Heterogeneous Wireless Sensor Networks Enabled Situational Awareness Enhancement for Armed Forces Operating in an Urban Environment

Pawel Kaniewski
Radiocommunications and EW Dept.
Military Communications Institute
Zegrze, Poland
ORCID 0000-0001-8907-8637

Janusz Romanik
Radiocommunications and EW Dept.
Military Communications Institute
Zegrze, Poland
ORCID 0000-0002-6067-423X

Krzysztof Zubel
Radiocommunications and EW Dept.
Military Communications Institute
Zegrze, Poland
ORCID 0000-0002-4207-5786

Edward Golan
Radiocommunications and EW Dept.
Military Communications Institute
Zegrze, Poland
e.golan@wil.waw.pl

Maria D. R-Moreno
TNO
The Hague, The Netherlands
ORCID 0000-0002-7024-0427

Paweł Skokowski
Institute of Communications Systems
Military University of Technology
Warsaw, Poland
pawel.skokowski@wat.edu.pl

Jan M. Kelner
Institute of Communications Systems
Military University of Technology
Warsaw, Poland
jan.kelner@wat.edu.pl

Krzysztof Malon
Institute of Communications Systems
Military University of Technology
Warsaw, Poland
krzysztof.malon@wat.edu.pl

Krzysztof Maślanka
Institute of Communications *Systems*
Military University of Technology
Warsaw, Poland
krzysztof.maslanka@wat.edu.pl

Emil Guszczyński
ITTI Sp. o.o.
Poznań, Poland
emil.guszczynski@itti.com.pl

Łukasz Szklarski
ITTI Sp. o.o.
Poznań, Poland
lukasz.szklarski@itti.com.pl

RR Venkatesha Prasad
Delft University of Technology
Delft, The Netherlands
r.r.venkateshaprasad@tudelft.nl

***Abstract*—Situational awareness of armed forces acting in an urban environment is a key factor determining the success of military operations. In 2021 the European Defence Agency established the project on Wireless Sensor Networks for Urban Local Areas Surveillance. The main goal of the project is to assess how the situational awareness in an urban environment can be enhanced with the application of heterogeneous, autonomous and reconfigurable sensors. The paper presents a novel comprehensive approach that takes into account modelling and management of heterogeneous sensors, energy harvesting techniques, planning and management of the communication backbone, network security for data transfer and authorization for secure information exchange. The architecture of the system and the information flow are presented. The topology aspects are discussed and the sensing part is described. The paper finally highlights new essential enhancements of C2 with particular emphasis on mission planning, data fusion and threat prediction.**

Keywords—situational awareness, wireless sensor networks, communications management, military operation in urban terrain

I. Introduction

Armed forces of NATO countries have been engaged in numerous military operations in various parts of the world. Therefore combat and peacekeeping operations have been conducted in different geographic, climatic and cultural conditions. A significant part of these operations took place in urban areas often occupied by a combination of non-combatants and hostile forces [1].

The success of a military operation depends on a number of factors, including Situational Awareness (SA) that supports the decision-making process. The SA is often split in three parts: perception of the elements in the environment, comprehension of the situation, and projection of future status. It is obvious that building SA increases the demand for the efficient delivery of information to the command system and exchange of information within this system, e.g., data from sensor networks or reconnaissance systems. Despite technological developments, i.e., more robust waveforms and wideband devices offering higher throughput, it is still very challenging to get reliable and high data rate wireless links in urban areas.

Besides, limited capacity of batteries powering hand-held and man-pack radios is another factor influencing dependability of wireless systems.

One of the main challenges in urban areas is that threats are more difficult to forecast and can occur almost anywhere, which means that large areas have to be monitored persistently. This can be achieved by means of large scale networks of wireless unattended sensors powered by energy harvesting sources.

Although many studies on Wireless Sensor Networks (WSN) have been carried out, they strongly focus on specific sensor network aspects, e.g. sensor technologies, data fusion algorithms, or a limited number of nodes in homogenous terrain. Moreover, these aspects are mostly implemented during the design phase, which makes the deployed network very static and thus unable to adapt to changes in the battlefield. Therefore, what seems to be lacking is a

This work is supported by the European Defence Agency under CONTRACT NO B 1486 IAP4 GP.

multidisciplinary approach to autonomously adapt a large network of sensors and energy harvesting resources at runtime (i.e. after deployment).

To address this problem, in 2021 the European Defence Agency initiated the project named Wireless sensor Networks for urban Local Areas Surveillance (WINLAS) [2]. The objective of the WINLAS project is to demonstrate how situational awareness of armed forces in an urban environment can be improved with the application of heterogeneous, autonomous, reconfigurable sensors.

The rest of the paper is organized as follows: related works (Section II), urban area scenarios (Section III), system architecture (Section IV), system components (Section V) summary and future works (Section VI).

II. Related Works

WSNs are defined as self-configured and infrastructure-less wireless networks that enable the observation of physical or environmental conditions and the direct transfer of information over the network to the sink where information is usually visualized and analysed. The application areas of WSNs are very wide [3].

An overview of defence applications of WSNs was presented in [4], [5]. The operational context of modern military engagement has been divided into four scenarios: battlefield, urban, other-than-war and force protection. These scenarios were a starting point to define the requirements and limitations for WSN applications. The types of sensors and their capabilities determine and limit the use of WSN in defined scenarios, as presented in Table I.

TABLE I. Classes of Military WSN Applications [4]

Sensor types	**Operation scenario**			
	Battle-field	**Urban**	**OTW**	**Force protection**
Presence/ Intrusion	SHLM, AAP	SDT	-	SHLM, AAP, SDT
CBRNE	RCS	-	VDM	VDM, RCS
Ranging	-	EARS, INS	BL, INS	EARS, BL, SDL, PP
Imaging	ASW	SDL, MCM	-	SDL, MCM, PP
Noise	-	ATS	ATS	ATS

Abbreviations used in Table I [4]: AAP: Aerostat acoustic payload for transient detection; ASW: Low-cost acoustic sensors for littoral anti-submarine warfare; ATS: Acoustic threatening sound recognition system; BL: Time difference of arrival blast localization using a network of disposable sensors; SDT: Soldier detection and tracking; CBRNE: Chemical, Biological, Radiological, Nuclear and Explosive; EARS: Early attack reaction sensor; INS: Inertial Navigation System; MCM: Novel optical sensor system for missile canisters continuous monitoring; OTW: Other Than War; PP: Perimeter protection; RCS: A low-cost remote chemical sensor for E-UAV platforms; SDL: Sniper detection and localization; SHLM: Self-healing land mines; VDM: Chemical, biological, and explosive vapor detection with micro cantilever array sensors.

The performance of the military WSNs application depends on many factors, including sensor capabilities, type of sensors, the wireless communication architecture, its range and appropriate data processing [5], [6].

In [7] authors focused on military requirements for flexible wireless sensor networks. The following aspects were taken into account: actual costs per node, the current mode of deployment (mainly manual network set-up) and physical size. Their conclusion was, that only limited existing products meet the current military requirements, as WSNs are composed of larger sensor devices and consist only of small numbers of nodes. The authors highlighted that the dimensions and weight of sensors have to be kept as small as possible. Moreover, the current trend in the development of sensors is to get disposable and cheap devices [8] that can be applied in large quantities. Some types of sensors have to be able to discover their neighbourhood and to automatically create the wireless network [14]. Although the sensor network primarily is considered to be static, it has to be able to detect and adapt to changes of the topology, e.g., node disappearance [12]. For most of operations, the WSN is supposed to cover an area of the size ranging from 5 km^2 to 20 km^2 [5], [7]. The communication range of a single sensor should amount to a few hundred meters. Both the number and the density of sensors will most likely increase significantly in the future [9]. An important aspect is also the arrangement of the sensors in a given area. The placement of the sensors may affect the quality of the results obtained [10], [11].

In literature energy efficiency is noted as one of the key issues for WSN, because sensor nodes have limited energy sources (batteries) [15]. Solutions that enable obtaining energy from the environment to power the sensors are also proposed [16], [17].

It is assumed that the communication chain will be composed of sensor nodes, gateway(s) and the sink. Although bi-directional transfer is supposed, the majority of information will flow from the sensor node to the gateway. Data rates depend on the type of sensors and thus may vary significantly, from low data rates for pressure sensors to high rates for cameras. Moreover, WSNs are expected to provide reliable communication resistant to detection and interception or intentional jamming and interferences from other WSNs [13].

To achieve the goal of the WINLAS project a novel comprehensive approach is required, that integrates all of the following aspects:

- Modelling of various devices for obtaining energy using e.g. vibration, motion, and piezoelectricity; and managing network communications with consideration of different network topologies, energy-dependent routing strategies, and network traffic load calculations.
- Modelling and management of heterogeneous sensors, including optical, infrared (IR), radar, life signs, and chemical, biological, radiological and nuclear (CBRN) sensors.
- Techniques for combining distributed sensor data for use in urban environments, including all aspects of network security for data transfer and authorization for secure information exchange.
- Networking of a large number of heterogeneous energy sensing and harvesting devices to provide condensed information to Command and Control (C2), with particular emphasis on autonomous adjustment to avoid human intervention.

III. Scenarios

An urban area in the centre of Poland has been chosen to visualise scenarios and define the topology (Fig. 1). The area is characterised with the following attributes: a) part of the city with approx. 12 000 of citizens and an area of approx. 6 km^2; b) the city is surrounded by flat plains to the south and highlands to the north; c) the river flows through the city from the north-east to the south-west; d) the city-centre is a dense urban area with high buildings; e) low and medium-height buildings prevail in the suburbs; f) an industrial area is located to the north of the city (power plant, small and medium factories); g) an airport is located to the south of the city; h) the nearest village is located by the river at a distance of 3 km from the city (north-east). The topology has been extended with further information on weather conditions and available capabilities for the WINLAS concept. Capabilities include sensors or sensor nodes, platforms and armed forces. The capabilities primarily have been based on what is available within the WINLAS consortium at present. However, the list could be extended if more would be available.

Fig. 1. WINLAS area for scenarios.

Finally, all scenarios are described as joint missions involving capabilities from two different countries. The threats and the available capabilities have been varied between scenarios. An overview of the scenario visualisations is shown in Fig. 2.

Four scenarios have been defined:

- a reconnaissance scenario with the aim to confirm that the urban area is safe to enter (no red forces present in the area) and in case of a residual threat to identify, localise and monitor the threat,
- a surveillance scenario with the aim to protect critical infrastructure and in case of detection of suspicious activities to track the potential red forces and intervene, if necessary,
- a patrol scenario with the aim to detect and localise suspicious activities in an area of interest, to track the potential red forces and to intervene if necessary, additionally to extract a person (e.g., evacuate coalition services' informer),
- a convoy scenario with the aim to escort a humanitarian aid from the airport to the designated location in the urban area and in case of suspicious activities to track the potential red forces and intervene if necessary.

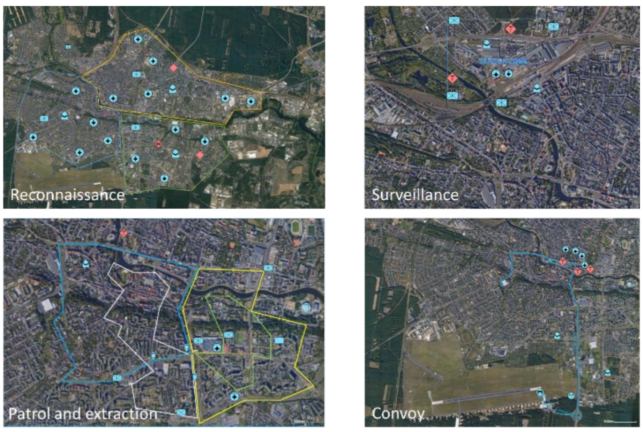

Fig. 2. Visualisation of the four working scenarios.

IV. System Architecture

A. Reference Architecture

In literature the typical architecture of the WSN consists of sensing nodes connected seamlessly through a gateway and the existing network to the sink. It is assumed that the sink receives, stores and processes data from sensors. In military solutions, where the network must be autonomous, the tactical communication backbone is used as the network infrastructure and the C2 software plays the role of the sink. Notice that in WINLAS system we use the name Battlefield Management System (BMS) that is the extended C2 software.

To get a comprehensive view of the system we considered its physical and functional architecture. The physical architecture of the WINLAS system is presented in Fig. 3. The main components are: BMS, the Communication backbone and the Sensing component.

The *BMS* is a software tool composed of the C2 core and a set of new subcomponents that are application specific.

The *Communication backbone* is defined as a backbone network consisting of backbone nodes and gateways with the tool providing management capabilities.

The *Sensing component* is created by a set of sensing devices.

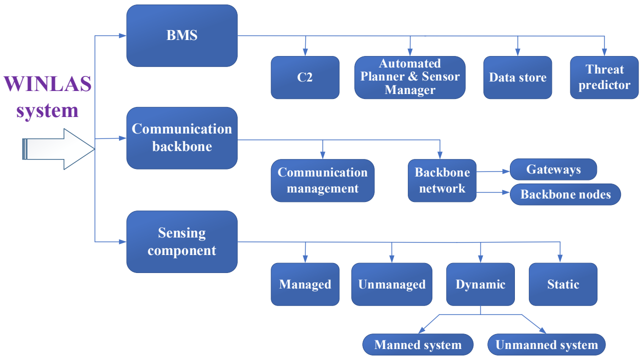

Fig. 3. System architecture – physical view.

The WINLAS system functional architecture is composed of the following main components: Information exchange, Plan and execute and Build situation awareness.

The *Information exchange* component provides the following functionalities: a) Authentication; b) Authorization; c) Data storage; d) Data distribution; e) Communication management, e.g. setting frequency channels or transmitted power levels; f) Sensor management, e.g. setting of threshold values of the sensors; g) Asset control, e.g. autonomous or remote control of an asset; h) Situation picture distribution.

The *Plan and execute* component provides the following functionalities: a) Plan mission, e.g. route/motion/path planning of platforms and the use of sensors; b) Execute mission, e.g. sensing and collecting data; c) Monitor mission plan; d) Re-planning, e.g. new threat identified; e) Monitor communication backbone; f) Monitor asset/sensor state, e.g. the level of battery; g) Harvest energy.

The *Build situational awareness* component provides the following functionalities: a) Sensing; b) Detection; c) Classification, e.g. the discrimination between a person, a car or a truck; d) Identification; e) Localization; f) Tracking; g) Object fusion; h) Potential threat detection; i) Threat analysis, e.g. RCIED, saboteurs; j) Threat prediction, e.g. RCIED explosion, sabotage; k) Situation assessment.

B. Information Flow

Based on the system architecture described above and our experience in the area of automated command systems, below we present the presumed information flow for the WINLAS system. This information flow includes all types of data exchanged between system elements: a) C2 system data; b) Sensing data; c) Management data (telemetry data - dynamic sensors, control and configuration data, status and health state).

The information flow inside each component of the WINLAS system and between elements of different components is shown in Fig. 4.

The C2 component, due to its hierarchical nature, encompasses the entire system from the high level (HQ) to the level of the local operator of a single asset or a dismounted soldier. Depending on the operational scenario lower level C2 instances may have limited functionality, i.e. only C2 Core function.

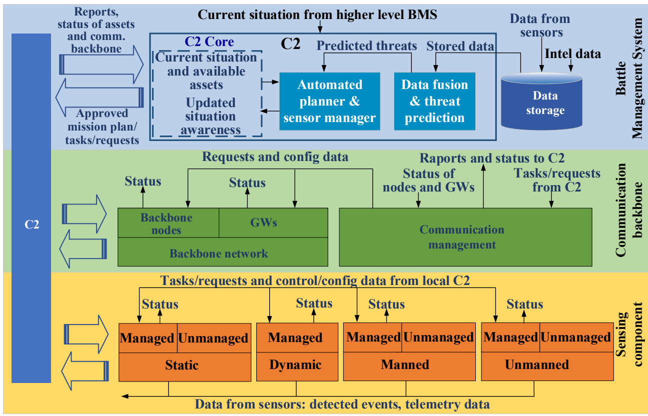

Fig. 4. Information flow.

The information flow between the *C2 instances* of the whole WINLAS system is as follows: a) Approved mission plan (for commanding staff); b) Tasks (for assets); c) Requests (e.g. to get the asset status or health parameters); d) Situation awareness; e) Reports; f) Status of assets and communication backbone.

The information flow within the *BMS component* includes: a) Current situation picture - to the Automated Planner & Sensor Manager; b) Available assets - to the Automated Planner & Sensor Manager; c) Stored data - from Data storage to the Data fusion & threat predictor; d) Predicted threat - from the Data fusion & threat predictor to the Automated Planner & Sensor Manager; e) Updated situation awareness - from the Automated Planner & Sensor Manager.

The information flow to the *BMS component* covers: a) current situation from higher level; b) C2 data from lower levels, e.g. reports, status, telemetry data; c) data from sensors to the Data storage; d) data from INTEL to the Data storage.

The information flow to/from/within the *Communication Backbone* component comprises of: a) Tasks / Requests - from C2; b) Reports / Status - to C2; c) Requests - to Backbone nodes and GWs; d) Config data - to Backbone nodes and GWs; e) Status - from Backbone nodes and GWs.

The information flow to/from/within the *Sensing component* includes: a) Tasks / Requests - from C2; b) Control data / Config data - from local C2; c) Status - from assets; d) Detected events / Telemetry data - to C2/BMS.

V. SYSTEM COMPONENTS

A. Sensing Component

The sensing component consists of different types of sensors that provide information needed to create and update the situational picture. A selection of those available within the WINLAS consortium are described below.

Radiomonitoring sensor will be used for spectrum situation awareness building [18], [19], [20]. It is a dedicated device, which means a receiver for spectrum monitoring placed on a soldier or platform, e.g., an Unmanned Aerial Vehicle (UAV) or Unmanned Ground Vehicle (UGV). Software defined radio (SDR) hardware is selected for the implementation. Energy Detection (Estimated Noise Power – ED) is proposed as a radio signal activity solution because of implementation simplicity and low requirements regarding computational power [21]. The authors suggest to use emulation (for Data Fusion purposes) of waveform identification for the Friend, Foe, Neutral (FFN) difference to support Red Force Tracking (RFT) or Blue Force Tracking (BFT) functionalities/services. As a hardware platform SDR USRP B200 mini with frequency range from 70 MHz to 6 GHz and 20 MHz bandwidth was selected. Integration with UAV platform (DJI Mavic 3 Cine) and microcomputer (Raspberry Pi4) is proposed for a complete radiomonitoring sensor (Fig. 5) as a flexible device that can increase mobility and spectrum monitoring range/coverage area [22].

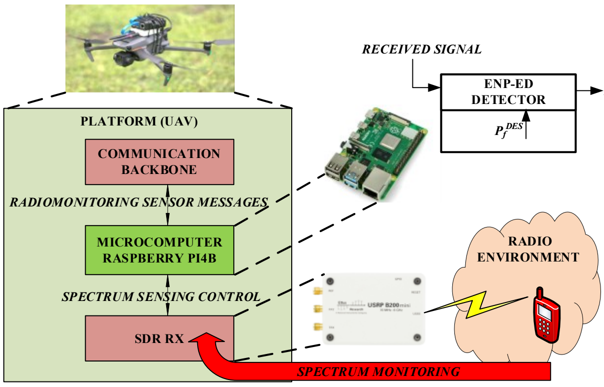

Fig. 5. Radiomonitoring sensor diagram and hardware used for the development.

From WINLAS architecture point of view the radiomonitoring sensor as a “Sensing Component” is of the managed sensor type and can be static or dynamic and manned or unmanned.

The radiomonitoring sensor will be integrated into WINLAS with the following parameters: a)frequency to monitor in [MHz]: single or frequency list, b) bandwidth in [MHz] for detection (IQ sampling) on the radio frequency: not more than 20 MHz, c) time of measurement [s] for each frequency (might be the same for the whole list or defined independently), d) monitoring period [s]: what is the period for the radio monitoring process, if “0” continuously, e) result type: hard/soft/IQ samples, desired false alarm selection for hard and soft detection, f) FFN identification, g) how many last stored results shall be sent back to the BMS.

The acoustic-seismic sensor combines two detecting systems. The device is encased in a durable IP55 casing and has been tested in temperatures ranging from -10 to + 40 Celsius degrees. The sensors' ability to function regardless of lighting conditions by utilizing sound waves and ground vibrations is to be of a significant advantage for the system.

The seismic component of the sensor can detect ground vibrations generated by moving vehicles or people. It is embedded in the ground to transmit soil vibrations using acceleration sensors. Its detection algorithms are threshold-based with noise filtering to reduce external noise, such as rain droplets.

The detection method of the acoustic component is based on collecting surrounding noises, filtering them out, then recognizing and categorizing any unusual sound occurrence. To make the most of this method, a trained neural network is constructed to categorize events such as the passing of wheeled vehicles, general human activity (within a small radius), and discharged gunshots (larger radius).

Other components inside the sensing subsystem in the WINLAS project are the CBRN sensors that include:

- Gas Detection Array – Personal (GDA-P), based on Ion Mobility Spectrometer (IMS) H2O chemistry and Electrochemical Cell (EC),
- Gas Detection Array – Personal (GDA-P), based on IMS NH3 chemistry and Photo Ionization Detector (PID),
- AP4C - Flame Photometric Detector (FPD).

The integration of several detection methods enables the identification of a vast array of chemical compounds. In light of this, a deployment strategy was implemented that involves the utilization of two distinct sensor types, namely GDA and AP4C, as well as two types of GDA devices that employ different supporting technologies (EC and PID) and are based on varying chemistry. This approach has been adopted to augment the system's data filtration capabilities and improve the precision of identification. The aforementioned sensors are intended to be integrated into a singular sensor node, which will collect and refine sensor data prior to transmitting it to WINLAS' BMS. In order to achieve internal integration a module called translator was developed. This module is affixed to individual sensors and facilitates additional wireless communication with the sensor node. The ESP32-based module acts as both a gateway between sensor and node (CBRN sensors) and a primary filtering unit (seismic module).

The fundamental step in the sensor network design is consideration of the transmission medium. Many of the Internet of Things (IoT) devices and sensors are majorly resource-constrained hindering ubiquitous adoption in various applications, including environmental monitoring, tracking animals, monitoring some physical parameters of a person, etc. The current IoT devices are energy constrained since they use batteries or harvest energy in tiny amounts. They often are deployed in places where the battery cannot be replaced. Further, the devices have to be low cost thus, computation power would be very much limited. Since these devices cannot have sophisticated protocols running they need to be as simple as possible. Further, the requirement for the range is also huge, often multiple kilometres. Any sophisticated MAC protocol using channel sensing consumes a large amount of energy and is computationally demanding; this leads to draining the batteries [27], [28]. Low Power WANs (LPWANs) can guarantee energy-efficient communication using hopping techniques. Long-range and efficient communication requiring minimal amounts of energy for small payloads is established with a single hop spending not more than a few hundred micro-watts.

LoRa is a new low-power and long-range communication protocol. LoRa uses a Chirp Spread Spectrum (CSS) modulation scheme that is robust towards noise and interference, see Fig. 6. LoRa offers 50 kbps rate at ranges of up to 10 km-40 km, depending on the environment (urban/rural) requiring a maximum of 27 dBm of transmission power [29]. In contrast, 2G-4G consumes 800x higher power. LoRa has multiple Spreading Factor (SF) which is the rate at which the frequency reaches from its lowest value to its highest. The spreading factor is defined by a value from 7-12.

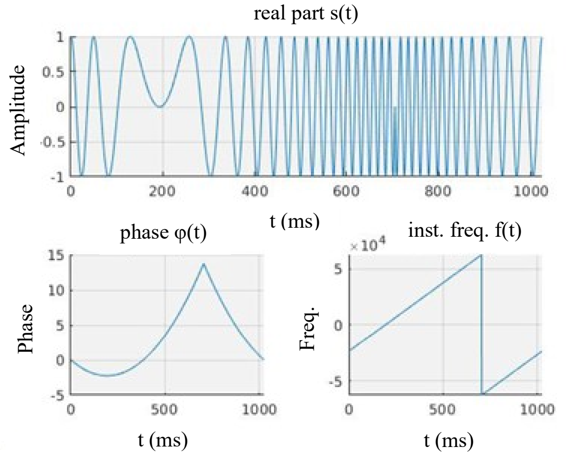

Fig. 6. CSS Waveform, phase, and instantaneous frequency of LoRa chirps [30].

A network involving LoRa nodes using a LoRa physical layer communication is called Long Range Wide Area Network (LoRaWAN) which offers easy deployment, and operational longevity to energy-constrained IoT devices. The IoT devices communicate in a best-effort fashion in extended ranges. Because of the CSS, the range of the LoRa can be in terms of kilometers and thus a Gateway can serve a large area. The deployment, the protocol, and the operation are very simple since LoRaWAN uses the simple ALOHA-like design of the MAC layer. The architecture of the LoRaWAN is shown in Fig. 7. The LoRa-based IoT nodes transmit the LoRa frames to the Gateways and multiple gateways can receive the frame. The gateways then decode the frame and send the data from the frames to the network servers that are accessed by application servers and then users. In our case, the gateways, network servers, and applications could be running on the same system. The single sensors could use LoRaWAN to directly send information to the command centre.

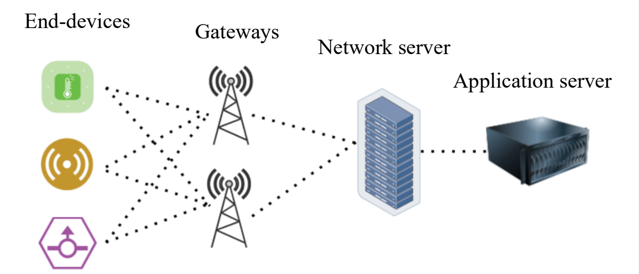

Fig. 7. LoRa Network Architecture.

Robust communication with LoRaWAN is ensured by the CSS, the MAC being ALOHA-like and multiple gateways receiving the frames. However, the lack of any central controller for managing the traffic can results in the packet collision rate being high in dense LoRaWAN deployments with high traffic loads.

B. *Communication Backbone*

Wireless communication in urban areas is always a challenge for planners of the system and for commanders. There have been many NATO and EDA projects addressing this problem [1], [23], [24], [25]. The main conclusion is that there are no universal solutions fitting all kinds of scenarios. The organization of the communication backbone always depends on a given operational goal and the circumstances, like terrain, opposing forces capabilities or jamming. The communication system has to be reliable and work efficiently despite the dynamics and unpredictability of the conducted operation.

Different types of star-shaped network topologies are analysed for the WINLAS project, as presented in Fig. 8.

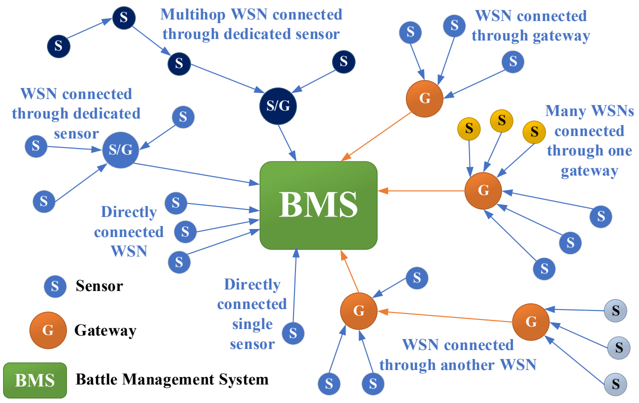

Fig. 8. Types of the star-shaped topologies.

Directly connected single sensor is the simplest variant of the WSN network. The main assumption in this variant is that the sensor uses the same type of radio device for wireless communication as is used by the receiving centre to communicate with other elements e.g., armoured vehicles.

Directly connected WSN is a typical variant of the previous case, where the WSN network is enriched with more sensors. As a result, a significant increase in the traffic load of a network can be expected. It can lead to congestion in the network and problems delivering information to the recipient.

WSN connected through dedicated sensor. When a dedicated sensor node is in an advantageous location and acts as an intermediary, it is possible to increase the range of communication between the WSN network and the receiving centre. Intermediary nodes must have a memory to store and forward information. If sensors or a receiving centre move, an intermediary node may be replaced by another intermediary node. This can be a part of the planning dynamics dependent on a change in operational situation.

Multi-hop WSN connected through dedicated sensor enable a significant increase in the range of wireless communication, especially in urban operations. The intermediary nodes in the WSN must have the functionality of a router and a memory to store and forward information. In the case of multi-hop topology, a so-called hidden node can pose problems. It manifests itself as the occurrence of collisions (interference) in a situation when two sensor nodes outside the mutual wireless communication range try to transmit to the same common intermediary node. In the absence of access control or receipt confirmation mechanisms the information coming from both sensors will be lost.

WSN connected through gateway is the most popular type of the communication between WSN and receiving centre (commander). Most wireless sensors manufacturers provide their devices with a dedicated hub that communicates with the sensors via a radio link, while having a wired connection with the receiving centre.

Many WSNs connected through one gateway. In case of the same type of radio link in each WSN the gateway node and sensors should have implemented some collision avoidance mechanism in the physical layer. In case of different types of radio links in each WSN the complexity level of the gateway will grow with the increase in the number of WSN served, because each WSN will have to have its own transceiver in the gateway. Additionally, data flows from different WSN will compete for access to the radio uplink from the gateway to receiving centre (commander). Some QoS mechanisms should be implemented in the gateway.

WSN connected through another WSN. This type of topology allows individual wireless sensor networks to be connected in a chain, thus significantly increasing the range of communication with remote sensor networks. However, it should be remembered that linking networks in a chain leads to the so-called snowball effect. It manifests itself in an increase in the amount of information sent on each span of the chain, leading to overloading of links in the sections closest to the receiving centre (commander).

In addition to the star-shaped topologies shown above, *mesh topologies* were also considered in the project. Mesh connections between sensors and commander (receiving centre) enables a significant increase in the area covered by the many wireless sensor networks. There is also a hidden node problem as in the multi-hop topology described above. This type of network requires that individual nodes have implemented routing mechanisms.

C. *Battlefield Management System*

Mission Planner

The WINLAS BMS is the system in which information from the sensor network will be integrated to support the command and control of the military unit at hand. In the core of the BMS there is an Automated Planner (AP). Planning is the area of Artificial Intelligence (AI) that computationally studies the deliberation process of creating a plan [26]. That process consists of selecting a sequence of actions that meet one or more goals and a set of constraints imposed by the domain. Planning is the reasoning side of acting. When acting (or executing a process), we need to decide how to perform the chosen activities while reacting to the environment where they are taking place. Each action in the plan can be seen as an abstract task that needs to be refined into sub-actions or commands that are more concrete.

There are several ways to handle partially observable, nondeterministic, and unknown environments. We have sensorless planning (also known as conformant planning) for environments with no observations; contingency planning for partially observable and nondeterministic environments; and online planning and replanning for unknown environments. This last approach is the one that will be followed by the BMS.

In any of the mentioned cases, it is important to make the distinction between domain dependent and domain independent planning. For some type of problems, domain specific planning methods have been developed that are tailor-made for that kind of problem. However, for the BMS we have focused on domain independent planning.

Fig. 9 shows the structure, inputs and outputs of a domain independent planner. The left part shows the Knowledge Representation (based on descriptive models) with two inputs: the domain with the description of the actions based on preconditions and postconditions, and the problem with the description of the Initial State (IS) and goals. In the middle part of the figure is the search process. Before searching for a solution there is a validation program to syntactically check that the syntax of the domain and problem files are correct as well as the logic or procedural inferences. All the algorithms defined in this part are domain independent to comply with AI principles. Finally, on the right side, is the solution, that can be an ordered sequence or parallel actions plan. It may also not find a solution (failure) based on the domain model definition and/or the problem provided to the planner and refer back to the operator.

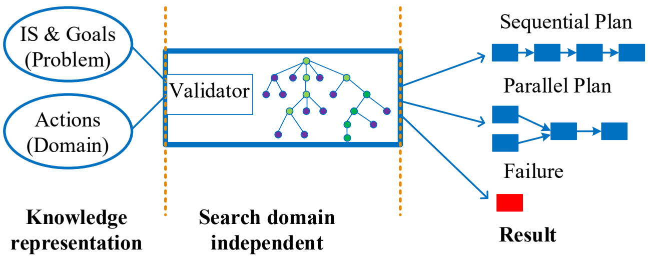

Fig. 9. Components of an AI automated planner.

Situational Awareness

All the information about the sensor's status will be translated into the initial state of the AP as well as a probability distribution on where for example, the red forces are moving (this can determine the setting of new goals dynamically), Fig. 10.

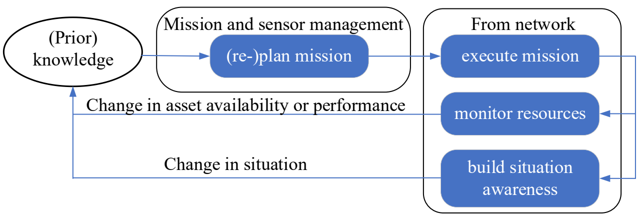

Fig. 10. Situational awareness function in the WINLAS system.

The state of the preconditions of each action and the expected effects will be checked to assess whether anything in the outside world has changed. In case the preconditions or postconditions do not hold, the AP will replan or explore the possibility of repairing those parts of the plan that could be affected by the changes on the preconditions or postconditions. Then, the user can define the goals or some goals may be inferred from the information gathered by the sensors.

VI. Summary and Future Works

The WINLAS project is still in progress. Until now the following topics were covered: scenarios, requirements for the system and the reference architecture of the system. The following tasks are being developed: communications management, energy harvesting, development and integration of sensors, development of the mission manager. Below we shortly refer to each task.

Communications Management

The main goal of communications management is to work out recommendations for the mission manager. This task requires extensive simulations and analysis of results. The following constraints related to the communication backbone have been identified.

Broadband UHF radios enable high data rate transfer for the distance up to a few kilometres in LOS conditions. In urban areas this distance may be significantly reduced, which may result in unstable or broken communication links between vehicles. One possible solution to avoid such a situation is the deployment of a relaying node. Depending on the scenario, the role of the relaying node can play one of the recon vehicles that is strategically located or a dedicated drone. If the drone cannot be launched, e.g., in case of unfavourable weather conditions, a manpack radio deployed on a high building may relay the data between vehicles.

Narrowband VHF radios offer voice service or low throughput data links for the distance up to 25 kilometres in LOS conditions. Although in urban environment the VHF radio network may intermittently suffer from short-breaks or wireless links may be of poor quality, it is considered that voice services and short messages like BFT will be supported.

Communication with a UAV requires LOS conditions to get a high throughput data link, e.g. to transfer a videostream or high quality pictures, and have a reliable control link to manage the drone, e.g., (re)task, report the battery status or current flight parameters. In military solutions, a wireless connection with a tactical drone is provided in one of the military bands. Currently offered solutions of such wireless systems cover a wide frequency range from 200 MHz to 6 GHz. Note, that the frequency sub-bands within the band 4.4 GHz – 4.8 GHz are commonly used for this purpose.

In case of wireless sensors, communication links depend on the distance, local conditions (obstacles) and the type of a sensor. Videostreams or high quality pictures can be sent from the camera to the recon vehicle only in LOS conditions. Short messages such as alerts, alarms or telemetry data can be exchanged in NLOS conditions, assuming that there is a dedicated relaying node or that the group of sensors operates as a WSN with routing mechanisms.

Development of Sensors

During the WINLAS project, a sensor node is developed whereby individual sensors, connectors, and nodes are integrated into a unified entity that can function autonomously and generate data that is not attributable to other system components. The internal network of the sensor node can be expanded by incorporating diverse types of sensors. In the event that an extension of the system is required, the open design utilizing a robust sensor node and translator modules as connectors has the capacity to accommodate additional sensing units.

Development of the Mission Manager

One of the essential preconditions provided to the mission manager are results of the wireless system simulations which show constraints in the deployment of sensors and vehicles from the point of view of the communication manager. The optimal way to combine this type of data into mission planning process is being developed.

Other work concerns modelling of the mission with a description of the initial states and mission goals. In the next step, a suitable mission plan is created automatically to achieve the mission goals. The planner selects the appropriate set of assets, i.e., sensors and platforms for a given plan. Further works will focus on the development of mechanisms for automatic assignment and transfer of tasks to individual sensors and platforms. A UAV equipped with the camera is a typical example of such a set of platform and sensor that is foreseen for the first phase of tests. The other types of sensors will be applied in next phases of the WINLAS project.

ACKNOWLEDGMENT

The authors would like to thank Mrs. Yolanda Rieter-Barrell for useful advices, suggestions and final proofreading.

REFERENCES

[1] RTO Technical Report TR-IST-067, Technical Communications in Urban Operations. Report documents the Findings of Task Group IST-067. Published September 2010.

[2] I. Montiel-Sánchez, “Defence Internet of Things (dIoT). The way ahead,” European Defence Matters, A magazine of the European Defence Agency, Issue 14, 2017, p. 15.

[3] L. Gashi, A. Luma, and Y. Januzaj, “The integration of Wireless Sensor Networks, Mobile Networks and Cloud Engineering for a decision support system - A Systematic Literature Review,” 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 2022, pp. 1-8.

[4] M. P. Durišić, Z. Tafa, G. Dimić, and V.Milutinović “A Survey of Military Applications of Wireless Sensor Networks”. MECO-2012 Bar, Montenegro.

[5] A. Ali, S.A. Changazi, Y. K. Jadoon, and M. Quasim “Military Operations: Wireless Sensor Networks based Applications to Reinforce Future Battlefield Command System”. 2020 IEEE 23rd International Multitopic Conference (INMIC). Bahawalpur, Pakistan.

[6] S. Pragadeswaran, S. Madhumitha, and S. Gopinath, “Certain Investigations on Military Applications of Wireless Sensor Networks,” International Journal of Advanced Research in Science, Communication and Technology (IJARSCT) Volume 3, Issue 1, March 2021.

[7] M. Winkler, K.-D. Tuchs, K. Hughes, and G. Barclay, “Theoretical and practical aspects of military wireless sensor networks,” in Journal of Telecomunications and Information Technology, 2/2008, pp. 37-45.

[8] S. R. Boselin Prabhu, M. Pradeep, and E. Gajendran, “Military applications of wireless sensor network system,” A Multidisciplinary Journal of Scientific Research & Education, Volume: 2, Issue: 12, December 2016.

[9] M. Suchański, P. Kaniewski, J. Romanik, E. Golan, and K. Zubel, “Radio Environment Maps for Military Cognitive Networks: Density of Sensor Network vs. Map Quality,” (2019). In book: Cognitive Radio-Oriented Wireless Networks (pp.195-207).

[10] M. Suchański, P. Kaniewski, J. Romanik, E. Golan, and K Zubel, “Radio Environment Maps for Military Cognitive Networks: Deployment of Sensors vs. Map Quality,” In Proceedings of the 2019 International Conference on Military Communications and Information Systems (ICMCIS), Budva, Montenegro, 14–15 May 2019; pp. 1–6.

[11] K. Junosza-Szaniawski, D. Nogalski, and P. Rzążewski, “Exact and Approximation Algorithms for Sensor Placement Against DDoS Attacks,” International Journal of Applied Mathematics and Computer Science, vol.32, no.1, 2022, pp.35-49.

[12] A. Zhuk, V. Romaniuk, E. Stepanenko, and A. Romaniuk, “Methodology of the tactical wireless sensor networks control,” 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv-Slavske, Ukraine, 2018, pp. 1047-1050.

[13] S. Laitrakun and E. J. Coyle, “Collision-aware distributed estimation in WSNs using sensor-censoring random access,” MILCOM 2015 IEEE Military Communications Conference, Tampa, FL, USA, 2015, pp. 1039-1045.

[14] G. You and Y. Zhu, “Structure and Key Technologies of Wireless Sensor Network,” Cross Strait Radio Science & Wireless Technology Conference (CSRSWTC), Fuzhou, China, 2020, pp. 1-2.

[15] N. Mohammad, S. Muhammad, A. Bashar, and M. A. Khan, “Design and modeling of energy efficient WSN architecture for tactical applications,” Military Communications and Information Systems Conference (MilCIS), Canberra, ACT, Australia, 2017, pp. 1-6.

[16] P. Mohan and N. M. R, “Ranking of Sensor Nodes by Optimizing Sensor Data in Energy Harvesting Wireless Sensor Network,” IEEE International Conference on Data Science and Information System (ICDSIS), Hassan, India, 2022, pp. 1-6.

[17] M. T. Le, V. D. Ngo, P. T. Duong, V. T. Tran, and Q. C. Nguyen, “Dual-Band Funny-Face Wi-Fi Energy Harvester for Indoor Battery-less Wireless Sensor,” 4th International Conference on Smart Sensors and Application (ICSSA), Kuala Lumpur, Malaysia, 2022, pp. 1-4.

[18] K. Malon “Dynamic Spectrum Access in Ad-Hoc Radio Networks with Cognitive Nodes” Military University of Technology: Warsaw, Poland, 2021; ISBN 978-83-7938-327-6.

[19] P. Skokowski, “Electromagnetic Situation Awareness Building in Ad-Hoc Networks with Cognitive Nodes”; Military University of Technology: Warsaw, Poland, 2021; ISBN 978-83-7938-323-8.

[20] P. Skokowski, K. Malon, and J. Łopatka, "Building the electromagnetic situation awareness in MANET cognitive radio networks for urban areas", Sensors, vol. 22, no. 3, pp. 716, Jan. 2022

[21] P. Skokowski, K. Malon, and J. Łopatka, "Properties of centralized cooperative sensing in cognitive radio networks", Proceedings of SPIE 10418 2016 XI Conference on Reconnaissance and Electronic Warfare Systems (CREWS), vol. 10418, pp. 1041807, Apr. 2017.

[22] K. Malon, P. Skokowski, and J. Lopatka, “Optimization of wireless sensor network deployment for electromagnetic situation monitoring,” International Journal of Microwave and Wireless Technologies, 10(7), pp. 746 – 753, 2018

[23] RTO Technical Report. (February 2009). Command and Control Challenges in Urban Operations. Final Report of Task Group IST-046 / RTG-008.

[24] RTO Technical Report 71. (April 2003). Urban operations in the year 2020. Report by the RTO Studies, Analysis and Simulation Panel Study Group SAS-030.

[25] European Defence Agency. (September 2010). Wireless robust link for urban force operations. Contract A-0692-RT-GC “WOLF”.

[26] G. Malik, D. Nau, and P. Traverso, (2016). Automated Planning and Acting. Cambridge University Press.

[27] T. R. Park, T. H. Kim, J. Y. Choi, S. Choi, and W. H. Kwon. “Throughput and energy consumption analysis of IEEE 802.15. 4 slotted CSMA/CA”. In: Electronics Letters 41.18 (2005), pp. 1017–1019.

[28] R. Bruno, M. Conti, and E. Gregori. “Optimization of efficiency and energy consumption in p-persistent CSMA-based wireless LANs”. In: IEEE Transactions on Mobile Computing 1.1 (2002), pp. 10–31.

[29] Semtech. LoRa® wireless RF products. https://www.semtech.com /products/wireless-rf/lora-transceivers/sx1261.

[30] Maria Teresa Blanco Abad, Designing and implementing SFMAC: A MAC protocol for LoRa networks for efficient use of unlicensed bands, MSc Thesis, Delft University of Technology.