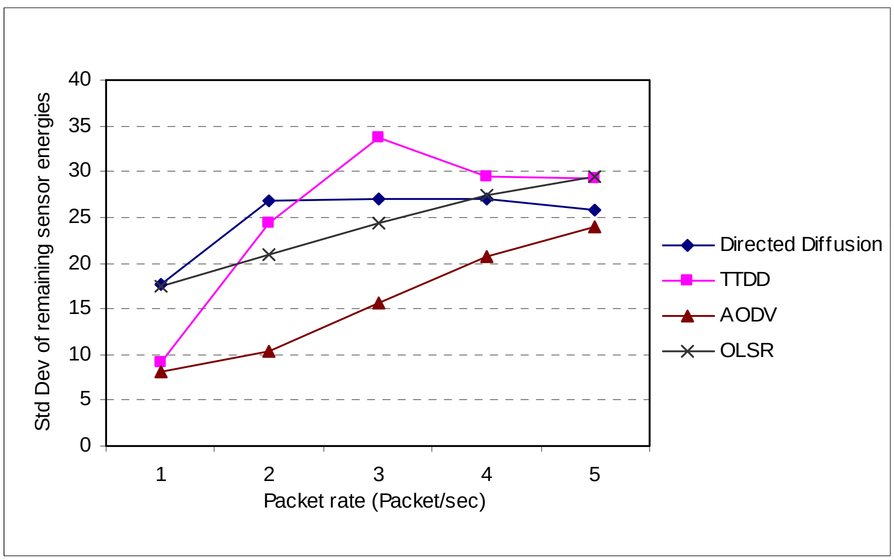

Figure 28: Effect of data rate on energy fairness

approach. This is also the case with TTDD up to a certain data traffic level where energy fairness trend becomes flat due to the drop in its ability to forward traffic. In the case of directed diffusion, since the selection of routes is based on the lowest delay, fairness decreases only up to 2 packets per second in this experiment and then the trend becomes flat as the routing paths become more diversified with the increased overall latency.

5.4 Discussion

As we mentioned earlier, our objective is to find a starting point for the research and development with regard to dissemination protocol to use within practical wireless sensor networks for military applications and others. We have conducted our experiments for this purpose and decided not to exclude any potential techniques despite some theoretical assertions against some techniques such as the MANET ones. We find from these experiments that one of the MANET protocols that we experimented with, AODV, which belongs to the on-demand or reactive family of routing protocols performs well consistently from core routing perspective. This means that the reliability of this technique is higher than others. This provides a good starting point from which we can launch investigation efforts. However, and as we have shown earlier in Chapter 4 that MANET techniques in general and AODV in particular lack some of the characteristics that are required for the operation of many of the sensor network applications. As well, the techniques that have been developed specifically for sensor networks have features such as the data-oriented operation that make them more suitable from this point of view for the operation in this type of networks. Therefore the question that has to be answered here prior to conducting further research is: do we fix the core performance issues for the sensor network protocols that have been developed for sensor networks, or rather do we enhance the features of proven MANET protocols and adapt them for operation in sensor networks?

Our assertion at this point is that extending proven well-performing MANET protocols to adapt to the requirements of sensor networks may prove more fruitful than repairing the core routing performance issues of the new techniques.

We therefore recommend performing further research on proven MANET protocols especially those that belong to the on-demand routing category such as AODV from the following main perspectives:

- Extending the protocols to handle data-oriented operation
- Investigating protocol's ability to function in heterogeneous sensor networks and deciding on the needed extensions to handle this
- Enhancing its energy-efficient capabilities
- Investigating its operation with wireless sensor network friendly addressing schemes
- Integrating the protocol with MAC layers that are possibly to be used in sensor networks such as IEEE 802.15 [24] etc.

6. Summary

The objective of this report is to initiate the research effort on data dissemination techniques for practical wireless sensor networks that can be used in military mission-critical applications.
To pave the way for this, we discussed the different aspects of wireless sensor networks as related to data dissemination within these networks. The structure and operation of sensor networks have been discussed. This discussion resulted in extracting the main features that characterize these networks. We then discussed the main system elements on which data routing depends. We discussed energy efficiency, addressing, localization and routing strategy. We also showed the relationship that ties these elements together and the overall effect on data routing within this type of networks. Based on this discussion, we listed the main requirements that are placed on the routing protocols as a result of the special nature of sensor networks.

We then classified the techniques that can be used for data routing in sensor networks into clustered and non-clustered techniques. We described the differences between the two classes. We also indicated that there are many techniques that have been developed specifically for sensor networks and span the two classes. We also discussed the potential use of some MANET techniques after adapting them for the needs of sensor networks. As examples of the two classes, we described some of the popular techniques that have been developed specifically for sensor networks as well as some popular MANET protocols that can potentially be used for sensor networks.

We performed some comparison experiments that simulate realistic sensor network situations in order to come up with an algorithm that performs best from core routing perspective. The goal is to come up with a starting point for further research, which is the main goal behind this report. We used the directed diffusion, TTDD, AODV and OLSR algorithms for our comparison. We ran 5 experiments: changing network population, changing sink nodes mobility conditions, changing number of source nodes, changing number of sink nodes, and changing data transmission rates. We found that AODV, which belongs to the on-demand MANET routing category, performs best of all the algorithms that we tested for the conditions of our experiments.

Based on our test results, we have two possible approaches for further research. The first approach is to attempt to improve the performance issues that we found with the algorithms that have been designed specifically for sensor networks. The second approach is to extend proven MANET protocols that show promising results from core routing perspective for the needs of sensor networks. The first approach can prove quite challenging since it involves potential changes to the core routing strategy of the algorithm in question. The second approach seems more promising since it involves keeping the core functionality intact and developing techniques to deal with the nature of the networks on top of this solid routing strategy.

Our recommendation for further research based on this report is to proceed with extending a robust MANET routing technique, possibly AODV, to the needs and requirements of mission-critical wireless sensor networks. Within the scope of this research, the SASNet network structure needs to be analyzed and factored into the design of the targeted routing scheme. For example, the different levels of communications within the network (e.g. among the sensor network nodes, soldiers/vehicles to sensor network, sensor network to command centers, etc) need to be studied. Based on the outcome, the relationships between the routing communications for these layers should be established. The objective would be to ensure reliable and resource-conscious end-to-end routing communications framework.

References

[1] K. Akkaya and M. Younis, “A survey on routing protocols for wireless sensor networks” in Elsevier Journal of Ad Hoc Networks, Volume 3, Issue 3, May 2005, pages 325-349.

[2] N. Bulusu, J. Heidemann and D. Estrin, “GPS-less Low Cost Outdoor Localization For Very Small Devices”, IEEE Personal Communications, Special Issue on "Smart Spaces and Environments", Vol. 7, No. 5, October 2000, pages 28-34.

[3] B. Chen, K. Jamieson, H. Balakrishnan, and Robert Morris, “Span: An Energy-Efficient Coordination Algorithm for Topology Maintenance in Ad Hoc Wireless Networks”, in Proceedings of the ACM Mobile Computing and Networking Conference, Rome, Italy, 2001, pages 85-96.

[4] A. Dunkles, J. Alonso and T. Voigt, “Making TCP/IP viable for wireless sensor networks”, In Proceedings of the First European Workshop on Wireless Sensor Networks (EWSN'04), work-in-progress session, , January 2004, Berlin, Germany.

[5] D. Estrin, R. Govindan, J. Heidemann and S. Kumar, “Next Century Challenges: Scalable Coordination in Sensor Networks”, Proceedings of the 5th annual ACM/IEEE international conference on Mobile Computing and Networking (MobiCom ’99), Seattle, WA, USA, August 1999, pages 263-269.

[6] Y. Gadallah and T. Kunz, "A protocol independent energy saving technique for mobile ad hoc networks", accepted for the special issue on Mobile and Wireless Networking, International Journal of High Performance Computing and Networking (IJHPCN), Vol 4, Issue 1, 2006.

[7] Vlado Handziski, Andreas Köpke. C. Frank and H. Karl, “Semantic Addressing for Wireless Sensor Networks”, Technical Report TKN-04-005, Telecommunications Networks Group, Technical University of Berlin, Germany, May 2004.

[8] C. Intanagonwiwat and R. Govindan and D. Estrin and J. Heidemann and F. Silva, “Directed diffusion for wireless sensor networks”, ACM/IEEE Transactions on Networking, Volume 11, Issue 1, February 2003, pages 2-16.

[9] INRIA – Project HIPERCOM. http://hipercom.inria.fr/olsr/

[10] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum and L. Viennot, “ Optimized Link State Routing protocol for Ad Hoc Networks”, IEEE INMIC, Pakistan 2001.

[11] S. PalChaudhuri, S. Du, A. K. Saha, and D. B. Johnson, “TreeCast: A Stateless Addressing and Routing Architecture for Sensor Networks”, Proceedings of the 18th International Parallel and Distributed Processing Symposium (IPDPS'04), April 2004, Santa Fe, New Mexico, USA.

[12] C. E. Perkins and E. M. Royer, “Ad-hoc On-Demand Distance Vector Routing”, Proceedings of 2nd IEEE workshop on Mobile Computing Systems and Applications, February 1999, pages 90-100.

[13] W. R. Heinzelman, A. Chandrakasan and H. Balakrishna, “Energy-Efficient Communication Protocol for Wireless Microsensor Networks”, Proceedings of the Hawaii International Conference on System Sciences, Maui, Hawaii, January 2000, pages 10-19.

[14] Chris Savarese, Jan M. Rabaey, and Jan Beutel, "Locationing in distributed ad-hoc wireless sensor networks", in Proceedings of International Conference on Acoustics, Speech and Signal Processing (ICASSP 2001).
[15] A. Savvides, C. Han, M. B. Strivastava, "Dynamic fine-grained localization in Ad-Hoc networks of sensors", in Proceedings of the ACM Mobile Computing and Networking Conference, Rome, Italy, 2001, pages 166-179.
[16] C. C. Schurgers, G. Kulkarni and M.B. Srivastava, "Distributed On-Demand Address Assignment in Wireless Sensor Networks" IEEE Transactions on Parallel and Distributed Systems, Vol.13, No: 10, October 2002 Distributed Systems, Vol.13, No: 10, October 2002
[17] UCLA Internet Lab – GRAB Project. http://irl.cs.ucla.edu/GRAB/
[18] B. Warneke, M. Last, B. Liebowitz and K. Pister, " SmartDust: Communicating with a Cubic-Millimeter Computer", IEEE computer, Vol. 34, No. 1, 2001, pages 44-51.
[19] Ya Xu, J. Heidemann and D. Estrin, "Geography-informed Energy Conversion for Ad Hoc Routing", in Proceedings of the ACM Mobile Computing and Networking Conference, Rome, Italy, July 2001, pages 70-84.
[20] F.Ye, H. Luo, J. Cheng, S. Lu and L. Zhang , "A Two-Tier Data Dissemination Model for Large-scale Wireless Sensor Networks", Proceedings of the 8th Annual International Conference on Mobile Computing and Networking (ACM MobiCom), September 2002, Atlanta, Georgia, USA, pages 148-159.
[21] R. Zheng and R. Kravets, " On-demand Power Management for Ad Hoc Networks", in Proceedings of INFOCOM, San Francisco, CA, April 2003, pages 1-11.
[22] The Network Simulator – ns-2. http://www.isi.edu/nsnam/ns/
[23] Cross Bow Sensor Product Information Guide : http://www.xbow.com/Support/Support_pdf_files/XBOW_Smart_Dust_ProductInfoGuide.pdf
[24] IEEE Standard 802.15.1, IEEE Standard for Information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs), LAN MAN Standards Committee of the IEEE Computer Society, 2002.

List of Abbreviations and Acronyms

AODV	Ad-hoc On-Demand Distance Vector
CDMA	Code division multiple access
GPS	Global Positioning System
IEEE	The Institute of Electrical and Electronics Engineers
IP	Internet Protocol
LEACH	Low-Energy Adaptive Clustering Hierarchy
MAC	Media Access Control
MANET	Mobile Ad hoc NETworks
MPR	Multi Point Relay
ns-2	network simulator version 2
OASIS	Optical Acoustic SATCOM Integrated Sensor
OLSR	Optimized Link State Routing
SASNet	Self-healing Autonomous Sensor NETwork
TDMA	Time Division Multiple Access
TTDD	Two-Tier Data Dissemination

This page intentionally left blank

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (the name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Establishment sponsoring a contractor's report, or tasking agency, are entered in section 8.) Communications Research Centre Canada 3701 Carling Ave Ottawa, Ontario	2. SECURITY CLASSIFICATION (overall security classification of the document, including special warning terms if applicable) UNCLASSIFIED

3. TITLE (the complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S,C or U) in parentheses after the title.)

Data Routing in Wireless Sensor Networks: Requirements, Design Considerations and Research Recommendations (U)

4. AUTHORS (Last name, first name, middle initial)

Gadallah, Yasser

5. DATE OF PUBLICATION (month and year of publication of document) April 2006	6a. NO. OF PAGES (total containing information. Include Annexes, Appendices, etc.) 39	6b. NO. OF REFS (total cited in document) 24

7. DESCRIPTIVE NOTES (the category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Technical Memorandum

8. SPONSORING ACTIVITY (the name of the department project office or laboratory sponsoring the research and development. Include the address.)

Defence R&D Canada - Ottawa
3701 Carling Ave.
Ottawa, Ontario

9a. PROJECT OR GRANT NO. (if appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant) N/A	9b. CONTRACT NO. (if appropriate, the applicable number under which the document was written) 12PA
10a. ORIGINATOR'S DOCUMENT NUMBER (the official document number by which the document is identified by the originating activity. This number must be unique to this document.) CRC-RP-2006-002	10b. OTHER DOCUMENT NOS. (Any other numbers which may be assigned this document either by the originator or by the sponsor) DRDC Ottawa TM 2006-134

11. DOCUMENT AVAILABILITY (any limitations on further dissemination of the document, other than those imposed by security classification)

(X) Unlimited distribution
( ) Distribution limited to defence departments and defence contractors; further distribution only as approved
( ) Distribution limited to defence departments and Canadian defence contractors; further distribution only as approved
( ) Distribution limited to government departments and agencies; further distribution only as approved
( ) Distribution limited to defence departments; further distribution only as approved
( ) Other (please specify):

12. DOCUMENT ANNOUNCEMENT (any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in 11) is possible, a wider announcement audience may be selected.)

N/A

13. ABSTRACT (a brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual).

Current military wireless sensor networks, such as Optical Acoustic SATCOM Integrated Sensor (OASIS) from Textron Systems, are composed of mini sensors that have the ability to sense phenomena from the surrounding environment and communicate the gathered data to a base unit where the information is sent via satellite to a command and control unit. These systems have limited coverage, require carefully planned deployments and have a single point of failure.

New wireless sensor networks are composed of sensors that collaborate in performing sensing tasks and improve detection and tracking performance through multiple observations, geometric diversity, extended detection range and faster response time. These sensors form an ad hoc network to deliver aggregate information from geographically diverse areas to their destinations. The sensors act as relays and can be randomly deployed, allowing for extended coverage.

Data routing in sensor networks has the main function of establishing and maintaining paths through which this data is transmitted from their sources to their destinations. In this report, we explore the design issues of data routing protocols in wireless sensor networks. Our main goal is to establish a solid starting point for research on routing protocols for military mission-critical wireless sensor networks. As such, we first discuss the characteristics of sensor networks in order to extract some requirements on the operation of routing protocols within these networks. Then, we discuss the non-routing components of the operation that have a direct impact on the routing function. We provide a brief description of these elements as well as establish the link between them in order to extract a list of the required features of the routing component. We then describe some of the routing algorithms that have either been developed specifically for wireless sensor networks or belong to the mobile ad hoc networks, MANET, family (the parent class of wireless sensor networks) and have good performance characteristics. Finally we conduct an experimental comparison study between four routing protocols, two of which were designed for wireless sensor networks and the other two belong to the MANET protocol family. Our experiments reveal that an on-demand MANET protocol outperforms the other protocols from core routing perspective. We therefore make our recommendations for future research which include extending the resulting best protocol to comply with the requirements that we established in this study.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus. e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus-identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Wireless Sensor Networks, Routing, MANET

Defence R&D Canada

Canada's leader in Defence
and National Security
Science and Technology

R & D pour la défense Canada

Chef de file au Canada en matière
de science et de technologie pour
la défense et la sécurité nationale

DEFENCE DÉFENSE

www.drdc-rddc.gc.ca