12TH ICCRTS "Adapting C2 to the 21st Century"

Wireless Sensor Networking Support to Military Operations on Urban Terrain

Track 2: Networks and Networking

Track 8: C2 Technologies and Systems

Dr. António Grilo
IST/UTL, INESC,
Rua Alves Redol, nº 9
1000-029 LISBOA,
Portugal
Tel: +351-213100226
antonio.grilo@inesc.pt

(contact author)

Rui Silva
ESTIG,
Rua Afonso III,
nº1
7800-050 Beja,
Portugal
rs.beja@gmail.com

Lt Col Paulo Nunes
CINAMIL/
Academia Militar
Paço da Rainha, 29
1169-203 LISBOA,
Portugal
pfvnunes@net.sapo.pt

Maj José Martins
CINAMIL
Academia Militar
Paço da Rainha, 29
1169-203 LISBOA,
Portugal
josecarloslm@netcabo.pt

Prof. Mário Nunes
IST/UTL, INESC,
Rua Alves Redol, nº 9
1000-029 LISBOA,
Portugal
Mario.nunes@inesc.pt

Wireless Sensor Networking Support to Military Operations on Urban Terrain[1]

Dr. António Grilo
IST/UTL, INESC,
Rua Alves Redol, nº 9
1000-029 LISBOA,
Portugal
Tel: +351-213100226
antonio.grilo@inesc.pt
(contact author)

Rui Silva
ESTIG,
Rua Afonso III,
nº1
7800-050 Beja,
Portugal
rs.beja@gmail.com

Lt Col Paulo Nunes
CINAMIL/
Academia Militar
Paço da Rainha, 29
1169-203 LISBOA,
Portugal
pfvnunes@net.sapo.pt

Maj José Martins
CINAMIL
Academia Militar
Paço da Rainha, 29
1169-203 LISBOA,
Portugal
josecarloslm@netcabo.pt

Prof. Mário Nunes
IST/UTL, INESC,
Rua Alves Redol, nº 9
1000-029 LISBOA,
Portugal
mario.nunes@inesc.pt

Abstract

FP6 IST research project Ubiquitous Sensing and Security in the European Homeland (UbiSeq&Sens) aims at providing a comprehensive architecture for medium and large scale Wireless Sensor Networks (WSN)s, with the full level of security and reliability required to make them trusted and secure for all applications, while considering early-warning and tracking in a Homeland Security/Defense context (e.g., support of anti-terrorist SWAT team operations) as one of the scenarios for system demonstration. This paper extrapolates from this scenario, defining an architecture for WSNs supporting Military Operations in Urban Terrain (MOUT) in the context of XXIst century Operations Other Than War (OOTH). Based on the defined architecture, the authors identify the main WSN Networking and Security issues and challenges that must be overcome to provide the assurance, efficiency and reliability required by the warfighter, which constitute the focus of ongoing work in IST FP6 UbiSeq&Sens.

Keywords:.Wireless Sensor Networks, Network Centric Military Communications, Military Operations on Urban Terrain, IST FP6 UbiSec&Sens

1 Introduction

Wireless Sensor Networks (WSNs) have motivated intense research, in academia, industry and on the military sector due to its potential to support distributed micro-sensing in environments for which conventional networks are impractical or when the required sensor density demands a robust, secure and cost-effective solution. WSNs rely on large numbers of cheap devices, which are greatly limited in terms of processing, communications and autonomy capabilities. Despite reduced, the capabilities of these devices are leveraged through collaboration in distributed in-network data fusion and processing tasks, with final results that are equivalent to those obtained with centralized processing.

Early-warning and tracking is an application where WSNs have seen significant progress in the last few years, with some practical solutions already existing on the market. However, these commercial WSN systems still lack the security, reliability and efficiency required for this kind of application. FP6 IST research project Ubiquitous Sensing and Security in the European Homeland (UbiSeq&Sens) tries to overcome these limitations. The overall objective of UbiSeq&Sens is to provide a comprehensive architecture for medium and large scale WSNs, with the full level of security and reliability required to make them trusted and secure for all applications, while considering early-warning and tracking in a Homeland Security/Defense context (e.g., support of anti-terrorist SWAT team operations) as one of the scenarios for system demonstration. This

[1] The work described in this paper is based on results of IST FP6 project UbiSec&Sens (http://www.ist-ubisecsens.org/). UbiSec&Sens receives research funding from the European Community's Sixth Framework Programme. Apart from this, the European Commission has no responsibility for the content of this paper.

The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

project, which started in the beginning of 2006 has now completed the scenario specification phase, triggering the beginning of the design work.

The end of the Cold War in the beginning of the 1990s and the reality brought by the dramatic events of September 11th 2001 have led to a shift of the focus of military operations to Operations Other Than War (OOTW) with emphasis on Peace Keeping, Making and Building. The Rules Of Engagement (ROE) associated with these missions significantly constrain the options available to warfighters engaged on Military Operations on Urban Terrain (MOUT). In fact, most of the reality experienced by these warfighters bears more similarity with Homeland Security and counterterrorism operations than with traditional military operations. Consequently, many of the operational concepts are common to both types of scenarios, and so are the supporting technologies. In effect, in the context of so called Three Block War[2] [1], characteristics of the XXIst century, the use of disproportionate force in MOUT is unacceptable, requiring clearing of hostile urban areas to be made block-by-block, or even room-by-room by infantry teams that must directly intervene on the scene. The complexity of urban environments usually precludes full situation awareness. This, coupled with the fact that the adversary is usually expected to have a better understanding about the operational environment, poses significant risks to the life and integrity of warfighters. In such missions, Network Centric Warfare [2] assisted by robust sensor networking is paramount to reduce situation uncertainty, providing early-warning and tracking of unpredicted intrusions in areas considered already cleared, thus denying the intruder the advantage of surprise.

This paper proposes a WSN architecture in the context of MOUT (section 2), extrapolating from the UbiSeq&Sens Homeland Security scenario definition, but taking into account MOUT specificities. Based on the delineated architecture, it identifies the main WSN Networking and Security issues and challenges (sections 3 and 4 respectively) that must overcome in order to provide the assurance and reliability required by the warfighter, which constitute the focus of ongoing work in IST FP6 UbiSeq&Sens. Finally, the paper presents some conclusions and the envisaged way ahead (section 5).

2 MOUT WSN Architecture

The MOUT WSN architecture is depicted in Figure 1. The MOUT WSN nodes are deployed by infantry team elements as they clear the terrain. Once deployed, these nodes self-organize into a multi-hop network, establishing data paths from each individual sensor to special sink nodes. Sink nodes may operate as gateways between the WSN and higher echelon tactical networks, using appropriate technologies like the Joint Tactical Radio System (JTRS) or SATCOM to connect to Command Posts (CP)s where the information from several information systems, sensors and sensor networks is gathered, fused and analysed and where higher-level tactical decisions are made. Deployment must take into account robustness in the connectivity to CPs and consequently it is desirable to deploy several sink nodes, conveniently positioned in a way that minimizes the risk of WSN partition. Warfighters may also be equipped with Personal Digital Assistants (PDAs) or other wireless terminals that allow direct connection to the WSN, turning them into mobile sink nodes. Similar capabilities may be available to robotic elements like Unmanned Aerial Systems (UAS)s or Unmanned Ground Vehicles (UGV)s. Both warfighters and robots may also carry sensors, making them mobile source nodes as well.

[2] General Charles Krulak (USMC) set the stage for the importance of the flexibility and innovation required from the Strategic Corporal when he discussed the need to fight the “three block war.” He stated that, *"in one moment in time, our service members will be feeding and clothing displaced refugees - providing humanitarian assistance. In the next moment, they will be holding two warring tribes apart - conducting peacekeeping operations. Finally, they will be fighting a highly lethal mid-intensity battle. All on the same day, all within three city blocks. It will be what we call the three block war."* In. Krulak, Charles. “The Strategic Corporal: Leadership in the Three Block War.” *Marine Corps Gazette.* Vol 83, No 1. January 1999. pp. 18-22.

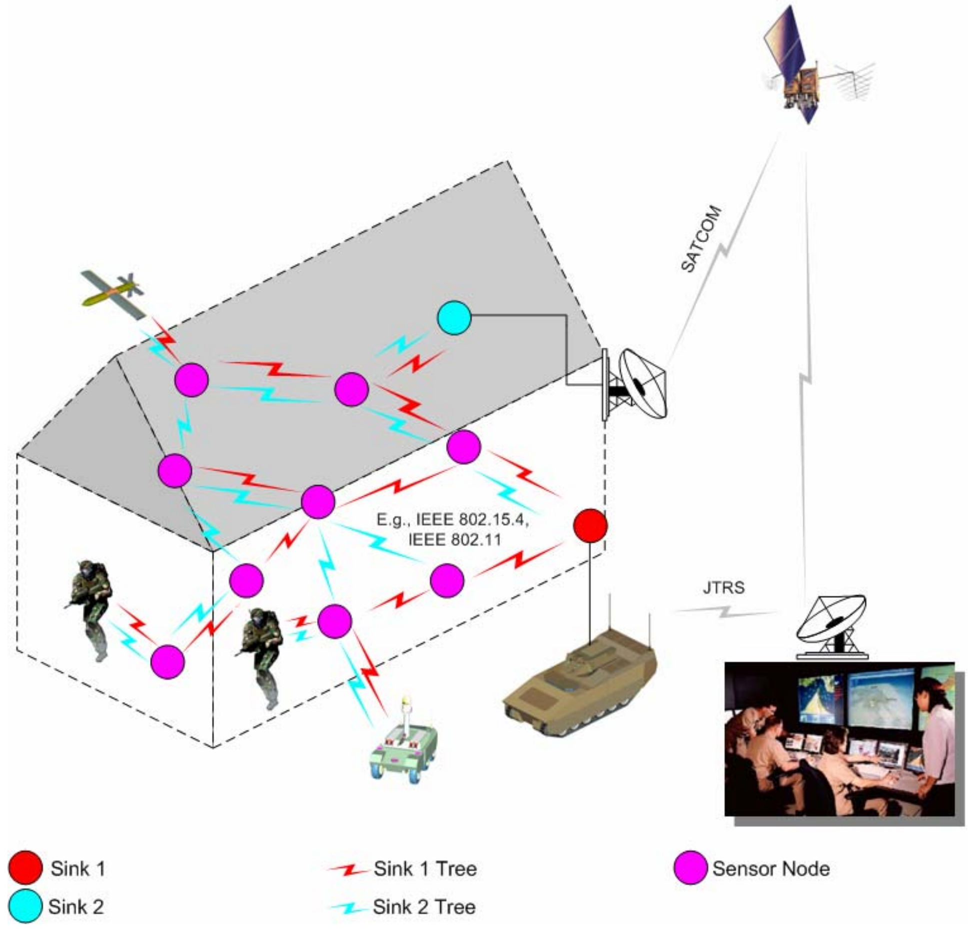

Figure 1: Architecture of the MOUT WSN.

Functional requirements point to the use of the following sensor types:

- Presence/Intrusion (e.g., based on a combination of infrared, photoelectric, laser, acoustic, vibration, etc.);
- Ranging[3] (e.g., RADAR, LIDAR, ultrasonic, etc.);
- Imaging (including infrared and LADAR imaging)[4];
- Noise (acoustic sensor able to produce an audio stream);
- Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) and Toxic Industrial Material (TIM) detectors.

Presence/intrusion sensors doubtless constitute the most useful type of sensor for this scenario. Ranging and Imaging (which can also be used as presence sensors) come next as extra means to increase situation awareness. CBRNE and TIM sensors will also be useful to equip robots, once they become available with the required degrees of miniaturization and effectiveness, which still present many issues and currently constitute active research topics.

[3] Ranging sensors can sometimes be used as presence sensors.

[4] Imaging sensors can sometimes be used as presence sensors.

Intrusion and CBRNE/TIM detectors are the most suitable to operate as alarm triggers. Imaging, noise and ranging sensors present special requirements demanding them to be more capable than other sensors in terms of processing, communications and energy capabilities.

The identified distribution patterns – which greatly rely on multicast and multiple reverse-multicast – and the fact that there is potentially more than one sink, point to a WSN topology that consists of the overlay of several trees, where each sink node forms the root of one element tree.

The density of sensor deployment, network longevity, the nature and size of the area to be covered, constitute important factors that define the required number of nodes and the selected communication technology. Most often, these factors result into multi-tier heterogeneous network solutions, integrating different wireless technologies, each with its own advantages and constraints in terms of energy consumption, range, data rate, latency, etc. Common examples are IEEE 802.15.4 [3] and IEEE 802.11 [4] (see Figure 2). Presence/intrusion and CBRNE/TIM sensors provide the worst case, asking for greater number and density of sensors and a short-range low-power communications technology such as IEEE 802.15.4 (although for reasons of performance and hop number reduction, a heterogeneous solution might be preferred). Due to their bandwidth requirements, ranging, noise and imaging sensors should be directly connected to high bandwidth backbone networks (e.g., IEEE 802.11).

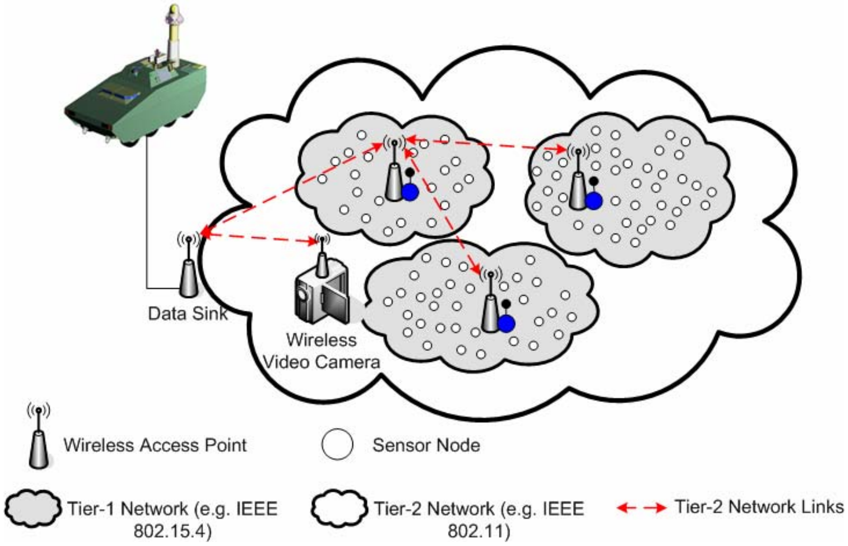

Figure 2: Two-tier MOUT WSN.

3 Networking Issues and Challenges

Within IST FP6 UbiSeq&Sens, "Networking" refers to the functions traditionally expected from the Transport (e.g., Delivery Reliability, Quality of Service and Congestion Control), Network (e.g., Topology Control, Routing) and Data Link (e.g., Medium Access Control – MAC –, link reliability) layers. Energy-efficiency is another aspect that spans all layers of the WSN protocol stack. In fact, current WSN node constraints prevent the use of complex and demanding IP-based protocol architectures. Close-coupling between the traditional Transport, Network and Data Link layers is required instead. This section provides an overview of the main networking challenges and achievements of IST FP6 UbiSeq&Sens.

3.1 Transport Layer

In order to characterise QoS requirements, several data flows were identified and characterised according to the following factors (see Table 1):

- Source (sinks or sensors);
- Destination (sinks or sensors);

- Traffic distribution pattern (Unicast, Multicast, Reverse-Multicast[5], Broadcast, Geocast[6]);
- Traffic generation pattern (on-demand, alarm driven, periodic);
- Delay sensitivity: High (less than 5 s) or Low (less than a few tens of seconds);

Table 1: Data flows identified for the MOUT WSN.

	Source	Destination	Traffic Distribution	Traffic Generation	Delay Sensitivity
Intrusion report	Sensor	Sink	Ucast/ RMcast	all	High
CBRNE report	Sensor	Sink	Ucast/ RMcast	all	High
Ranging report	Sensor	Sink	Ucast/ RMcast	all	High
Imaging / Noise report	Sensor	Sink	Ucast/ RMcast	all	Low
WSN status	Sensor	Sink	Ucast / RMcast	On-demand	Average
Data request	Sink	Sensor	Ucast / Mcast / Bcast / Gcast	On-demand	High
Configuration command	Sink	Sensor	Ucast / Mcast / Bcast / Gcast	On-demand	Low

Some data flows require guaranteed delivery. However, not all data requires full reliability, a fact that can be exploited to increase transport efficiency. For example in alarm triggering sensors, abrupt measurement change reports require full reliability. Where measurements are stable within well-defined bounds, periodic reporting can tolerate some loss, which means that these reports can be sent with partial (< 100%) reliability. The transport mechanisms must be flexible enough to adapt to the best trade-off between reliability and efficiency. Table 2 shows the different reliability requirements envisaged for each type of data flow, taking into account the following factors:

- Reliability grade (none, partial, total): Partial reliability requires a lower amount of resources.
- Reliability mode: Message-oriented (reliability looks at individual messages) or timeliness-oriented (most recent messages replace older ones in a flow). Timeliness-oriented reliability requires a lower amount of resources.

[5] Also designated Convergecast.

[6] Geocast is a form of location-based broadcast in which a packet is broadcast to every node within a defined geographical area.

Table 2: Reliability requirements.

	Reliability grade	**Reliability mode**
Intrusion report	On-Demand / Alarm / End of Alarm: Total Periodic reporting within bounds: Partial	On-Demand / Alarm / End of Alarm: Message-oriented Periodic reporting within bounds: Timeliness-oriented
CBRNE report	On-Demand / Alarm / End of Alarm: Total Periodic reporting within bounds: Partial	On-Demand / Alarm / End of Alarm: Message-oriented Periodic reporting within bounds: Timeliness-oriented
Ranging report	Total	Timeliness-oriented
Imaging / Noise report	Total or Partial (depends on error resilience mechanisms implemented by the codecs)	Message-oriented
WSN status	Total	Message –oriented
Data request	Total	Message –oriented
Configuration command	Total	Message –oriented

State-of-the-art reliable transport protocols like Pump Slowly, Fetch Quickly (PSFQ) [5] or Reliable Multi-Segment Transport (RMST) [6] are not designed to offer this degree of flexibility. On the other hand, Event-to-Sink Reliable Transport ERST) [7] supports partial reliability but presents efficiency issues that make it unpractical for utilization in real WSNs. This is the reason why the ongoing development of new reliable and efficient transport protocol is regarded as one of the main networking challenges in IST FP6 UbiSec&Sens. An initial specification of a Distributed Transport for Sensor Networks (DTSN) [8] was already produced, but performance evaluation is still ongoing. DTSN bears some resemblance to RMST and PSFQ regarding some basic mechanisms like caching in relay nodes and selective repeat Automatic Repeat Request (ARQ), but includes new functionalities and optimization that confer more flexibility and efficiency. An example of these mechanisms is the support of partial reliability through probabilistic memorization at the source, defined by different classes of service. Performance results have shown that a significant throughput gain can be achieved with partial reliability relative to full reliability (see Figure 3), a feature that can be exploited by some types of flows.

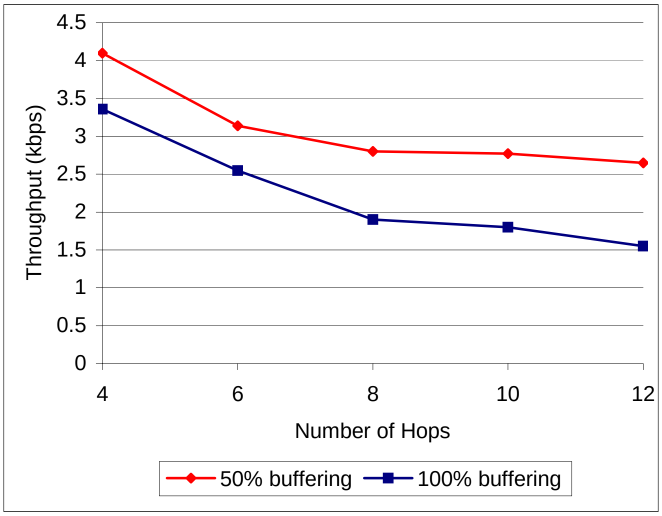

Figure 3: Throughput achieved by a service class with 50% of memorization probability at the source, versus 100% reliability.

DTSN is also designed to be closely-coupled with routing, although its only requirement is the support of individual node addressing by the routing protocol (see below). An implementation of the DTSN total reliability service in TinyOS 1.1 is already available. The DTSN implementation is now being extended and ported to TinyOS 2.0.

3.2 Routing and In-Network Processing

An important performance requirement is to minimize the probability of false alarms in intrusion and CBRNE detection (the alarm-triggering sensors). Sensor redundancy can accomplish this, allowing the system to look at the results of the aggregation/fusion of measurements reported by individual sensors covering the same vicinity. An option is to perform aggregation/fusion at the CPs or warfighter terminals, provided that measurement reports from all relevant individual sensors are delivered by the WSN. Another option is to exploit sensor redundancy in a way that also increases network efficiency. This is possible if data aggregation/fusion is performed inside the WSN. In-network processing leads to traffic reduction because only the results of the aggregation/fusion are delivered to the sink nodes instead of individual sensor measurements. When the fused sensor vicinity is large, it is mandatory that sensing sensor nodes are undoubtedly identified with respect to their location, or at least to identify a well defined area from where fused data stem. Election of aggregation/fusion nodes is another issue that must be addressed by the Routing layer.

Some operations are performed over specific sensor nodes (e.g. on-demand imaging requests) and some sensor data must bear node-specific positioning information. For other sensor data types – even if geographically referenced – only the result from the fusion/aggregation of data from several nodes is required (e.g. intrusion or CBRNE detection in an area covered by several sensors). When sensor nodes must be individually addressed, a pure data-centric routing architecture such as Directed Diffusion [9] is not enough. A hybrid node-centric / data-centric solution is then necessary. Another important research challenge consists of assuring low-latency energy-efficient routing to/from mobile sinks/sources, which also requires low-level support at the MAC layer. This issues are currently under investigation in IST FP6 UbiSec&Sens.

3.3 Medium Access Control

The low delays required by intrusion and CBRNE alert reports cannot be achieved by the Transport layer only. The maximization of WSN longevity through low duty cycles will likely compromise established delay bounds, even if the Transport and Routing protocols behave optimally. In order to achieve an acceptable trade-off of the low duty-cycle and low delay bound requirements, a new MAC protocol is required, since state-of-the-art solutions do not address this issue. This is an area where significant progress has already been made in IST FP6 UbiSec&Sens.

A new MAC protocol was developed designated Tone-Propagated MAC (TP-MAC) [10]. In order to achieve low duty cycle, the proposed TP-MAC protocol inherits some important features from other MAC protocols, namely synchronized wake-up periods (S-MAC [11], T-MAC [12], SCP-MAC [13]), and synchronized wake-up-tone announcement of data availability associated with scheduled channel polling (SCP-MAC). However, in TP-MAC the wake-up-tones are propagated across the WSN so that the nodes in the path from source to destination are woken-up as quickly as possible, before the arrival of the heralded data packets. In this way, TP-MAC is able to achieve low delivery latency even if the WSN node duty-cycle is extremely low, preventing or at least ameliorating the early-sleeping problem.

TP-MAC is based on the convergecast communication paradigm, assuming that the WSN is organized in a logical tree topology, associated with one sink, which corresponds to the root node. This again imposes some cross-layer constraints on the Network (i.e. Routing) layer, which is not a real limitation, since most typical WSN scenarios require convergecast of sensor data towards sink nodes. In fact, TP-MAC supports topologies with more than one sink node, though at the cost of some energy-efficiency. The detailed multi-sink support mechanism will not be explained in detail due to space limitations.

In a tree-structure rooted at the sink node, it is possible to define different levels defined by the minimum hop distance relative to the sink node. In this way, the sink node constitutes level 0 and the level number increases as hop distance to the sink node increases. The establishment of network levels is at the core of the wake-up-tone propagation mechanism.

TP-MAC establishes super-frame periods for channel access, each starting by a synchronization wake-up-tone and two wake-up-tone propagation windows (upstream and downstream), followed by a data transmission window (see Figure 4). The size of the tone propagation window can be different for upstream and downstream, depending on the latency requirements. The channel access method in the transmission window can be based on any MAC protocol, e.g. plain CSMA/CA, S-MAC, T-MAC, SCP-MAC, etc.

The synchronization tone marks the beginning of the super-frame structure. This tone is periodically activated by the sink node and slowly propagated downstream to announce the transmission of a broadcast synchronizing/re-synchronizing SYNC packet in the data transmission window. The details of synchronization establishment/maintenance will also not be explained in this paper due to space limitations.

The wake-up-tone propagation windows allow the announcement of data and establishment of fast paths from source to destination.

When no data traffic is generated, each node only has to poll the channel once in each wake-up-tone propagation window (only in the slot that corresponds to its level), and sometimes also in the synchronization slot. The nodes are allowed to sleep during the rest of the super-frame.

When a node has data to transmit, it first sends a wake-up upstream tone (e.g., for sensing data destined to the sink node), or a waking downstream tone (e.g., for control messages issued by the sink node to sensor nodes). The wake-up-tone propagation window structure guarantees that nearby nodes in the next upper/lower level listen to the generated wake-up-tone. They then propagate the tone upstream/downstream, as it can be seen in the tone propagation windows of Fig. 1. If a node detects a wake-up-tone in the last slot of a propagation window, then it shall only propagate it in the next super-frame. The tone propagation mechanism, which resembles the data propagation mechanism of D-MAC [14], assures that nodes within some hop distance are woken-up in just one operation cycle, forming a fast-path before actual data arrives. The maximum distance that a wake-up tone can reach in a single super-frame is equal to the number of tones in each tone propagation window, which is a configuration parameter.

The nodes that form a fast path stay active in the data transmission window, for a pre-defined time interval, which is dimensioned to keep those nodes active until the announced data arrives. The timeout mechanism is similar to that defined in T-MAC.

TP-MAC nodes only poll the media for a number slightly above two times per cycle (two polls, respectively for upstream and downstream propagated tones in each super-frame, and more seldom for the synchronization/re-synchronization tone), propagating the wake-up tones fast and deeply through the network (and thus opening fast data transmission paths). In this way it is possible to achieve low latencies simultaneously with low duty cycles.

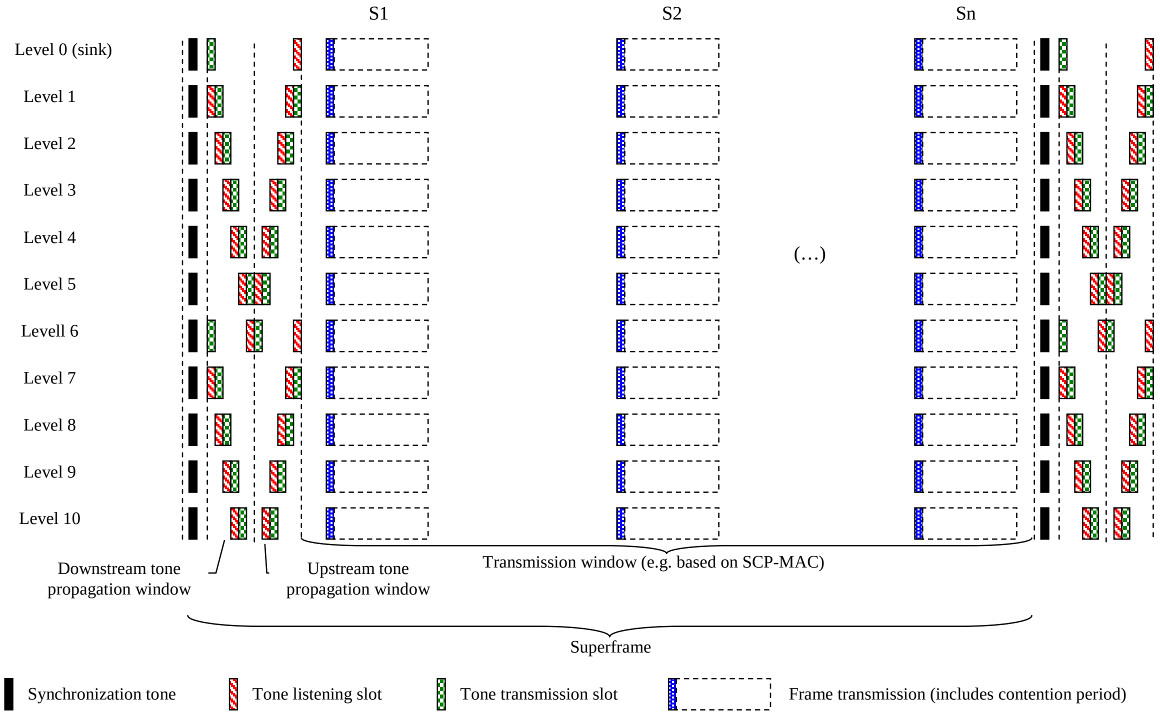

Figure 4: TP-MAC super-frame structure and wake-up-tone propagation.

An analytical model was developed to compare TP-MAC with SCP-MAC, under the assumption that SCP-MAC is used by TP-MAC for data transmission. This model addresses the relationship between duty-cycle during periods without traffic, and the minimum latency that can be achieved once the first packet of an active stream is generated.

Figure 5 shows the ratio between the duty cycles of TP-MAC and SCP-MAC as a percentage, for different numbers of hops, and different sizes of the wake-up-tone propagation window. Other TP-MAC parameters are the following: number of transmission slots: 10; synchronization tone period: 5 cycles. It is worth to note that TP-MAC duty cycle decreases with increasing number of hops, but its energy efficiency gain with respect to SCP-MAC stabilizes for high numbers of hops. It is also shown that higher number of tones can give higher energy efficiency gain. For instance, for 10 tones, we can obtain a duty cycle as low as 22% of the SCP-MAC duty cycle, for large network sizes.

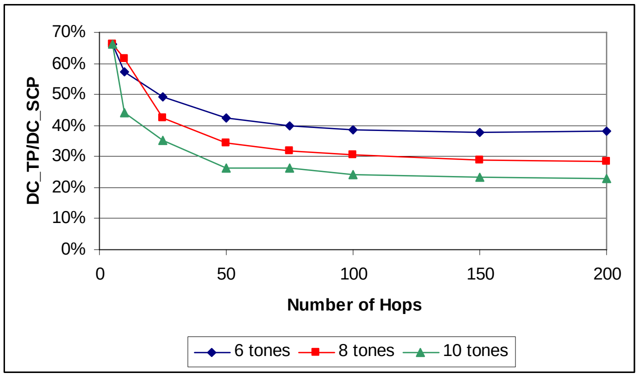

Figure 5: Ratio between the duty cycles of TP-MAC and SCP-MAC as a function of the number of hops and the size of the wake-up-tone propagation window.

The development of TP-MAC is still not fully completed. Among the remaining issues is the support of efficient mechanisms to deal with sink/source mobility. The INESC team is also developing another MAC protocol, this time based on TDMA principles for implementation simplicity, but incorporating some features of TP-MAC.

4 Security Issues and Challenges

Information and network assurance are vital to the successful conduct of Network Centric Operations. At the WSN level, these requirements are reflected as protection against physical attacks against the network equipment (WSN nodes) or logical attacks against WSN communications. This section will focus on the main issues and technical challenges that these possible attacks entail in a MOUT WSN scenario.

4.1 Physical Attacks

Considering the physical attacks it is desired that the capture of one or more nodes of the WSN do not compromise the security of the whole system [15]. Mechanisms must be in place to minimize the probabilities of successful physical tampering of captured WSN nodes on the part of the attacker. Physical analysis of one or more captured WSN nodes by the attacker would expose essential security information such as encryption keys, allowing the attacker to enter and expand its control of the MOUT WSN. This could then be used to passively exploit MOUT WSN sensing data to his own benefit, or otherwise to cause ruptures in MOUT WSN operation.

The tampering protection mechanisms implemented in each WSN node must take into account the possible use by the attacker of sophisticated procedures in order to analyse the WSN node. For example, the WSN nodes should have the capability to detect these physical attacks and should self-destruct upon detection of a physical attack. The kind of mechanisms used to detect a physical attack can range from a simple “open box sensor”, or an “acceleration sensor”, or even a “GPS movement sensor”, installed inside the tamper resistant box that contains the WSN node. More sophisticated mechanisms considered for implementation include the detection of environmental actions taken by attackers, namely temperature, clock frequency or voltage decrease/increase beyond the operating range of WSN nodes, so that the sensing and/or communications behaviour of the node become compromised.

4.2 Logical Attacks

Logical attacks are of more concern than physical attacks because they are not so easily detected. Taking a global view on the logical attacks we can classify them into passive and active attacks [16]. Following is a description of these two kinds of attacks, clearly identifying their target Security Services in the MOUT WSN.

Passive attacks are those that simply gather and process the information exchanged between the WSN nodes, and are here designated Passive Man-in-the-Middle attacks. These attacks will likely be targeted at the Confidentiality Security Service of the WSN. To counter this kind of attack a One Time Pad encryption system must be used for all the messages in the WSN, which means that every message in the WSN will be encrypted using a different key. Due to the particularities of WSN communications, and looking at the MOUT WSN in particular, which is mostly alarm-oriented with little traffic being exchanged during normal operation, the simple analysis of network activity may indicate that an alarm condition was triggered. Even if there is network activity in the absence of alarm conditions (e.g. periodic exchange of control messages), since the messages are generally short and some message types may be periodically repeated or at least present very similar content or format, the attacker may be able to identify unusual traffic patterns as indicators of alarm triggering. This is a characteristic that makes WSNs very susceptible to a special kind of Passive Attack that simply relies on the analysis of the traffic pattern of the WSN nodes. In order to counter this, the WSN nodes should send some special messages with the purpose of confusing an attacker performing Traffic Analysis. In addition to this and assuming the use of a different key for each single message, INESC is currently developing a system in which the content of the message is itself reorganized in a way that even for equal messages, the encrypted payload is always different. As result, cryptanalysis of the captured messages becomes twice difficult because even for equal messages encrypted used different keys, the content itself is modified in a unique manner using a different mechanism for each message. We are currently disregarding attacks directed at the system’s encryption key as the latter will never be repeated between different messages.

Active attacks, which are here designated Active Man-in-the-Middle attacks, can assume several forms that can be grouped in three main classes:

- Forgery of a message to be inserted into the WSN;

- Replay of a captured message into the WSN;
- Insertion of a modified captured message into the WSN.

Concerning the first class or message forgery attack, it is assumed that the attacker has some knowledge about the process of construction of real messages, but in this case the encryption key must be in conformance with the One Time Pad system and we assume that this will be very difficult to guess as a Perfect Secrecy basis. Consequently, this kind of attack would more probably be targeted at the Authentication Security Service, where the attacker tries to authenticate with the WSN as a first stage to enter the network communications flow. It could also be targeted at inserting wrong information into the WSN, for instance information about routing, and in this way affect the Coherence and Consistency of the WSN.

Another Security Service that could be targeted by forgery attacks is the Availability of the WSN or at least of some restricted portions of the WSN. This could be achieved by the activation of a jamming signal that would lead to a Denial of Service situation. Some countermeasures against this last situation consist of dynamically changing the transmission band (or spreading sequence in case of CDMA) or supporting adaptive transmission power control. Changing routing paths to divert traffic around affected WSN portions is another possible countermeasure.

Concerning the second class or replay attack, they can be used to target the Authentication Security Service and the Coherence and Consistency of the WSN even more easily than with a forgery attack. Sequence control using timestamps or message lifetime, are possible countermeasures.

Concerning the third class of message modification attack, it could be targeted at the Message Integrity Security Service, Authentication Security Service as well as at the Coherence and Consistency of the WSN. In this last situation it could easily compromise the routing and data aggregation/fusion functions of the WSN.

Moreover, it must be added that in the last two classes, the place of capture and insertion into the WSN can be different. In this case we are in the presence of a Wormhole Attack in which captured messages may be relayed between two different locations using a separate broadband wireless or even wired connection. Wormhole attacks can lead to an increased entropy, inefficiency and even disruption of communications by interfering with routing. This is why countermeasures against Wormhole attacks are usually implemented at the routing layer. In fact, Secure Routing is an area to which IST FP6 UbiSec&Sens is paying considerable attention.

The challenge of all the aspects related with Logical Attacks stated above is now under deep analysis and research in UbiSec&Sens. INESC in particular is also developing an enhanced key establishment and distribution scheme under the recommendations stated in [17].

5 Conclusions and Future Work

This paper has presented an architecture for WSN networking support to MOUT operations in the context of XXIst century Operations Other Than War, based on work developed within the IST FP6 UbiSec&Sens project, which has now completed the scenario definition phase. Based on the presented architecture definition, the main networking and security issues and challenges were identified and matched against ongoing research at IST FP6 UbiSec&Sens, with emphasis on the work being done at INESC. In the Networking arena, some achievements can already me mentioned:

- Specification and initial evaluation of the Distributed Transport for Sensor Networks (DTSN), a new reliable transport protocol, whose flexibility allows it to be tailored to the different degrees and trade-offs of reliability and quality of service required by the different traffic flows transported by the MOUT WSN.
- Specification and initial evaluation of the Tone-Propagated MAC protocol, a new MAC protocol specially suited to alarm-oriented WSN applications such as MOUT. This MAC protocol provides low latencies in the transport of time-critical messages (e.g., intrusion reports), while allowing for ultra-low duty cycles to maximize WSN longevity, minimizing maintenance.

Work will proceed with the enhancement and further evaluation of the protocols mentioned above, as well as the development of efficient routing mechanisms supporting aggregator node election.

In the Security arena, work is being done to develop more robust key pre-distribution schemes as well as advanced message payload encryption mechanisms to prevent message matching analysis. Secure routing, including countermeasures against Wormhole attacks, is another important research topic considered in project IST FP6 UbiSec&Sens. Transport layer security, which has been a neglected topic so far, is also being addressed in the context of DTSN development.

6 References

[1] D. Alberts, R. Hayes, '*Power to the Edge*', Command and Control Research Program (CCRP), DoD, Washington DC, USA, 2003.

[2] D. Alberts, J. Garstka, F. Stain, '*Network Centric Warfare – Developing and Leveraging Information Superiority*', 2nd Edition (Revised), Command and Control Research Program (CCRP), DoD, Washington DC, USA, 2000.

[3] IEEE Std. 802.15.4, "Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)", 2003.

[4] IEEE Std. 802.11, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", 1999.

[5] C. Wan, A. Campbell, L. Krishnamurthy, "PSFQ: A Reliable Transport Protocol For Wireless Sensor Networks", First ACM International Workshop on Wireless Sensor Networks and Applications (WSNA'2002), Atlanta, Georgia, USA, September 2002.

[6] F. Stann, J. Heidemann, "RMST: Reliable Data Transport in Sensor Networks", Proc. IEEE International Workshop on Sensor Net Protocols and Applications (SNPA), Anchorage, Alaska, USA, May 2003.

[7] Y. Sankarasubramaniam, O. Akan, I. Akyildiz, "ESRT: Event-to-Sink Reliable Transport in Wireless Sensor Networks", Proc. of the ACM MobiHoc'03, Annapolis, Maryland, USA, June 2003.

[8] B. Marchi, "Reliable and Efficient Transport in Wireless Sensor Networks", M.Sc. Thesis, University of Cagliari (the development and supervision was done at INESC, Lisboa, Portugal), Department of Electrotechnical and Electronic Engineering, Cagliari, Italy, April 2006.

[9] C. Intanagonwiwat, R. Govindan, D. Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks", In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCOM '00), Boston, Massachussetts, USA, August 2000.

[10] A. Grilo, M. Macedo, M. S. Nunes, "An Energy-Efficient Low-Latency Multi-sink MAC Protocol for Alarm-driven Wireless Sensor Networks", Proceedings of the 3rd EuroNGI Workshop on Wireless and Mobility, Sitges/Barcelona, Spain, June 2006. In J. García, Llorenç Cerdà, "Wireless Systems and Mobility in Next Generation Internet", Lecture Notes on Computer Science, Springer, Vol. 4369, ISBN-978-3-540-70968-8, pp. 87-101, 2007.

[11] W. Ye, J. Heidemann, D. Estrin, "An Energy-Efficient MAC Protocol for Wireless Sensor Networks", Proc. of the IEEE INFOCOM, pp. 1567-1576, New York, NY, USA, June 2002.

[12] T. Dam, K. Langendoen, "An Adaptive Energy-Efficient MAC Protocol for Wireless Sensor Networks", Proc. of the First ACM SenSys Conference, pp. 172-180, Los Angeles, CA, USA, November 2003.

[13] W. Ye, J. Heidemann, "Ultra-Low Duty Cycle MAC with Scheduled Channel Polling", Technical Report ISI-TR-2005-604, USC/Information Sciences Institute, CA, USA, July 2005.

[14] G. Lu, B. Krishnamachari, C. Raghavendra, "An Adaptive Energy-Efficient and Low-Latency MAC for Data Gathering in Wireless Sensor Networks", in Proceedings of the 18th International Parallel and Distributed Processing Symposium (IPDPS'2004), Santa Fe, NM, USA, April 2004.

[15] Federal Information Processing Standards Publication (FIPS PUB) 140-2, "Security Requirements for Cryptographic Modules", National Institute of Standards and Technology, May 2001.

[16] W. Stallings, '*Cryptography and Network Security Principles and Practices*', 4th Edition, Prentice Hall, 2006

[17] Institute of Standards and Technology Special Publication 800-56, “Recommendation on Key Establishment Schemes”, Draft 2.0, National Institute of Standards and Technology, 2003.