Paper

Theoretical and practical aspects of military wireless sensor networks

Michael Winkler, Klaus-Dieter Tuchs, Kester Hughes, and Graeme Barclay

Abstract—Wireless sensor networks can be used by the military for a number of purposes such as monitoring militant activity in remote areas and force protection. Being equipped with appropriate sensors these networks can enable detection of enemy movement, identification of enemy force and analysis of their movement and progress. The focus of this article is on the military requirements for flexible wireless sensor networks. Based on the main networking characteristics and military use-cases, insight into specific military requirements is given in order to facilitate the reader's understanding of the operation of these networks in the near to medium term (within the next three to eight years). The article structures the evolution of military sensor networking devices by identifying three generations of sensors along with their capabilities. Existing developer solutions are presented and an overview of some existing tailored products for the military environment is given. The article concludes with an analysis of outstanding engineering and scientific challenges in order to achieve fully flexible, security proved, ad hoc, self-organizing and scalable military sensor networks.

Keywords— wireless sensor networks, military sensor applications, joint intelligence surveillance reconnaissance (JISR), military sensors, energy efficient routing, WSN generations.

1. Introduction

There have been large amounts of research undertaken during the past decade in the areas of ad hoc networking and wireless sensor networks (WSNs) and significant progress has been achieved. Possible civilian use-cases for such networks include industrial plant monitoring and environmental monitoring. However, one area commonly cited as a primary use of sensor networks is for military benefit. Frequently, assumptions are stated regarding the requirements for military networks to motivate the work. The aim of this paper is to explore the military requirements of wireless sensor networks in the near to medium term (three to eight years) and to identify areas of research which would improve military usability.

2. The main characteristics of a sensor network

Wireless ad hoc sensor networks generally consist of a variable number of stationary sensors (also known as nodes) spread across a geographical area. The capabilities of these nodes typically comprise monitoring the environment and capturing specific information; the transmission of collected (and possibly preprocessed) data; as well as the forwarding of data obtained from neighbor nodes using wireless bearers[1]. A typical network structure is shown in Fig. 1.

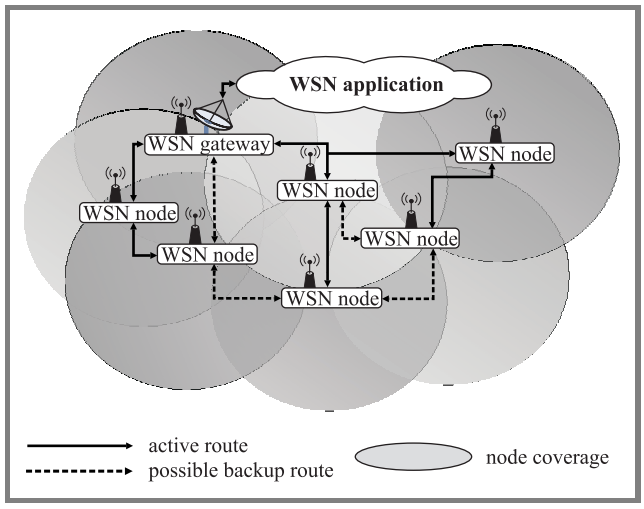

Fig. 1. Network set-up of a typical wireless ad hoc sensor network.

The information flow in a wireless sensor network will in general be from the sensor nodes to one or more wireless sensor network gateways. The network gateways can serve as data fusion points and provide reach-back capability. The reach-back capability can be based on different approaches such as:

- near real time connection, e.g., via longer range wireless transmissions (high frequency) or via a satellite link;
- asynchronous data transfer to passing unmanned aerial vehicles (UAVs).

Data processing can generally occur in three areas of the sensor network as shown in Fig. 2.
Processing can be carried out on the sensor node itself (such as the removal of unwanted signals from a target signal). Processing at the node reduces the amount of data to be passed over the network. This ensures that data loadings can be kept within the capacity capabilities of the radio system. In general, power consumption for the transmission of data is greater than the power consumption required to

[1]It is worth noting that by appropriately equipping sensor nodes with active capabilities, the network can operate actively as well as passively. The Defense Advanced Research Projects Agency (DARPA) Wolfpack concept of small, low-cost distributed jammers exemplifies an active network [1].

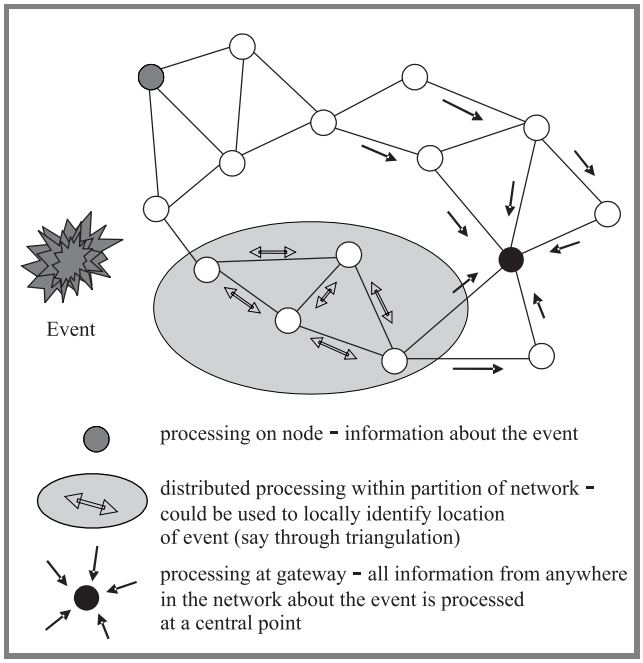

Fig. 2. Processing within a sensor network.

perform the same amount of processing data, thus there are power efficiency benefits in processing the data at source. Data processing can also be used to alleviate the amount of processing to be carried out at any gateways in the system. However, some data processing depends on data coming from multiple sources and therefore processing at source is not always possible.

Data processing can also be distributed within the network. This can be especially useful in large networks as it not only alleviates the amount of processing at the gateway but dramatically reduces the data loading which sensor nodes have to relay across the network. Hierarchical topologies lend themselves easily to perform distributed processing at "head" or "cluster" nodes (i.e., those nodes which logically "manage" other nodes in the hierarchy). However, there is an overhead associated with distributed processing. Either extra routing overhead is required to be able to pass data to be processed to specified nodes, or flooding techniques must be employed. Flooding techniques will forward user data to all or a limited subgroup of nodes thus negating the need for routing overhead traffic. These techniques allow unprocessed data to be exchanged between nodes adjacent to an "event" so that they can each do the processing required to locate the event. Then only the processed information is passed back to the gateway.

Finally, data can be processed at the gateway node(s). This allows the gateway to minimize the data it will send over the reach-back channel. Processing at the gateway thus will enable less power to be consumed in reach-back transmissions thus increasing the gateway's longevity and subsequently the lifetime of the whole network (as the gateway node is frequently the first node to fail due to depletion of its power source).

3. Military requirements

One of the main drivers for investigating wireless sensor networks is their use in military applications. The military use-cases for wireless sensor networks are diverse. They encompass applications such as:

– monitoring militant activity in remote areas of specific interest (e.g., key roads, villages);

– force protection (e.g., ensuring that buildings which have been cleared remain clear from infiltration by an adversary).

One prominent use-case which has received a great deal of interest from military personnel recently is base protection (or force protection in general). A possible set-up is depicted in Fig. 3.

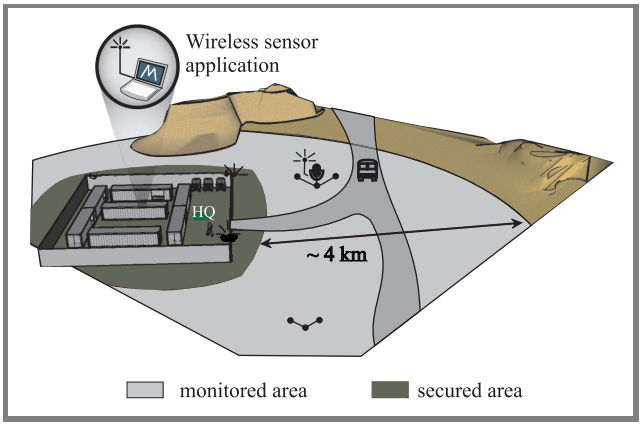

Fig. 3. Wireless sensors in support of base protection (e.g., making use of acoustic as well as electro-optical sensors).

Having deployed a headquarters in an area of active engagement it is essential to prevent the base from being attacked. The surrounding terrain may be undulating or mountainous and potentially could be obscured in trees and vegetation. Attack could come in the form of militant groups on foot or with motor vehicles.
In order to facilitate an early detection, the perimeter protection in Fig. 3 would cover a belt around the camp of up to 4 km, while in practice ranges of up to 10 km might be a requirement. Detection may be needed throughout the whole of this range whilst identification may only be required within a belt of around one to 1–2 km around the base.

3.1. Typical assumptions in the research community

Military applications are a primary use of wireless sensor networking and are best served by informed research that avoids making assumptions that are based on presumed military requirements. Many research papers propose algorithms for network sizes of thousands of sensor nodes and above. It is assumed that sensor nodes will be extremely small, lightweight and cheap. These are combined with

the need for long battery lifetime. These assumptions have led to the following requirements:

– tailored routing and transport protocols are needed;

– short distances between nodes (often just a few metres) are taken for granted;

– special-purpose operating systems are required.

In practice these assumptions are more challenging than required in the near-term for current military needs while other aspects such as tamper-resistance are not sufficiently addressed. The following section gives an insight into current requirements for sensor networks in the military environment.

3.2. Realistic assumptions for military usage

In order to facilitate a meaningful operation of wireless sensor networks for military purposes in the near to medium term, there are a number of requirements which the military expect to be met.

Physical attributes of sensors. It is likely that the sensor nodes themselves could be hand deployed in advance of an operation. They could be transported to the area of deployment by vehicle. Thus the physical size and weight of the sensor need not be a major constraint. Sensor nodes the size of a matchbox, although desirable, are not currently expected and a sensor node (without including antenna) of order 20–30 cm in height would be acceptable. In occasional instances sensor nodes may be air dropped or deployed through a rocket launcher and would need to be suitably ruggedized.

Self-configuration after deployment. Sensor nodes must be able to rapidly identify neighbours within communications range and configure themselves into an ad hoc network. The network is likely to remain reasonably static as sensor nodes are unlikely to be moved during operation. The network should be able to cope with a node failing and reconfiguration of the network should occur without manual intervention.

Network size. For the majority of operations the area to be covered by the network may be between 5–20 km^2. Generally a communications range between nodes of around 250–500 m would be acceptable. This would amount to networks with less than 100 nodes being required. In occasional cases communication ranges of greater than 1 km would be desirable.

Information flows. Initially one-way communications can be seen as sufficient, i.e., from the sensor network to the WSN gateway and beyond. This is sufficient to achieve improved situational awareness for the warfighter as well as for the commander. In the medium term some degree of control within the network will be beneficial, e.g., the ability to orient cameras. This would however necessitate the need for communications in both directions. This need for two way communications should be reflected in the network security concept in order to avoid information leakage between a stub sensor network and the core military network to which it is attached.

Duration of usage. Some networks are only required to operate for periods of days, although generally periods of one to two months can be seen as a reasonable for military sensor networks. In the base protection example (Fig. 3) an exchange of batteries is practical and could extend the lifetime further. In some instances the network may not require to be functional throughout the whole day (perhaps only needed at night) or transmission of data from the WSN gateways may only be needed two or three times a day.

Physically and electronically inconspicuous operation. It would be beneficial if the nodes were covert in appearance with a small electromagnetic emission pattern so as to remain hidden from potential adversaries.

Data type. Even limited amounts of text ($<$ 30 bytes) can help to ensure information superiority by identifying an incident and providing location reports. This means data transmission rates do not need to be high. However, military commanders are likely to request imagery and video (both real-time and non-real time) in the future.

Data reliability. In many cases it is vital to ensure that data has been received by the end-user successfully, and techniques to guarantee delivery should be included. Also data should be received in a secure manner without the opportunity for interception and tampering by any eavesdropper.

Denial of service. Any network should be able to react against a denial of service attack by an adversary, at least by providing the means to report the incident of an attack such as jamming.

Tamper-proof. The data held on the node along with any crypto material must not be available to any third party even if the node itself is captured. The sensor nodes should have anti-tamper mechanisms in-built to address this.

Costs. As relevant information can be gained by the use of networks with just a few tens of sensors, and the retrieval of sensors after use might be desirable (e.g., for security reasons), the price for a single node is generally not as critical as in the "civil Bluetooth-focussed market".

4. Current technologies

4.1. Generations of sensor products

In a similar fashion to the evolution of mobile cellular technologies, it is possible to describe the evolution of military sensor devices in terms of generations.

First generation sensor networks (1GSN). Sensor networks consist of individual sensor devices. Deployment is via manual emplacement. The network is fully preconfigured. Access to information is via manual retrieval of the device itself, or long-range point-to-point communication links.

Second generation sensor networks (2GSN). Sensors work in collaboration to cover an area. The network is typically a hub and spoke formation with a small number of sensors (typically 3 or 4) communicating with a control node equipped with a reach-back link. They are typically manually deployed, relying heavily on preconfiguration.

Third generation sensor networks (3GSN). The latest generation of sensors encompasses self-organising, flexible and scalable networks. Sensors communicate with one another for two purposes, communications services (e.g., automatic relaying of messages to a network gateway) and in-network processing (data aggregation and data fusion). Sensor networks can contain many tens or even hundreds of nodes. Deployment can be hand-emplaced or remotely air-dropped. The sensors are able to establish and – if required – publish and make use of their own geographic location, e.g., based on global positioning system (GPS).

4.2. Fully integrated solutions

Companies such as SenTech, Textron and Lockheed Martin have systems with a variety of sensors (including seismic, acoustic, infrared) which transfer their data directly to a ground station over a number of long-range non-line of sight bearers (including satcom, very high frequency and high frequency bearers). These generally fit into the 1GSN category of networks where each node is equipped with its own backhaul system.

There is a number of 2GSN systems becoming available such as the Terrain Commander and Future Combat System from Textron Systems, or the Falcon Watch System from Harris which will provide processed information from a number of sensors (including acoustic, seismic, magnetic, electro-optical and passive infrared). However, in general, there are very few of the 2GSN systems on the market. Neither, the 1GSN or 2GSN systems are truly ad hoc multi-hop in nature requiring either a direct link back to a remote ground station or a direct link back to a gateway node. There are a few 3GSN ad hoc systems advertised although many of these appear to be immature and still at proof-of-concept stage.

The majority of the systems are aimed at military use (as well as industrial plant monitoring) and many of them cite perimeter protection as their main function (for both military assets and civilian assets such as airstrips).

4.3. Wireless sensor network components

Flexible ad hoc sensor networking needs to be supported by tailored network components such as the sensors themselves and special-purpose routing protocols. Significant scientific and engineering effort has been spent on some of these components which is reflected in the following.

Routing protocols should enable self-configuration after network deployment. They have influence on traffic latency (as some routing protocols will find routes at set-up whilst others require a route to be found prior to each transmission of user traffic), on networking overhead, on energy efficiency, on the speed of network recovery in case of failures, on traffic assurance. Three main classes of routing protocols for energy-efficient wireless sensor networks have been identified [2–4]:

- **Hierarchical/node-centric**. Most routing protocols follow this approach. These protocols aim at clustering the nodes so that "cluster heads" can perform some aggregation. This reduces the amount of data to be transmitted and saves energy. The scalability of these protocols is very good. However, their routing tables may take time to converge (i.e., choose the most appropriate route) if frequent network topology changes occur (which can happen if nodes can transition into suspend mode to conserve energy).
- **Location based/position-centric**. This routing class is based on the exact (GPS) or relative (triangulation, analysis of neighbor dependencies) position of the single nodes. The distance between sensor nodes can be used to estimate the required transmission power which facilitates energy efficient routing.
- **Data-centric**. In the data-centric approach the sensor network is seen from the application point of view as a pool of data. The interface to the network will forward a query and the network will return the data to satisfy the query condition. The routing is driven by the query of the application, not on the identity of the involved nodes or sensors. The underlying implementation of the routing protocol might still be hierarchical/node-centric, and it may only be the interface available to the user that is data-centric.

Other classification of routing protocols for wireless sensor networks can characterize the network by their ability to make use of multipath transmissions, to aggregate data and to eliminate redundant information:

- **Multipath**. The main reason for transmissions via several paths is to provide tolerance to faults in the network. The protocols address the fact that they take advantage of more than one route to the gateway. Mechanisms must be integrated to ensure that only limited (or ideally no) redundant information will be produced.
- **Data processing**. Data processing can be performed at different places in the network as discussed in the context of Fig. 2. Intelligent data aggregation allows the network to operate in an energy efficient manner as less data needs to flow over the network.
- **Negotiation based**. High level data descriptors can be used to eliminate redundant information through negotiation. The nodes will send negotiation messages to prevent or suppress the exchange of duplicated or unwanted information. It is important to ensure that the level of negotiation overhead is limited.

A selection of routing protocols for wireless sensor networks which are subdivided into classes and associated

Table 1
Routing protocols with associated characteristics

Routing protocol	Node-centric	Position-centric	Data-centric	Multipath	Data processing	Negotiation based
LEACH [5]	✓				✓	✓
PEGASIS [6]	✓				✓	
Tiny-AODV [7]	✓				✓	
MECN [8]		✓				
Geographic adaptive fidelity [9]		✓			✓	
GEAR [10]		✓				
SPIN [11]			✓	✓	✓	✓
Directed diffusion [12]			✓	✓	✓	✓
Rumor routing [13]			✓		✓	
Gradient-based routing [14]			✓		✓	
COUGAR [15]			✓		✓	

with the above-mentioned characteristics is shown in Table 1. The presented protocols are just a sample of the protocols discussed in literature. The usage of these protocols in available products is however still rare and generally non-specialized protocols such as optimized link state routing (OSLR) are used as these protocols are more mature.

In the future, disruption tolerant networking (DTN) techniques [16, 17] may receive further attention. These help to provide end-to-end communications in networks with large delays and/or frequent interruptions. Also the connection of the sensor network through the network gateways to the end application might profit from this approach – especially if this reach-back capability is not always present as in the case of the UAV relay.

Medium access control (MAC). The medium access control scheme defines how multiple radios will access the medium and is used to avoid collisions should two or more radios wish to transmit simultaneously. The MAC scheme has an influence on the efficiency of a distributed sensor network in three ways: throughput, delay and energy. Throughput can suffer due to collisions when two or more nodes transmit information at the same time. This wastes energy as well as introducing longer periods of idle listening. Within the range of specialized MAC protocols for wireless sensor networks, two generic types can be identified [18]:

- **Scheduled protocols**. These are time division multiple access (TDMA) based protocols mostly used in combination with hierarchical/node centric routing protocols as cluster heads are needed for synchronization purposes.
- **Contention protocols**. Carrier sense multiple access (CSMA) is an important part of the contention based protocols. Modifications of the MAC scheme of the Institute of Electrical and Electronic Engineers (IEEE) 802.11 family addressing frequency changes as well as protocol optimizations can be found.

Within existing wireless sensor products and developer kits the use of "Commercial off the Shelf" (COTS) protocols stemming from wireless local area network (WLAN), Bluetooth or Zigbee are common, and mature implementations of specialized MAC protocols are rare.

Transmission technologies. Based on an analysis of military use-cases it becomes apparent that low data rates of just a few kilobits per second can often be sufficient while transmission ranges of a few tens of metres or better a few hundreds of metres are desirable. Sufficient coverage can then be achieved based on multi-hopping (allowing intermediate nodes to relay data). This hopping concept has the additional positive effect, that the output power can be reduced facilitating a low probability of detection and interception.

In case of other signals being transmitted within the same frequency band – be it due to other users or to jamming – the transmission technology should provide some robustness against narrowband interference. Combined with the desire to achieve inconspicuous operation, the following transmission technologies can subsequently be seen as prominent for use in military wireless sensor networks:

- direct sequence spread spectrum (DS-SS),
- frequency hopping spread spectrum (FH-SS),
- pulsed ultra-wideband (UWB).

In many prototype networks, COTS chipsets are being used providing transmission based on:

- Bluetooth (FH-SS),
- ZigBee (IEEE 802.15.4/WPAN, DS-SS) or
- WLAN (IEEE 802.11b using DS-SS as well).

Table 2

Developer platforms and their operating systems (updated and expanded from [22])

Platform	MCU	RAM [KB]	Program memory [KB]	Nonvolatile data memory [KB]	Radio chip	Tiny OS	Tiny OS V2	Mantis OS	SOS
BTnode3	ATMega128	64	128	180	CC1000 ZV4002 Bluet.	✓	✓		
Cricket	ATMega128	4	128	512	CC1000	✓			
imote	ARM 7	64	512	0	ZV4002 Bluet.	✓			
imote2	Intel PXA271	256	$32 \cdot 10^8$	0	CC2420	✓	✓		
MANTIS nymph	ATMega 128	4	128	64	CC1000			✓	
mica	ATMega 128	4	128	512	TR1000	✓			
mica2	ATMega 128	4	128	512	CC1000	✓	✓	✓	✓
mica2Dot	ATMega 128	4	128	512	CC1000	✓	✓	✓	
micaz	ATMega 128	4	128	512	CC2420	✓	✓	✓	✓
rene2	ATMega 163	1	8	32	TR1000	✓			
TelosA	TI MSP430	2	60	512	CC2420	✓			
TelosB	TI MSP430	10	48	1000	CC2420	✓	✓	✓	
Tmote Sky	TI MSP430	10	48	1000	CC2420	✓			
tinynode	TI MSP430	10	48	512	XE1205	✓			✓
XYZ	ARM 7	32	256	256	CC2420				✓

However, while remaining within the legal power limits for the respective frequency bands, the transmission ranges are not generally sufficient with WLAN achieving only distances of around 200 metres in practice[2].

Sensor types. A wide range of different sensor types which are usable for wireless sensor applications are available on the market:

– acoustic sensors,

– seismic sensors,

– magnetic sensors,

– infrared sensors,

– electro-optical sensors (closed circuit TV, etc.),

– electromagnetic sensors.

Significant effort is necessary for proper integration into larger-scale sensor networks, and one of the greatest challenges is improving sensor accuracy to keep the false alarm rate to a minimum. The need for a reliable detection of critical incidents has led to the use of **multi-modal sensors**. The intelligent combination of sensors and their joint accuracy are essential for future robust sensor applications. Furthermore, multi-modal sensors can minimize the power consumption as well as the generated traffic, e.g., if a video camera is enabled by an acoustic sensor or an infrared sensor.

Security. There are a number of security solutions to the issues inherent in a wireless sensor network. A wireless sensor network is like any other data exchange network with generic vulnerabilities and associated solutions including:

- **Eavesdropping**. The potential for an enemy to intercept and decode messages passed between devices in the sensor network. Protection is possible using available civil crypto to prevent successful eavesdropping in a sensor network, particularly as the information is generally of only short-term utility.

- **Spoofing**. The potential for a (non-legitimate) node to pass itself off as a legitimate network node and thereby subvert network exchanges. Current cryptographic authentication mechanisms are available which would be appropriate for wireless sensor networks.

- **Message integrity**. The ability of messages to be passed between nodes unchanged or unmodified enroute. Cryptographic protection and strong integrity checks (e.g., secure hash) are available now and provide robust protection against message tampering and replay attacks.

[2]Dependent on terrain and other environmental factors and with an omni-directional antenna.

- **Denial of service**. Preventing nodes in the network from being able to access and use the radio network to pass messages. Low-cost transceivers currently do not have robust anti-jam capabilities making sensor networks susceptible to this type of attack.

- **Geolocation**. The ability to locate the geographical position of nodes in the sensor network by detecting and receiving emissions from the devices. Reducing transmissions to an absolute minimum both in duration and number reduces the chance that an adversary will detect or locate a sensor network. This optimization can be included in the protocol choice and design. However, there will always be the danger that an adversary will detect transmissions, particularly if they suspect that an area contains a sensor network.

- **Physical compromise**. The ability of an enemy to extract useful intelligence and information out of a sensor node that has been located and captured. It is likely physical compromise can be addressed through simple anti-tamper mechanisms, e.g., microswitches, and fill-purge mechanisms to purge system memory of sensitive data. These are tried and tested approaches to physical resilience.

4.4. Developer kits

A number of developer solutions ("developer kits") which include sensor platforms, operating systems and transmission technologies are currently available. These are useful for research purposes as well as to foster the development of versatile sensor network applications. Table 2 shows a summarized overview of existing platforms including some of their technical parameters.

5. Research opportunities

5.1. Engineering challenges

Current wireless sensor networks can make use of multiple years of research on ad hoc networking, energy-efficient routing and related areas. Consequently, the use-cases illustrated in this paper can be met to a greater or lesser extent by existing technologies. The key challenges to deploying military wireless sensor networks are more practical engineering problems than fundamental research issues as listed below:

– clear identification of several simultaneous events, and a reliable correlation of information from neighboring nodes;

– classification of objects and events in addition to their pure detection; an automatic identification and classification of objects and events would support a quick and appropriate reaction and would hence improve the use for military purposes;

– improved integration of different types of sensors (multi-modal sensors) for enhanced information reliability; as many events have a number of simultaneous effects such as creating not only noise but also emitting electromagnetic waves, combining sensors for a "joint detection" is expected to significantly improve the reliability especially in challenging environments;

– radio communications for use of wireless sensors in, specifically, urban warfare provides further challenges such as overcoming possibly strong interference from many sources, shadowing from buildings coupled with severe multipath transmission and at the same time achieving sufficient coverage and energy-efficiency with inconspicuous small-scale antennas and electromagnetic patterns;

– miniaturization of sensors allowing for a quick and automated network deployment and unsuspicious operation;

– robustness of sensors for deployment from planes or by rocket-launches;

– avoidance of data loops in large sensor networks;

– appropriate anti-tamper mechanisms;

– the optimization of sensor networks to provide the most efficient coverage of a geographic area; a number of trade-offs need to be considered including cost (minimizing the cost per unit area of coverage), communications range, sensor range, device size, weight, power, capability (e.g., detect and classify or just detect), and deployment mechanisms;

– agree on common formats and standards for sensor data and communications exchange.

5.2. Scientific challenges

Capabilities required for 3GSN sensor networks are far-reaching, and the step from existing 2GSN to future 3GSN truly ad hoc systems is huge. Research has still to address a number of challenges in order to increase the usability, flexibility and security, as well as to facilitate longer-term operations. These challenges include:

– security, particularly regarding the effectiveness of reputation approaches to protect against the injection of spoof messages or jamming;

– suitable power supplies and energy efficient protocols to meet the long-endurance applications where networks may be in place for several months; this includes power scavenging (e.g., EU IST VIBES project [19, 20]) and novel power sources [21];

– effective and efficient remote air delivery of sensors ensuring even density and coverage across area;

– robustness of data fusion and analysis, ensuring that data from multiple sensors can be appropriately processed to accurately detect and track moving objects even in the presence of measurement inaccuracies, distortions and communications delays.

6. Conclusions

Wireless sensor networks will have a role to play for a number of military purposes such as enemy movement detection and force tracking.

Comparing the actual military requirements with the current research and the available products, some misalignments become obvious. Much effort in current academic research is spent on optimization, e.g., routing protocols to work with tens of thousands of nodes, which are assumed to be small, lightweight and cheap. The paper has addressed the military requirements for actual costs per node, the current mode of deployment (mainly manual network set-up) and physical size. The limited existing products tend to address the current military requirements in that they are composed of larger sensor devices and consist only of small numbers of nodes (often even < 30 nodes).

The key challenges to deploying military wireless sensor networks are more practical engineering problems than fundamental research issues. However there are still outstanding scientific challenges as stated in this paper. Urban warfare scenarios are especially demanding and efforts such as the optimization of multi-modal sensors need to be addressed.

The use of common formats for sensor data such as textual information or images facilitates information exchange across network boundaries and promotes openness between sensor network vendors. This allows those requiring kit to purchase from multiple suppliers and keeps a competitive market place open (i.e., no one supplier can monopolize the supply base). The use of appropriate NATO STANAGs (standardization agreements) is encouraged.

References

[1] Wolfpack program, US Defense Advanced Research Projects Agency (DARPA), http://web-ext2.darpa.mil/sto/strategic/wolfpack.html

[2] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks", *Ad-hoc Netw.*, no. 3, pp. 325–249, 2005 (first published in Nov. 2003).

[3] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: a survey", *IEEE Wirel. Commun.*, vol. 11, iss. 6, pp. 6–28, 2004.

[4] D. Niculescu, "Communication paradigms for sensor networks", *IEEE Commun. Mag.*, vol. 43, iss. 3, pp. 116–122, 2005.

[5] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocols for wireless microsensor networks", in *Proc. Int. Conf. Syst. Sci.*, Hawaii, USA, 2000.

[6] S. Lindsey and C. S. Raghavendra, "PEGASIS: power efficient gathering in sensor information systems", in *IEEE Aerosp. Conf. Proc.*, Montana, USA, 2002, vol. 3, pp. 3-1125–3-1130.

[7] TinyOS 2007, http://www.tinyos.net/

[8] V. Rodoplu and T. H. Meng, "Minimum energy mobile wireless networks", *IEEE JSAC*, vol. 17, no. 8, pp. 1333–1344, 1999.

[9] Y. Xu, J. Heidemann, and D. Estrin, "Geography informed energy conservation for ad hoc routing", in *Proc. 7th Ann. ACM/IEEE Int. Conf. Mob. Comp. Netw.*, Rome, Italy, 2001, pp. 70–84.

[10] Y. Yu, D. Estrin, and R. Govindan, "Geographical and energy-aware routing (GEAR): a recursive data dissemination protocol for wireless sensor networks", Techn. Rep., UCLA-CSD TR-010023, UCLA Comp. Sci. Dept., May 2001.

[11] J. Kulik, W. Rabiner, and H. Balakrishnan, "Adaptive protocols for information dissemination in wireless sensor networks", in *Proc. 5th ACM/IEEE MobiCom Conf.*, Seattle, USA, 1999.

[12] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks", in *Proc. ACM MobiCom 2000 Conf.*, Boston, USA, 2000, pp. 56–67.

[13] D. Braginsky and D. Estrin, "Rumor routing algorithm for sensor networks", in *Proc. 1st Worksh. Sens. Netw. Apps.*, Atlanta, USA, 2002.

[14] C. Schurgers and M. B. Srivastava, "Energy efficient routing in wireless sensor networks", in *Proc. MILCOM Conf.*, McLean, USA, 2001.

[15] Y. Yao and J. Gehrke, "The cougar approach to innetwork query processing in sensor networks", SIGMOD Record, Sept. 2002.

[16] Delay Tolerant Networking Research Group of the Internet Research Task Force (IRTF), http://www.dtnrg.org and http://www.irtf.org/

[17] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall, and H. Weiss, "Delay-tolerant networking", RFC 4838, Apr. 2007.

[18] C. S. Raghavendra, K. M. Sivalingam, and T. Znati, *Wireless Sensor Networks*. New York: Springer, 2006.

[19] VIBES project, on vibration energy scavenging, EU IST, 2004–2007, http://www.vibes.ecs.soton.ac.uk/

[20] S. P. Beeby, M. J. Tudor, R. N. Torah, T. O'Donnell, and S. J. Roy, "Micro electromagnetic generator for vibration energy harvesting", *J. Micromech. Microeng.*, vol. 17, pp. 1257–1265, 2007.

[21] "Radio isotope micropower sources program", US Defense Advanced Research Projects Agency (DARPA), http://www.darpa.mil/sto/smallunitops/rims.html

[22] M. Healy, T. Newe, and E. Lewis, "A survey of operating systems for wireless sensor nodes", in *5th Worksh. Internet, Telecommun. Sig. Proces.*, Hobart, Australia, 2006.

Michael Winkler received his M.Sc. (1997) after studies at the University of Bristol and the ENST Bretagne, his M.Sc. (1998) and Ph.D. (2005) degrees of the University of Hannover, Germany. He worked as a scientist at the Institute for Communications of the University of Hannover and as technology consultant for an international media company. His main fields of research are wireless OFDM-based transmissions and high data rate communication networks. In 2005 he joined the NATO C3 Agency, where he is leading the team on ad hoc networking.

e-mail: Michael.Winkler@nc3a.nato.int
NATO C3 AGENCY (NC3A)
P.O. Box 174
2501 CD The Hague, Netherlands

Klaus-Dieter Tuchs received his M.Sc. on electrical engineering in 1996 and his Ph.D. in 2002 at University of Hanover, Germany. He worked as a scientist at the Institute for Communications of the University of Hannover until 2003. His main research area was on the optimization of fault management systems and the development of data mining algorithms. From 2003 to 2006 he worked as a team leader at a telecommunications planning and consulting company (DOK SYSTEME). In 2007 he joined the NATO C3 Agency (The Hague, Netherlands) as a Senior Scientist for network management and telecommunication protocols.
e-mail: Klaus-Dieter.Tuchs@nc3a.nato.int
NATO C3 AGENCY (NC3A)
P.O. Box 174
2501 CD The Hague, Netherlands

Kester Hughes is an experienced, senior team leader with QinetiQ's Communications Division with broad experience in defining, managing and delivering complex defence related research programmes. He has a detailed knowledge and understanding of the breadth UK military communications systems. He has broad experience of a wide variety of communications systems and technologies including military specific systems, communications technologies for sensor networks, IP and the Internet, cellular networks, ATM and wireless LAN technology. In over sixteen years of working, he has contributed and lead many applied research tasks and provided advice and consultancy to MOD's procurement teams and industry.
e-mail: knhughes@QinetiQ.com
QinetiQ Malvern
St Andrews Road, Malvern
Worcestershire, WR14 3PS, UK

Graeme Barclay has a background in mathematics and joined QinetiQ (formerly DERA) in 2000. He is a part of the networks group within the communications department and has worked primarily on research for the UK Ministry of Defence investigating the use of communications equipment and technologies within the military tactical environment. Much of his work has involved analysing wireless communications systems and the effects of mobility and quality of service issues on end-to-end delivery. Recently he has been involved in the use of MANET protocols and has led a team responsible for providing networking solutions within a sensor network.
e-mail: gbarclay@QinetiQ.com
QinetiQ Malvern
St Andrews Road, Malvern
Worcestershire, WR14 3PS, UK