UAV-based Sensor Networks for Future Force Warriors

Jorma Jormakka
Department of Military Technology
National Defence University
Helsinki, Finland
jorma.o.jormakka@kolumbus.fi

Tapio Saarelainen
Department of Military Technology
National Defence University
Helsinki, Finland
tapio.saarelainen@mil.fi

***Abstract* - The Future Battlefield Commander relies on Command, Control, Communications, Computers, Information, Intelligence (C^4I^2) tools to perform optimally in his given tasks in versatile and hostile environments. The concept of war has changed from traditional wars to the asymmetric wars. This article presents a new networking concept for sensor networks, the Wireless Polling Sensor Network (WPSN) for the Dismounted Future Warrior. The WPSN comprises a small ad hoc network of mobile Unmanned Vehicles (UVs), and a fixed set of sensor nodes that continuously survey the area. The UVs move along pre-planned routes and poll the sensors. The article briefly describes the Future Warrior system, presents the WPSN solution, and explains the main use cases of the WPSN concept: road-side bomb detection, location service in built-up areas, and marking a target by Special Operations units. An evaluation of the advantages and disadvantages of the proposed WPSN concept is given; and a provably computationally secure crypto-protocol between base stations and other nodes, such as UAVs, is presented. The main output of the paper offers WPSN solutions together with SCPAs and UVs to attain the maximum performance at all warrior levels.**

Keywords - Wireless Sensor Network; Future Warrior; Situation Awareness, UAV, cryptology, One-Time Pad (OTP).

I. INTRODUCTION

This article describes a new concept called the Wireless Polling Sensor Network (WPSN) to be used in the Future Warrior gear. It comprises sensor nodes that are not networked with each other but communicate with a mobile ad hoc network of a small number of Unmanned Air Vehicles (UAVs), also called drones. The article presents the motivation and some applications of the concept. The article is an extended version of a paper [1] presented in the ICDT conference in 2010 and in addition to material from [1], it includes an evaluation of the basic concept of the proposed UAV-sensor network solution, and presents a new crypto-protocol based on exchanging One-Time Pads, used between base stations and other nodes of the proposed system. The crypto-protocol has appeared earlier in the departmental preprint series [2] but has not been published.

The main setting of the WPSN is the Future Warrior system. A warrior's electronic skeleton, shown in Fig. 1, is a backbone and a platform for implementing required electronic solutions to be used in modern warfare. The Wireless Polling Sensor Network is a part of a larger system of communication, navigation and positioning systems.

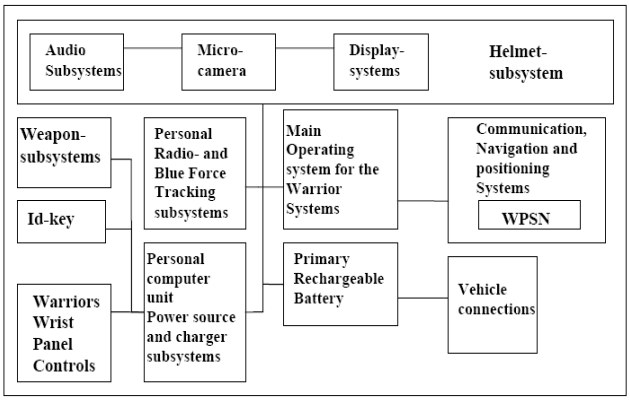

Figure 1. A Warrior's electronic skeleton.

Militaries search advantage in the future battlefield through novel solutions utilizing existing technologies and communication network systems and thereby enhancing the warrior efficiency. The main objective of these networks and technical solutions is to improve Situational Awareness (SA) [3] at all of the warrior levels in the decision-making process. Blue Force Tracking-systems (BFT) are an essential part of SA. They provide vital information for commanders in helping them to make better decisions and to avoid fratricide. Troops need to be constantly precisely located. It is crucial to improve the efficiency of dismounted operations with smaller and more capable units. The units require a great degree of flexibility and reliability in order to obtain their goals.

Future Warrior systems apply several levels of warriors from the least trained to the experienced commanders or the professionals of the Special Forces. Table 1 shows examples of different technical solutions that are needed at different warrior levels. Demands for the solutions are derived from the needs of the warriors at different levels according to their performance and tasks. The WPSN-system applications must be implemented into Future Warrior systems taking into account the different warrior levels.

One of the most important constraints imposed by the Future Warrior system is the maximum weight of any equipment in the warrior gear. For instance if a ground-based fixed sensor node has a mass can reach up to 10 kg the nodes

can be transported to the site by the Special Forces. The UGVs present a better payload platform, but they are significantly slower, and their control and communication systems need to be improved.

TABLE I. DIFFERENT WARRIOR LEVELS.

Warrior level	Basic Warrior	Squad / Platoon leader	The Company Commander	Special Force Soldier
Range for the systems (comms.)	up to 3 miles, WLAN / LAN, PTT-radio	up to 5 miles, WLAN / LAN, PTT-radio	up to 10 miles, WLAN / LAN, PTT-radio, SATCOM	up to 100 miles, WLAN / LAN, PTT-radio, SATCOM
Duties tasked	Defensive, offensive, reconnaissance	Defensive, offensive, reconnaissance + C4I2	Defensive, offensive, reconnaissance + C4I2	According to task
Demands for used solutions	Basic gear	Advanced gear and lightened C4I2	Gear for C4I2	According to task
Duration of operations	up to 72 hrs	up to 72 hrs	up to 72 hrs	up to 120 hrs
Military Operations in the woods	Yes	Yes	Yes	Yes
Military Operations in Urban Territory (MOUT)	Yes	Yes	Yes	Yes
Military Operations behind enemy lines	No	No	No	All
Hostage Missions	No	No	No	All
Rescue Missions	No	No	No	All
Need for fire support	No	No	YES	YES
Need for emergency evacuation in hostile territory	No	No	YES	YES

In order to motivate the WPSN concept, let us recall the typical structure of a Wireless Sensor Network (WSN). A WSN usually contains an ad hoc network of sensor nodes, a gateway node, and a control station. This results in problems with energy, security and in military applications of survivability. This type of a WSN loses connectivity when a sufficient number of nodes is removed or destroyed. It may also be too easily detected, and its life-time may be short and unpredictable. There are only few civilian applications available for ad hoc WSNs, such as applications for monitoring seismic and environmental changes. A more traditionally structured WSN comprises a base station and sensor nodes connected by wireless links.

Another motivation for WPSN we get from the present UAV systems for dismounted soldiers. UAVs bring a significant edge in the C^4I^2 environment as a new sensor and a relay platform but the present solutions are far from perfect. These systems have a base controller, a line-of-sight data link to the UAV and a relatively small UAV, typically equipped with a camera (Infra-Red or visual). Because of the line-of-sight requirement, they have a limited range and cannot be easily used in urban areas. Additionally, the camera does not see anything else than what is happening at the moment the UAV's camera surveys the area. A single small UAV has also a very small payload on the range of pounds [4].

The Wireless Polling Sensor Network (WPSN) is proposed as a solution to the problems of both the WSN and the small UAV systems. WPSN comprises a mobile ad hoc network of UAVs or UGVs with *1-n* nodes, *n* being a small number, and a set of fixed ground-based sensors. The network of UAV can operate as a multi-hop ad-hoc network in case it is motivated, for instance, by multi-sensor co-operation, or by a lack of a line-of-sight connection. A control station has a data link to a selected node of this mobile network. More than one node improves survivability in applications where nodes can be destroyed. The sensor nodes do not form a network but they are polled by a selected node of the mobile network. A possibility for this is created by adding a random-access event channel.

The WPSN solution has many advantages over the traditional WSNs: Polling can use sensor specific codes and security issues become easy. The fixed sensor nodes do not lose connectivity even if a high number of nodes are removed. The WPSN is a part of mobile mesh network systems operating in an environment of harsh propagation of channels and interference, frequent and rapid changes of network topology [5].

The need for a special gateway node, typical to a WSN, is removed: the fixed sensor nodes use directional antennas that only emit in the upward direction and an UAV polls them. The signal strength remains sufficient for a UAV on reasonable altitudes and the fixed sensor nodes are difficult to locate by ground-based measurements. The transmit antenna selection is a practical technique for achieving significant power gain, even with commodity hardware and without changes to the 802.11 protocols [6]. For example, field experiments have been conducted in which the network was based on the frequencies of 2,4 and 5,8 GHz, and also the 900 MHz frequency was used for the point to point mode [7]. The detection methods are based on motion, either seismic, or acoustic etc. The WPSN concept can use also in Unmanned Ground Vehicles (UGVs) instead of UAVs. In a UGV application, the fixed sensor nodes can, for example, be GPS pseudolites that an UGV installs [8]. The composition of this paper is as follows: Section 2 reviews the background work. Section 3 presents applications of UAV-based sensor networks and the overall evaluation of the concept. Section 4 concentrates on a provably computationally secure protocol between base stations and other nodes. Finally, Section 5 concludes the paper.

II. RELATED WORK

Several Future Soldier Programs are currently underway in various militaries, including the Finnish Army definition work contributing to its Future Warrior (Future Force Warrior, FFW) and its demands. The result involves defining the gear for each level of a Future Warrior. The critical solutions involve communicating, Situational Awareness (SA) and Command and Control (C2) information among highly dispersed battlefield units in a dynamic environment [3][9]. In fact, the US Army is fielding its new SA system known as Force XXI Battle Command and Brigade and Below (FBCB2) [9]. An extension of this is the Deep Green.

The need for UV-based sensor systems is clear. There are strict constraints on the weight and dimensions of equipment carried by a soldier and therefore it is essential for the Future Force Warrior (FFW) to be networked and to use external systems based on new innovations. One way of networking a soldier installing a high-bandwidth conformal antenna into the soldier's helmet with the coverage of over 750 MHz through a 2,7 GHz frequency band [10].

Systems that are very similar to the proposed WPSN, comprising a network of UVs and a fixed set of sensors, do not seem to exist yet. Presently UAVs are directly connected to a base station [11]. There are some experimental UAV networks [11][12]. UGV networks seem to be non-existing, while single UGVs are widely used e.g. by police forces. However, all technical elements of the WPSN solution are available. The novelty of the WPSN solution is not in technical elements but in the realization that the solution can fill certain currently critical military needs.

The WPSN system uses a mobile network of UVs. It can be considered as a Mobile Backbone Network (MBN) of a sensor network. A typical layout of a MBN is based on the Backbone network (Bnet), access nets (Anets) and regular (flat) ad hoc network(s) [13]. A Mobile Backbone Network Routing with the Flow Control (MBNR-FC) method is a known method to improve network throughput as well as the packet delay, the delay jitter and the loss ratio performance [14].

Possible solutions for tracking and location service have been searched from satellite positioning systems, like the Global Positioning System (GPS). With Differential Global Positioning Systems (DGPS) the errors of GPS can be corrected to the acceptable level of few meters [14] [7] [22]. However, GPS cannot always be relied on and especially militaries that do not own positioning satellites are constantly in search of alternative methods.

There are many existing MAC protocols and some of them can provide sufficient Quality of Service in a MANET. The mobile ad hoc network between the UAVs in the WPSN uses a MAC protocol called ISMA/RA (Inhibit Sense Multiple Access/with Reservation for Ad hoc networks) presented in [26]. It was developed in 2004 by the first author and Marko Ahvenainen [27] for military ad hoc networks, and has been implemented as a simulation model. ISMA/RA can be considered as a modification of ISMA/P [15]. The idea in ISMA/RA, as well as in ISMA/P and PRMA [16], is to guarantee bandwidth in multiple hops by a combination of random access and polling protocols, and by dividing the time axis into slots. The behavior of ISMA/P is analyzed in [17] and well understood. The TDMA approach for ad hoc WLAN networks is also used in HiperLAN/2, but the solution and performance issues (like in [18]) in HiperLAN are quite different from those of ISMA/RA. This paper offers a provably computationally secure protocol between base stations and other nodes combined with the introduced use cases of the WPSN. The introduced secure protocol combined with use cases of the WPSN enables the maximum performance at all warrior levels.

III. APPLICATIONS OF UAV-BASED SENSOR NETWORKS

The article describes three scenarios in which the WPSN can be utilized to maintain the initiative; namely, on the road, in built-up areas, including inside buildings, and, finally, how the Special Forces can utilize these systems [19].

A. Road side bomb detection

Increased Overseas Operations present road side bombs as a serious concern for the friendly troops due to the road side bombs' efficiency related to their unpredicted location. By using a solution based on the Wireless Polling Sensor Network, road side bombs can be detected using this new technology based on novel sensor data collection techniques. The detection procedure involves the following phases.

Firstly, the new concept of Wireless Polling Sensor Network comprises fixed sensor nodes, which do not communicate with each other. These nodes answer to mobile polling if they have something to report. The mobile polling nodes are a swarm of pre-programmed UAVs equipped with homing devices.

Secondly, the fixed nodes detect activity at the road-side, such as humans or large objects moving. The detection is based on a significant change in the electromagnetic spectrum, such as thermal, magnetic, or seismic change of the monitored area. The UAV patrols the area regularly, for instance, once an hour. Finally, as bombs are typically placed on the sites hours or days in advance, the WPSN application does not require real-time reporting to match the needs.

The fixed sensor nodes do not emit electromagnetic radiation except when the UAV sends a polling request with a specific code. The static nodes use directional antennas and communicate directly above (in a certain angle). A Wireless Polling Sensor Network has an edge over a traditional Wireless Sensor Network, for the system will remain functional even if some sensor nodes have been destroyed. A swarm of UAVs as polling devices gives an edge to the system resulting in reliable data gathering as seen in Fig. 2, and the arrows indicate the data transmission between the entities, the UAVs and the sensor nodes.

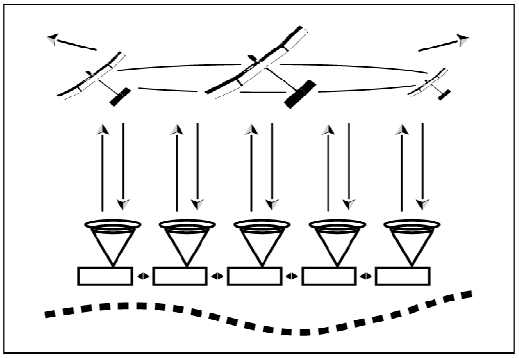

Figure 2. The structure of the WPSN with the swarm of UAVs.

Energy consumption in a multi-hop sensor network is higher than in the proposed solution since messages from other nodes must be relayed, and this depends on the placement of the nodes relative to the control point. The detection of the sensor nodes by the opponent is also much easier in a fixed multi-hop network. The WPSN has lower energy consumption together with better protection against detection, resulting in increased survivability of the network.

The polling procedure begins with mutual authentication of the UAV and the sensor. After authentication stage information is sent in encrypted from the sensor to the UAV. Since the transmitting power of a sensor is low, directional antennas are used for securing the transmission towards the

UAV. This enures the safety and QoS of transmission. The jamming of the system is made difficult by directional antennas. The system is battle-proof and answers only the UAV after a defined and pre-programmed identification protocol.

As the signal propagation time and the message forwarding delay are 10 ms and 15 ms, respectively, the communication delay can be understood to be on an accepted level when a swarm of UAVs is used to collect the accrued sensor data [29]. Since currently neither a test-laboratory nor UAVs can be utilized for testing purposes, the information referred to in this particular section of the paper is based on a relevant study [29]. As explained in Section III on page 3, the UAVs are used in swarms of three or four in order to ensure maximized data gathering and the validity of the sensor data. Moreover, as described in Section III, reliable communication between a single UAV and sensors takes only fragments of seconds after the identification procedures. In this case, the altitude of the swarm of UAVs is 400 meters. This altitude indicates that, once the angle of the transmitting sensor is from 5 to 7 degrees, the communication area at the altitude of 400 meters is at least 33,3 meters in diameter and in maximum 46,7 meters in diameter. In this example the speed of a single UAV is 80 km/h and 22 m/s allowing a UAV to receive a signal from a sensor for longer than a second. And again, as explained in [29], the signal propagation time and the message forwarding delay are 10 ms and 15 ms, which gives enough time for a single UAV to communicate with each sensor in a swarm of UAVs. And in case a single UAV fails to communicate with a sensor, another member of a swarm of UAVs can replace this function. When all the collected data are verified, these accrued data can be merged.

The topology of network systems has to be correctly coordinated (i.e., managing spectrum usage with group mobility patterns). The hierarchy of a network has to support this. This can be achieved by hierarchical design where devices are only to interact with their peers from the same group [19]. This means the swarm of UAVs communicates in the same intra-group while the UAVs and multi-sensors are in an inter-group with the UAVs. This ensures the QoS and proper maintenance of networks. Improved network performance can be obtained by using more channels, aggregation of more packets per frame and appropriate channel assignment [20]. A UAV can be used as a platform to provide the needed services, for example, Digital Video Broadcast – Terrestrial [DVB-T) and Digital Video Broadcast –Handheld (DVB-H) [21].

B. Location services in urban areas

Another interesting application of the WPSN is related to positioning and location services, especially in urban warfare. This solution is based on the Ground Positioning System (GPS) and the GPS-Pseudolite, better known as the Self-Calibrating Pseudolite Array (SCPA) [22] [8]. Studies indicate that the SCPA provides an effective means of acquiring a satellite-based Carrier-phase Differential GPS-type (CDGPS) centimeter-level positioning in locations without access to the GPS satellite constellation [8].

An Army tactical warfighter needs network services both On-The-Move (OTM) and At-The-Halt (ATH) [23]. One of the lessons learned from Iraq and Afghanistan was the need for a more robust Beyond-Line-Of-Sight (BLOS) communication capacity between the lower Army echelon Land Warriors, from Squad Leaders to Battalion Commanders [23].

The SCPA technique is used in Mars Rover Navigation [8]. The application can be as follows: The warrior polls the SCPA stationed on the urban battlefield (roof-tops, perimeters of buildings). The warrior acts as a polling UAV as described in Fig. 3, and the arrows indicate the data transmission between the entities and the triangle-shaped objects represent the SCPA.

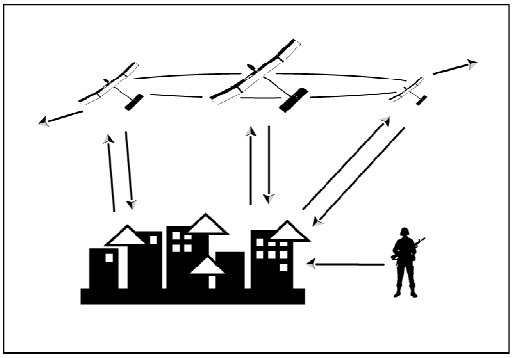

Figure 3. The WPSN presented in the urban infrastructure.

The proposed and described solutions have to be based on novel, generic and robust battlefield-proven solutions in order to meet the given needs, and this in turn involves addressing the topology of the network system carefully.

The novel sensor data collection techniques include: 1) the Development of a new networking concept: Wireless Polling Sensor Network, 2) A mobile ad hoc sensor network that can support near real-time streams, and 3) Generic SOA-interfaces for sensors and sensor platform control. One of these is the medium access control (MAC) algorithm and protocol for ad-hoc wireless networks that employs power control spatial-reuse scheduling techniques [24]. The Networks inside the WPSN solutions have to be functional and communicate as seen in Fig. 4, and the arrows indicate the data transmission between the entities, the UAVs and the sensor nodes.

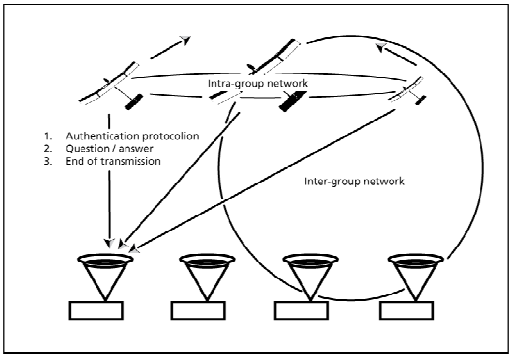

Figure 4. The principle of the network topology.

Since the power production and power consumption will remain as a challenge, certain actions need to be addressed. Thus when defining the network design, it has to be emphasized that network coding enables a more efficient, scalable and reliable wireless network [25].

The multi-sensor system comprises (Fig. 5): 1) a control unit (CU) that is placed on the operational centre, 2) a number of sensor control units (SCUs) that form a mobile ad hoc sensor network capable of near real-time data transfer, 3) sensor platforms, such as unmanned air or land vehicles, 4) different types of sensors, and 5) new algorithms for multi-sensor collaboration.

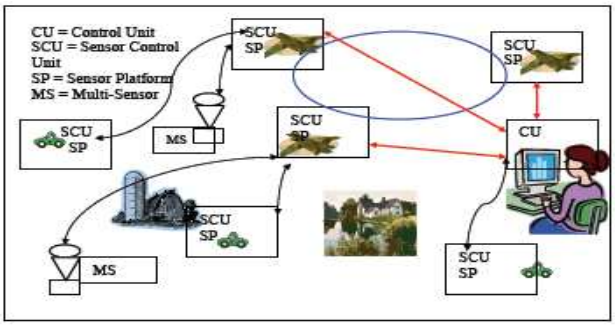

Figure 5. The network system of the WPSN.

Another application in an urban environment is a multi-hop mobile sensor network consisting of UGVs for investigation of buildings or placing SCPAs on a site. A network of a small number of such UGVs does not present technical problems as a small mobile ad hoc network, but it removes the need for a line-of-sight connection. The main new advantage is the addition of location mechanisms and pre-planned routes that are manually assisted when needed.

C. Solution for the special forces

The Special Forces need a precise location of a target to have it destroyed. Let us assume that in this example the selected target is heavily fortified, guarded and built of concrete, or buried deep in soil. The power of conventional weapons used by the Special Forces is not enough to destroy the target. Therefore, the target has to be marked for the bombs or guided missiles. This idea utilizes the possibilities of the Wireless Polling Sensor Network (WPSN), and the solution is based on the use of the SCPA. The idea is to set the SCPAs close to the selected target and measure the distance and direction from this specific spot at the target. This way the place of each SCPA is very precisely measured in relation to other SCPAs and the target. Once this has been done to each SCPA, a swarm of UAVs can be sent on their way to poll the SCPAs and collect the data to be transmitted to the destruction device for preparation purposes, if needed. The SCPAs do not form a network between each other, thus not transmitting, and they do not have a specific ground station. Pseudolites only answer the UAVs according to the communication protocol described earlier in Section III, B. In Fig. 6 below the arrows indicate the data transmission between the entities, and the question mark indicates the target to be destroyed.

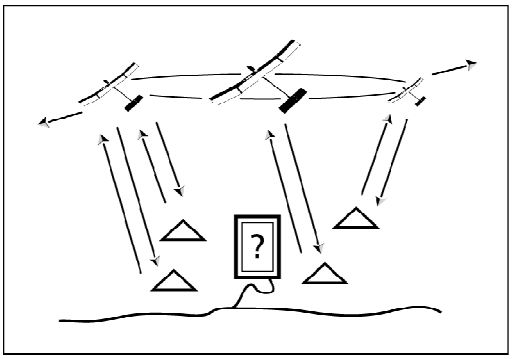

Figure 6. An example of the SCPA in the use of the Special Forces.

Once the pseudolites are set on their positions, the selected destruction device (in this case a fighter with an intelligent bomb) approaches the target at the selected moment and drops the bomb and dismisses the area. The destruction device polls the SCPAs while heading towards the target and, based on the collected data, the destruction device is being guided at its target. This protocol deletes the need to depend on GPS-satellites and thus gives an edge to gain the goals in rough and mountainous terrain, where GPS-satellites cannot be seen all the time. Jamming the SCPAs is not easy, for they transmit the encrypted data only once in a very narrow angle (5 – 7 degrees) straight upwards and after the bomb has the data, it is locked to its target.

In this paper the altitude for a swarm of UAVs has been defined to be 400 meters because a UAV is hard to detect or destroy from that altitude. Furthermore, the distance between the UAVs and ground-based sensors ensure reliable means of communication. Besides, small UAVs are relatively inexpensive and easy to replace which makes them an invaluable asset in military operations.

D. Evaluation of the concept

As the UAV sensor network is still on the design stage and no implementations can be tested, evaluation of the whole solution can only be based on looking at the basic ideas of the concept and finding its strengths and weaknesses. We go through some typical issues that should be considered for any sensor network solution.

Offered service: The proposed WPSN solution provides location and targeting service, and in the road side bomb application continuous sensor data collection from the area. In the last application the solution does not give reliable alarms of intrusion, unlike e.g. burglar alarm systems. Therefore the information is likely to include many false positives and a rapid reaction to each sensor data item that might indicate an effort to plant a bomb would be superfluous. It is sufficient to poll the sensor nodes after a relatively long period of time immediately before a patrol tour. The solution does not assist in fast response but can mitigate the effects and provide sensor data for

demonstrating that an incidence was planned, and possibly an identification of the attacker if voice sensors are used.

Coverage issues: The proposed system is suitable for areas so large that they cannot be easily covered by a fixed wireless base station, or by a WSN, and the set of sensors can be formed of disconnected parts, unlike in WSN. The use of a network of several UAVs is a clear improvement to the present applications where one UAV is controlled by a ground station and a line-of-sight connection is required. This limits the operational range of UAVs to roughly ten kilometers in open areas and prevents the use of UAVs in urban areas. A networked set of UAVs can increase the range by multi-hop routing. If one UAV has a line-of-sight connection to a ground station, it can forward messages to and from other UAVs. This requires that the MAC protocol supports real-time traffic. Controlling a UAV (and especially a number of them) through multi-hop connections is difficult but in the presented solution it is made possible by the sensor nodes: the UAVs have a pre-planned route and feedback information from the sensor nodes allows the UAVs to make corrections to their positions and to stay at the planned route. It is also expected that a ground based pilot can control the swarm of networked UAVs by steering only one of them and relying on suitable control protocols that keep the UAVs of the swarm in a fixed formation. Connectivity issues for an *n*-node UAV/UGV network can appear but they are typical to any mobile ad hoc network (MANET). In the case of WPSN, connectivity problems of the MANET are minor since the UAV/UGV nodes follow pre-assigned paths and the number *n* of nodes is small. Connectivity issues between the UAV/UGV and sensor nodes determine how strictly the UAV/UGV must follow the pre-assigned path but this restriction can be avoided by increasing the altitude of the UAV. From a sufficient altitude the UAV can receive data from all ground sensors.

Operational limitations: The most important restriction to the system is caused by weather conditions, which do not always allow the use of UAVs but this limitation is not seen as a major argument against the solution. The polling device could of course also be a ground-based vehicle avoiding the weather dependence. There is an advantage in using an UAV since camera picture from an UAV can often give a probable reason e.g. why a sensor node is not communicating. The solution requires usage of planned routes. There can naturally be many alternative planned routes. The concept does not in any way require that all sensor nodes must be polled in any specific order.

Performance issues: Performance evaluation of the whole system is not presented in this article since there are no real-life experiments so far. We can describe the main performance issues. Traffic congestion problems cannot appear in the system: the UAV/UGV makes the round e.g. every hour and collects sensor data from a relatively small number of sensors.

Dependability issues: The WSPN network cannot be easily disabled by removal or blocking of some nodes, as is the case for a WSN in essentially one-dimensional areas, such as a road where one parked truck may disconnect the WSN. A problem of a malicious network node unwilling to transfer data of other nodes does not occur since the sensor nodes communicate only with the polling network, which can be assumed secure. Unauthorized removal of sensor nodes is interpreted as a signal of undesired activity. There are ways to protect the sensor nodes against efforts to break the security algorithms protecting their communication with the polling nodes, e.g. by self-destruction, even if there is physical access to the sensor nodes. The sensor nodes should be difficult to find, otherwise they may be stolen. The communication mode of replying only to the polling node request makes the nodes difficult to find by electro-magnetic sensors.

Energy issues: Polling is in general considered a less efficient communication method than generating events from incidences, since many nodes have nothing to report. In the road-side bomb application there are some factors that change this conclusion. It is desirable to get a stay-alive announcement from each sensor in any case; therefore it is not sufficient to generate events only if something suspicious happens. The time to poll the sensor nodes is negligible compared to the time the polling UAV needs for the round trip for physical reasons, so polling is not slower in this case. The energy constraints in the UAV are not a limiting factor. It is of course possible to create a hierarchical sensor node structure where only some nodes communicate with the polling nodes while the other nodes report events to the communicating node. However, some robustness is lost in the hierarchical model. The polling network concept has a clear advantage in networks that are essentially one-dimensional, like a road side: a WSN node must pass messages created by other nodes; consequently its energy usage cannot be well predicted. In the WSPN solution energy usage can be well estimated and it is more important to have a good estimate of the battery life-time than a maximal prolongation of sensor operational time between battery recharge. The same patrol routes are not used for years, nor do the sensor nodes need to last for years without recharging. The energy needed to communicate with the polling node is not negligible, but especially as the communication is in free space, it is not assumed to be a limiting factor for the sensor node batteries. Sufficiency of energy in ground-based sensors and in UAV/UGV nodes is a limitation but the sensor nodes do not need to be especially small in this application.

Technology development: A proposed technological solution should have characteristics that make it more future-proof. The WSPN solution is open to development of sensor techniques. It may be possible in the near future to detect threats better from sensor data, e.g., to distinguish between a deer and a walking human. Applications of unmanned vehicles to military and crisis management situations are also a fast developing area. Ad hoc sensor networks have on the other hand met with certain scalability problems. A simple polling network concept seems to give future promises. A military system should be flexible enough to have a range of usages. While the WSPN concept has been created for the current need in road-side bomb detection, the system has other applications e.g. in location finding and in targeting.

Possible applications: The road side bomb detection is the main application. There is a current need for it and the existing methods, i.e., disabling communication to an IED by jamming, and surveillance by UAVs, are inadequate. The use of WPSN for targeting instead of GPS has some advantages and disadvantages. It is vulnerable to ground-based jamming but on the other hand, the frequency can be selected from a wider range. Location service in urban area is a much studied but difficult issue. The proposed system may be a partial solution.

IV. A PROVABLY COMPUTATIONALLY SECURE PROTOCOL BETWEEN BASE STATIONS AND OTHER NODES

In the case of UAVs and other easily captured nodes there is a special disadvantage in using ordinary crypto algorithms requiring stored key. There is also no time and no computing power for asymmetric algorithms. We will give a solution to this problem by novel idea of exchanging One-Time Pads and encrypting data with one of the OTPs. The other OTP must be discarded for security reasons.

A. Basic idea of the crypto-algorithm

One-time pad (OTP), or Vernam's cipher, is a crypto algorithm where the key is as long as the plain text. The modern version of the algorithm simply takes a bitwise exclusive or of the key and the plain text. Denoting exclusive or by $\otimes$, the key K by a sequence of symbols $K=(K_i)_i$, and plaintext by $A=(A_i)_i$, the cryptotext in OTP is $X=A\otimes K=(A_i\otimes K_i)_i$. OTP has perfect security because even if all keys are tried, it is not possible to break OTP: for any plain text there always exists a key that encrypts the plain text to the observed crypto text. OTP has only one problem, as the keys are very long, there is no convenient way to transfer keys to the sides in communication.

In this article we describe a simple method of exchanging OTP keys in such a way that we obtain a method with provable computational security. We will briefly explain the method. If A and B are two users and A wants to send data A to B, let us first assume that A and B have exchanged their OTP keys K_A and K_B in such a way that an attacker can see $K_A\otimes K_B$. If A sends $K_A\otimes A$, the attacker can only get

$$(K_A\otimes K_B)\otimes(K_A\otimes A)=K_B\otimes A$$

and cannot open the plain text A. This method would have perfect security, but we cannot exchange the OTP keys quite as well as here. The proposed method shows to the attacker $(K_{A,i}\otimes K_{B,i})_i$ and $(K_{A,i}\otimes K_{B,i+k})_i$ for some fixed k. Using this relation the attacker can guess one symbol $K_{A,i}$ and calculate the symbol $K_{A,i+k}$. Thus, we have only computational complexity. However, if the attacker can only guess half of the bits in one symbol, he does not gain any information of the next symbol. Indeed, let $K_{A,i}$ be divided into two disjoint sets of bits C and D and C is guessed, D is unknown. We can try to guess a set E of bits from $K_{A,i+k}$. The remaining set of bits in $K_{A,i+k}$ is denoted by F. The set C has at most half of the bits in a symbol and we cannot obtain more bits to E than there are in C. It turns out that the bits of E can be assigned any values and there always exist D and F such that E has the assigned values. Thus, guessing E in this way is not possible. There is another way to proceed: when C is guessed we can open a part of plain text A_i. If the plain text has internal correlations between bits, then we can try to guess the bits D. The proposed solution is that A is cryptotext of a conventional symmetric cipher which hides statistical correlation. This cipher cannot be broken because the cryptotext of the cipher is not seen. The attacker only sees the cryptotext xored by the OTP. The attacker can go through all keys of the symmetric cipher and guess the plain text, but this can be made harder than directly guessing the OTP symbol. This leaves guessing at least half of the OTP symbol as the only effective approach. The actual method is a bit more complicated than this simple idea and will be described later.

The proposed method requires sending three times as much data as a conventional symmetric cipher: exchanging the OTPs is necessary. Computation time is not necessarily increased and xoring is a fast operation. While there today exist good ciphers for which there are no effective attacks, there are reasons for searching for algorithms based on OTP exchange. One reason is that currently there are very few good crypto-algorithms, second is that algorithms based on hard mathematical problems invite mathematicians to try to break them and we do not know how long the algorithms stand. The third reason is that symmetric ciphers require storing the keys, so if a node holding a key is lost, security can be broken.

B. Related work

Exchanging OTPs as a method of provable computational security has not been proposed earlier to the author's best knowledge. There is no direct related work but the idea has been taken from Simon Singh's popular science book [28], on page 282 Singh mentions an algorithm, which we have drawn in Figure 1. Singh attributes it to an unknown inventor. To the authors' knowledge it has not been discussed in scientific literature, which is odd since the algorithm is quite interesting: only B needs to know the one-time pad. Let us look at it and later fix the problem it has.

Let r be a prime and we will use integers modulo r, i.e., not bits, as symbols in the following crypto algorithms.

Let $t \geq 1$ be an integer. A one-time pad (OTP) is a crypto algorithm that encodes the plain text

$$D(1), D(2), D(3), \ldots \quad (1)$$

with a key

$$K(1), K(2), K(3), \ldots \quad (2)$$

by taking the bit-wise exclusive or $\oplus$, thus the crypto text is

$$K(1) \oplus D(1), K(2) \oplus D(2), K(3) \oplus D(3), \ldots \quad (3)$$

The task is to get the key to both sides. Let us first consider an algorithm where A sends data $D(t)$ to B over a two-way additive channel. A sends the data in plain text and B sends a one-time pad $K(t)$ to A. Let us assume that the end-to-end delay is T symbols, see Figure 7.

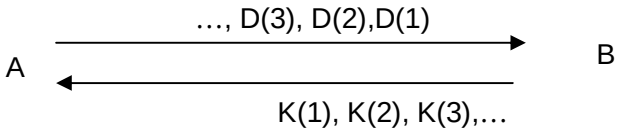

Figure 7. Interesting but insecure.

Let an eaves-dropper be located at a place that is j symbol transmission times from the place of A, or he can use directional antennas. He can read encrypted data

$$E(t) = D(1+t-j) + K(t-T+j)\beta_j . \quad (4)$$

The real number $\beta_j > 0$ gives the difference in signal strength of the signal from A and from B at the place j of the eaves-dropper. The fault of the protocol is that if the eaves-dropper listens in two places, j and i, and in two times t_1, t_2, he can subtract the signals and get the data. Let the times be chosen such that

$$t_1 + j = t_2 + i = a . \quad (5)$$

Then

$$\beta_i E(t_1) - \beta_j E(t_2) = (\beta_i - \beta_j) D(1+a) . \quad (6)$$

Thus, the algorithm in Figure 1 has a serious flaw. However, to some extent the problem can be removed: in order to get a secure algorithm A must send both the data and the key. As a way to get the key to A let us first think of sending it in plain text in a channel consisting of separate up-link and down-link channels as in Figure 8.

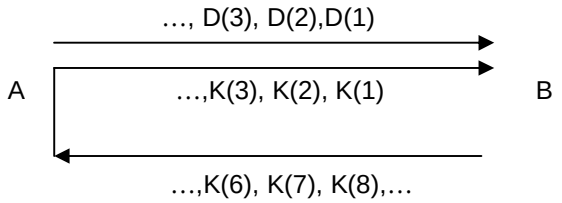

Figure 8. Better, but the key goes in plain text.

A echoes the OTP from B back to B. Now A learns the one-time pad of B. On the down-link we have the OTP, so it is secure. Let us secure the up-link by another one-time pad, this pad is created by A. For clarity, let us denote the OTP created by B by

$$K_B(1), K_B(2), K_B(3), \ldots \quad (7)$$

and the OTP created by A by

$$K_A(1), K_A(2), K_A(3), \ldots \quad (8)$$

There is no place to send any data, so let us forget sending the data and we shall only send the one-time pads as in Figure 9.

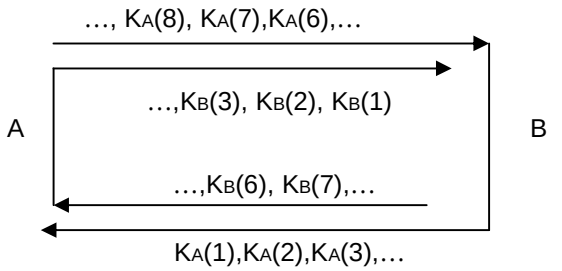

Figure 9. The basic idea of OTP exchange.

Let us denote by $g : Z_r \times Z_r \rightarrow Z_r$ a mapping used by A for encrypting $K_A(t)$ by $K_B(t-T)$. B applies

the same function g for encrypting $K_B(t)$ by $K_A(t-T)$. The function g is known to both A and B and does not contain any secret parameters. We assume that B can obtain $K_A(t)$ from knowing

$$K_B(t-T) \text{ and } g(K_A(t), K_B(t-T)). \quad (9)$$

Likewise, we assume that A can obtain $K_B(t)$ from knowing

$$K_A(t-T) \text{ and } g(K_B(t), K_A(t-T)). \quad (10)$$

The algorithm in Figure 3 is the proposed OTP exchange. Next e will analyze it.

C. Analysis

Let us assume that the eaves-dropper follows data both from the up-link and the down-link. Let us assume that he is j symbol transmission times from the place of A. On the down-link he hears

$$E_{down}(t) = g(K_A(1+t-j), K_B(1+t-j-T)) \quad (11)$$

On the up-link he hears

$$E_{up}(t) = g(K_B(t-T+j), K_A(t+j-2T)). \quad (12)$$

He cannot gain anything from listening in two places as signal strengths attenuate in the same way for the two parameters of the function g, it suffices to look at different times he reads data. Here we also do not need to assume that the channel is additive. The channel adds noise and distortion, but these issues are not of concern to us now. We focus on the cryptographic algorithm and assume that the channel has not errors or distortion. The eaves-dropper can read the up-link and the down-link in different times and try to solve the keys recursively. Let

$$t_2 = t_1 + 1 - 2j \quad (13)$$

and let us write

$$x_1 = K_B(t_1 - T + j) = K_B(1 + t_2 - j - T), \quad (14)$$
$$y_1 = K_A(t_1 + j - 2T), \; y_2 = K_A(1 + t_2 - j).$$

Then

$$E_{up}(t_1) = g(x_1, y_1), \; E_{down}(t_2) = g(y_2, x_1). \quad (15)$$

By guessing y_1 the eaves-dropper can solve x_1 from the first (up) equation because A can also do it. Having obtained x_1 the eaves-dropper can solve y_2 from the second (down) equation since B can also solve the equation. This can be continued to the next key symbols

$$E_{up}(t_3) = g(x_2, y_2), \; E_{up}(t_4) = g(y_2, x_3). \quad (16)$$

Thus, if there are unique solutions x_k, y_k, the eaves-dropper can obtain the whole one-time pads.

Let us firstly notice that values x_k, y_k that agree with what the eaves-dropper is listening can be computed for every guess y_1. As the algorithm treats all x_k, y_k in the same way, the eaves-dropper might just as well start from guessing any x_k or y_k. The important thing is that he does not get any more information from this OTP exchange protocol. If he wants to know if his guess is correct, he must compute some values x_k, $k = 1,2,...$ and check if he can open data encrypted by B. B encrypts data

$$D_B(1), D_B(2), D_B(3), \ldots \quad (17)$$

in the usual way as

$$K_B(1) \oplus D_B(1), K_B(2) \oplus D_B(2), K_B(3) \oplus D_B(3), \ldots$$

Perfect security of OTP does not any more hold. The first symbol may decode to anything depending on the guess of $K_B(1)$ but already at the second symbol the eaves-dropper may notice that data does not decode to some sensible data. The important question is if the eaves-dropper has any better way than guessing one key symbol or a large part of it. We can naturally select the symbol length in bits in such a way that guessing one symbol or a large part of it by brute force is sufficiently difficult.

If any faster way for the eaves-dropper exists depends largely on the function g. Let us select the function as

$$g(y, x) = x + y2^{n/2} \bmod r \quad (18)$$

where $n = \lceil \log_2 r \rceil$ is the number of bits in the prime r. Let

$$x = x_a + x_b \text{ and } y = y_a + y_b \quad (19)$$

be representations where x and y have been split into two parts that do not have any bits in common in their binary representations. For instance, x_a can be the low bits and x_b give the high bits, but we allow any kind of a split of bits

into x_a and x_b. The eaves-dropper can check if the bits in x_a are decoded into sensible data in the data sent by B. As B encrypts with OTP, there exists key bits x_a that decode the encrypted data into any selected data. The eaves-dropper must try to compute y by solving

$$e = g(y, x). \quad (20)$$

After obtaining the key symbol y the eaves-dropper can decrypt data encoded by A. If also some bits of data encrypted by A are sensible the eaves-dropper may try to conclude that he has made the correct guess of the bits x_a. If he can obtain all bits of x in this way, he has a method of effective crypto-analysis, but if he must guess a large part of x before he can conclude that the guess is correct, he needs a good guess before (15)-(16) can be used. Let us show that the latter case is true. The following theorem says that more than half of bits in a symbol x must be guessed before it is possible to test if the guess is correct.

Theorem 1. *Let* $e \in Z_r$ *be a fixed number. Let* $x = x_a + x_b$ *and* $y = y_a + y_b$ *be representations where* x *and* y *have been split into two parts that do not have any bits in common in their binary representations. Let* x_a *and* y_a *have maximum* $\frac{n}{2}$ *valid bits (i.e., the length of* x_a *and* y_a *can be* n *bits but only at most half of the bits are determined by* x_a *and* y_a*, the rest are determined by* x_b *and* y_b*). For any* x_a *and* y_a *there almost always exists* x_b *and* y_b *such that* $e = g(y, x)$. *Almost always here means with probability on the range of* $1 - 2^{-n}$.

Proof: Let us consider the first order congruence

$$g(y, x) - x_a - y_a 2^{n/2} \equiv x_b + y_b 2^{n/2} \pmod{r}. \quad (21)$$

As r is a prime, the number

$$z = x_b + y_b 2^{n/2} \pmod{r} \quad (22)$$

gets 2^n (possibly not different) values when x_b and y_b range over the numbers in $Z_{n/2}$. Different values (x_b, y_b) and (x_b', y_b') yield the same z only if

$$x_b + y_b 2^{n/2} - x_b' + y_b' 2^{n/2} \equiv 0 \pmod{r} \quad (23)$$

The number $x_b + y_b 2^{n/2} - x_b' + y_b' 2^{n/2}$ has typically about $2n$ bits and r has n bits. The probability that the number is divisible by r is about 2^{-n}. We can say that almost always z values from two (x_b, y_b) and (x_b', y_b') are different since there are 2^n possibilities for (x_b, y_b) and the probability 2^{-n} means that in average one z may not be obtained. The probability 2^{-n} is very small compared to the probability $2^{-n/2}$ of guessing x_a by brute force. Thus,

$$g(y, x) - x_a - y_a 2^{n/2} \equiv z \pmod{r} \quad (24)$$

can be satisfied for almost any selection of x_a and y_a.

From Theorem l we notice that unless the eaves-dropper can guess more than half of the bits in a symbol he cannot conclude anything by checking decrypted data. Even if the bits decrypted by x_a and y_a make sense, it does not mean anything at all. Just as in OTP, any sensible data for these bits can be obtained from some selection of x_a and y_a. Only if the eaves-dropper can guess more than half of the bits of a symbol, then x_b and y_b have only a limited range and z in the proof of Theorem 1 cannot be found. Then the equation $e = g(y, x)$ is usually not satisfied for any selected x_a and such y_a, that the data sent by A makes sense. We conclude that the algorithm has in a certain sense provable computational complexity of $2^{n/2}$ trials.

A provable lower bound of $2^{n/2}$ trials by brute force would be much better than the situation with conventional stream ciphers. While there has been recent progress in stream cipher design, new crypto-analytic methods can still be developed. The reason why the OTP exchange protocol could be better than modern stream ciphers is partly due to the fact that an algorithm encrypting real data must remove the structure of the data. The OTP exchange protocol is

encrypting random keys that do not have a structure. Partly the reason is that real data is encrypted with one-time pads that do not try to remove the structure from the data: they simply make every possible decoding of the data equally probable.

However, Theorem 1 does not quite say that there is a lower bound of $2^{n/2}$ trials by brute force. There are two possible ways of attack. In the first way the attacker may try to guess the correct x_a and check it by decrypting data encrypted by OTP. As every key symbol is randomly selected, the correct x_a is random and by Theorem 1 there is practically no chance that the attacker can gain anything unless x_a has more than half of the bits in a symbol. The only choice in this attack is to guess x_a by brute force.

The second way is that the attacker guesses data encrypted by OTP and computes the key symbols from the guessed data and the encrypted data. Then he checks if (15)-(16) is satisfied. This attack works well if plain text is encrypted. For instance, if any part of a text that has been encrypted by OTP is revealed and the encrypted data of the corresponding key exchange is obtained, it is a simple matter to open all text that has been encrypted with the OTP. Possible attacks include searching for published documents that have been encrypted by OTP. This is similar to the way the Japanese diplomat cipher was broken in the Second World War. The attack does not break the OTP system, but all other texts that are encrypted by the same OTP are broken. Another attack is searching for common long phrases. If the symbol length is 256 bits, the phrase must be longer than 128 bits, i.e., 16 bytes. Such are relatively long phrases, but not impossible to find in text. Then the attacker must search for the correct starting place, which is relatively easy. Such old style attacks work against OTP since OTP does not use diffusion and confusion: if plain text and encrypted text pairs are obtained, the key is immediately revealed. It is of no concern in OTP as keys are not reused but the dependences (15)-(16) of the OTP exchange make the property extremely dangerous.

The correction seems to be to encrypt plain text first with some good symmetric cipher and then use OTP. The symmetric cipher must be so good that guessing what crypto text some plain text produces is very difficult. The OTP hides all information of the crypto text produced by the symmetric cipher, thus the attacker does not have crypto text. The relations (15)-(16) do not mean that there are relations between the parts of the OTP. The OTP is a completely valid OTP where no symbols have any correlations with each other or with the text that they encrypt. Without any information of crypto text he does not have any information that has a relation to the key of the symmetric cipher, thus he cannot recover the key. We conclude that the attack of guessing the plain text is not possible for information theoretical reasons. The only remaining attack is to guess x_a by brute force. This is naturally much less than the original perfect security but it is quite good for a more practical system than plain OTP.

D. Possible modifications

Let us look briefly at another possibility. We may allow non-unique values for x_k, y_k. It does not make decoding data especially harder, the decoder must at each stage select from two values. As an example of such a possibility let us select

$$g(x,y) = x^i + xy + y^2 \bmod r, \tag{25}$$

where i >1 is some integer. The quadratic equation

$$e = y^2 \bmod r \tag{26}$$

has two solutions z and $r-z$ if e is a quadratic residue and no solutions if it is not. We can always complete (25) into a quadratic form as

$$(y + 2^{-1}x)^2 \equiv y^2 + xy - x^2 \bmod r, \tag{27}$$

thus

$$(y + 2^{-1}x)^2 \equiv g(x,y) - x^2 + x^i \bmod r. \tag{28}$$

The quadratic equation can be rather fast solved by the Shank-Tonelli Algorithm. (A rather fast free C-language implementation of the Shank-Tonelli Algorithm is in the *msieve* factorization software by J. Papadopoulos.)

The eaves-dropper must solve the values x_k, y_k recursively and he may have to keep trace of all paths for a small number of steps before he can decide if data can be decoded. This method may be suitable for an application where the symbol is small and the eaves-dropper cannot decide from a small umber of symbols if he has found the solution. We will not study this possibility further. There are several complications, such as quadratic non-residues, but it may be worth the mention the possibility of non-unique keys.

OTP exchange provides provably secure communications with some cost, i.e., bandwidth demands are increased. A conventional way to provide secure communication is e.g. by using the Diffie-Hellmann key exchange protocol for establishing a shared encryption key, and then encrypting data with a conventional symmetric algorithm. The gain of using OTP exchange is that it cannot be eavesdropped as it is provably computationally secure, and we can better estimate when and if it can be broken. Experiences from real wars, for instance with Enigma in the WWII, has shown that militaries should not trust conventional wisdom of how difficult encryption algorithms are to break.

D. Initializing OTP exchange

The protocol in Figure 3 must be started in some way so that key symbols are not revealed to an eaves-dropper at the start. A simple solution is that before A has obtained any part of the B's OTP, it encrypts data with A's credentials that must be known to B. The credentials must be long enough for encrypting T first symbols from A's OTP, a time stamp and a sequence number. The latter fields are needed to prevent replay of the start of communication. In a similar way, B also needs credentials known to A. Notice that (15)-(16) can be used backwards. If OTP encrypts plain text that can be guessed, user credentials are revealed. Therefore, plain text encrypted with OTP must be first encrypted with a conventional cipher.

E. Comments on error coding

OTP has good error propagation characteristics: one erroneous bit in crypto text only causes one erroneous bit in the plain text. Error coding data before encrypting is a possible solution because of small error propagation. OTP exchange has more worries from errors. If any error occurs in transmission from A to B, B gets a wrong key symbol $K_A(t)$ and consequently encrypts its own key symbols with wrong $K_A(t)$. Consequently, A obtains wrong $K_B(t)$ and uses it to encrypt key symbols. Neither side notices anything wrong while A and B obtain quite different versions of $K_A(t)$ and $K_B(t)$. As a result, data cannot be decrypted. Adding error codes to key symbols leads to dependences between key symbols and should be avoided. Therefore $E_{up}(t)$ and $E_{down}(t)$ must be extended by error coding. It is not necessarily best to use forward error coding since there is the return channel.

F. The issue of synchronization

The OTP exchange protocol needs the time T. Time synchronization in the protocol does not need any external protocol for synchronizing clocks. Both sides receive the OTP that they have sent and can synchronize to it with the ordinary HUNT mode, i.e., looking for the known bit sequence. This ability of the protocol can be used by other mechanisms. It directly gives the roundtrip delay from A to B. The round-trip delay can give location information e.g. if one of the sides is in a known place and the communication is through a communication satellite that does not add a time stamp.

G. Generation of key sequences

It might appear that one-time pads do not have any great advantage over ordinary stream ciphers since OTPs are usually generated by pseudo-random number generators. This is a wrong view. A typical stream cipher is essentially a pseudo random number generator but it has finite data as keys and possible other agreed parameters. Because this data is finite, the pseudo random sequence is finite. If an attacker collects enough data and keys are not changed often enough, he can take advantage of this periodicity. In the proposed method the OTP is not periodic. The OTPs of A and B are independent and created by A and B respectively. The other side learns the OTP through the OTP exchange. Even though the key symbols in the OTPs are probably created by pseudo random number generators, their parameters can be modified over time without the need of agreeing on them. Thus, the data is not finite as it must be in conventional stream ciphers.

V. CONCLUSIONS

This article suggests that viable methods exist, which improve the C^4I^2 of a warrior at all the levels. The examples covered are based on use cases of WPSN-solutions. They indicate that a warrior can obtain more critical information on the battlefield by using the presented WPSN solutions. This improves the general efficiency of a warrior at all levels. The platforms used today on the battlefield are not efficient. This is because they are based on a single sensor and they do not collect data in a way that would allow collaboration of multiple sensors. The proposed solution makes use of multi-sensor collaboration for improved location information and better situation awareness.

A warrior has to be functional and his gear needs to be planned according to the task. A key factor is the efficiency of a warrior, which can be gained via an improved Situational Awareness (SA), Blue Force Tracking (BFT) and Command and Control systems (C^4I^2). A warrior has to maintain his or her agility and stay active on the battlefield; all the gear cannot be attached.

Thus the warrior skeleton and its communication systems need to be carefully defined and built at each level due to the task requirements. Currently, the present solutions seen in active use are cumbersome and lack integration. The WPSN-solutions are unseen in these platforms. The maximum potential remains unreachable without sensor and data fusion. Militaries are moving towards smaller units while the demands keep increasing. At the same time troops are created for dismounted operations where a greater degree of flexibility and reliability of battle-proof and robust systems are needed.

The article discusses typical scenarios in which the WPSN can be invaluable. The effect of roadside bombs can be avoided once their precise location is known early and precisely enough. The increased knowledge at the basic warrior level in the form of location information gained from the SCPA on the battlefield improves the warrior's ability to carry out the task. Roadside bombs can be detected early enough and dismantled or destroyed before own or allied forces arrive at the spot. The Special Forces utilize the same output of the SCPA while conducting their ultimate tasks. Since the nodes of the WPSN do not communicate with each other, the system remains concealed, yet active. The WPSN node communicates with the UAV through encrypted messages. Thus the WPSN responds only after the UAV has

submitted a polling request with a specific code. Utilizing swarms of UAVs and UGVs has to be emphasized. The routes of Unmanned Vehicles (UVs) can be fed into the systems early enough to gain the needed information from the designated areas.

The WPSN-solution features many advantages over those of the traditional WSNs. This is, polling can use sensor specific codes and thereby security issues become easier to tackle. Moreover, energy consumption of the nodes in the fixed network is more equal since multi-hop data transmission is removed. The fixed sensor nodes do not lose connectivity even if a large number of nodes are removed.

As demonstrated via the presented use cases, WPSN solutions together with SCPAs and UVs can be utilized to reach the maximum performance at all warrior levels. Planning the warrior's gear requires a deep understanding of the environment and the demands set on a warrior. The warrior's niche and the nature of his or her missions have to be thoroughly understood. The keys to success can be found in precise planning based on the needs of warrior systems and subsystems from bottom to top.

REFERENCES

[1] T. Saarelainen, J. Jormakka, C4I2-Tools for future battlefield warriors, *Proceedings of the Fifth Telecommunication Conference on Digital Telecommunications IDCT '10*, 16.-19. June 2010, Athens, pp. 224-233, doi 10.1109/ICDT.2010.15.

[2] J. Jormakka, A Cyptoprotocol for Exchanging One time Pads," in *User's view on battlespace systems*, National Defence University, Department of Military Technology, Series 3, no 9, ISBN 978-951-25-1993-4, Edita, Helsinki 2009, pp. 137-147.

[3] G. Jakobson, J. Buford and L. Lewis, A Framework of Cognitive Situation Modelling and Recognition, Proceedings of the IEEE Symposium on Military Communications Conference, 2006. MILCOM 2006. IEEE Press, Oct. 2006, pp. 1 – 7, doi:10.1109/MILCOM.2006.302076.

[4] D. Hague, H.T. Kung, and B. Suter, Field Experimentation of Cots-based UAV Networking, Proceedings of the IEEE Symposium on Military Communications Conference, 2006. MILCOM 2006. IEEE Press, Oct. 2006, pp. 1 – 7, doi:10.1109/MILCOM.2006.302070.

[5] A. Blair, T. Brown, and M. Johnson, Tactical Mobile Mesh Network System Design, Proceedings of the IEEE Symposium on Military Communications Conference, 2007. MILCOM 2007. IEEE Press, Oct. 2007, pp. 1 – 7, doi:10.1109/MILCOM.2007.4454980.

[6] C-M. Cheng, P-H. Hsiao, H. T. Kung, and D. Vlah, Transmit Antenna Selection Based on Link-layer Channel Probing, Proceedings on the IEEE Symposium on World of Wireless, Mobile and Multimedia Networks, 2007. WoWMoM 2007. IEEE Press, Jun. 2007, pp. 1 – 6, doi:10.1109/WOWMOM.2007.4351703.

[7] O. Kosut, A. Turovsky, J. Sun, M. Ezovski, L. Tong, and G. Whipps, Integrated Mobile and Static Sensing for Target Tracking, Proceedings of the IEEE Symposium on Military Communications Conference, 2007. MILCOM 2007. IEEE Press, Oct. 2007, pp. 1 – 7, doi:10.1109/MILCOM.2007.4454968.

[8] M. Matsuoka, S.M. Rock, and M. G. Bualat, Autonomous Deployment of a Self-Calibrating Pseudolite Array for Mars Rover Navigation, Proceedings of the IEEE Symposium on Position Location and Navigation Symposium, 2004. (PLANS 2004) IEEE Press, Apr. 2004, pp. 733 – 739, INSPEC Accession Number: 7972394.

[9] K. R. Chevli, P.Y. Kim, A.A. Kagel, D.W. Moy, R.S.Pattay, R.A. Nichols, and A.D. Goldfinger, Blue Force Tracking Network Modeling and Simulation, Proceedings of the IEEE Symposium on Military Communications Conference, 2006. MILCOM 2006. IEEE press, Oct. 2006, pp. 1 – 7, doi:10.1109/MILCOM.2006.302050.

[10] D. Herold, L. Griffiths, and T.Y. Fung, Lightweight, High-Bandwidth Conformal Antenna System for Ballistic Helmets, Proceedings of the IEEE Symposium on Military Communications Conference, 2007. MILCOM 2007. IEEE Press, Oct. 2007, pp. 1 – 6, doi:10.1109/ MILCOM. 2007.4455055.

[11] P-J, Park, S-M, Choi, D-H, Lee, and B-S, Lee, Performance of UAV (Unmanned Aerial Vehicle) Communication System Adapting WiBro with Array Antenna, Proceedings of the IEEE Symposium on Advanced Communication Technology, 2009. ICACT 2009. IEEE Press, Feb. 2009, vol 2, pp. 1233 – 1237, INSPEC Accession Number: 10571377.

[12] A, Ruangwiset, Path Generation for Ground Target Tracking of Airplane-typed UAV, Proceedings of the IEEE Symposium on Robotics and Biomimetics, 2008. ROBIO 2008. IEEE Press, Feb. 2009, pp. 1354 – 1358, doi:10.1109/ROBIO.2009.4913197.

[13] I. Rubin, A. Behzad, Z. Runhe, L. Huiyu, and E. Caballero, TBONE: A Mobile-backbone Protocol for Ad-hoc Wireless Networks, Proceedings of the IEEE Symposium on Aerospace, 2002. IEEE Press, vol 6, pp. 6-2727 - 6-2740 vol.6, doi:10.1109/AERO.2002.1036113.

[14] H. Zheng, J. Shi, and L. Cao, Group-Mobility-Aware Spectrum Management for Future Digital Battlefields**,** Proceedings of the IEEE Symposium on Military Communications Conference, 2006. MILCOM 2006. IEEE Press, Oct. 2006, pp. 1 – 7, doi:10.1109/MILCOM.2006.302052.

[15] S. S. Chakraborty and S. Wager, A New Approach for Medium-Access Control for Data Traffic and Its Adaptation to the GSM General Packet Radio Services, *IEEE Transactions on Vehicular Technology*, Volume: 481, Jan. 1999, pp. 240 – 248.

[16] D. Googman, R.A. Valenzuela, K.T. Gayliard, and B. Ramamurthi, Packet Reservation Multiple Access for Local Wireless Communications, *IEEE Transactions on Communications*, vol. 37, issue 8, pp. 885 – 890, Aug. 1989, doi: 10.1109/26.31190.

[17] J. Jormakka, Performance Analysis of ISMA/P, *Transactions of Vehicular Technology*, vol.52, no. 1, January 2003, pp. 254 – 259.

[18] J. Habeta, R. Dutar and J, Wiegert, Performance Evaluation of HiperLAN/2 Multihop Ad Hoc Networks, *European Wireless 2002*, Feb. 2002.

[19] D. Al-Abri and J. McNair, Improving Localization Accuracy in Wireless Sensor Networks Using Location Verification Feedback, Proceedings of the IEEE Symposium on Military Communications Conference, 2007. MILCOM 2007. IEEE Press, Oct. 2007, pp. 1 – 7, doi:10.1109/ MILCOM.2007.4454844.

[20] O. Villavicencio, K. Lu, H. Zhu, and S. Kota, Performance of IEEE 802.11n in Multi-channel Multi-radio Wireless ad Hoc Network, MILCOM 2007, Proceedings of the IEEE Symposium on Military Communications Conference, 2007. MILCOM 2007. IEEE Press, Oct. 2007, pp. 1 – 6, doi:10.1109/MILCOM.2007.4454755.

[21] B. Bennett, P. Hemmings, and B. A. Hamilton, Operational Considerations of Deploying Wimax Technology as a Last-mile Tactical Communication System, Proceedings of the IEEE Symposium on Military Communications Conference, 2006. MILCOM 2006. IEEE Press, Oct. 2006, pp. 1 – 7, doi:10.1109/MILCOM.2006.302298.

[22] W. Wang, Z. Liu, and R. Xie, INS/GPS/Pseudolite Integrated Navigation for Land Vehicle in Urban Canyon Environments, Proceedings of the IEEE Symposium on Cybernetics and Intelligent Systems, 2004 IEEE Press, vol 2, pp. 1183 – 1186, doi:10.1109/ICCIS.2004.1460758.

[23] S. R. Ali, R.S. Wexler, and R. Hoffmann, Soldier Network Extension (SNE) On-The-Move Satellite Communications (SATCOM) for Army Tactical Battalion-level Network Healing and Thickening, Proceedings of the IEEE Symposium on Military Communications Conference, 2007. MILCOM 2007. IEEE Press, Oct. 2007, pp. 1 – 5, doi:10.1109/MILCOM.2007.4455035.

[24] A. Behzad, I. Rubin, and A. Mojibi-Yazdi, Distributed Power Controlled Medium Access Control for Ad-hoc Wireless Networks, Proceedings of the IEEE Symposium on Computer Communications, 2003. CCW 2003. Proceedings. 2003 IEEE Press, Oct. 2003, doi:10.1109/CCW. 2003.1240789.

[25] C. Fragouli, D. Katabi, A. Markopoulou, M. Rahul, and R. Hariharan, Wireless Network Coding: Opportunities & Challenges, Proceedings of the IEEE Sympoisum on Military Communications Conference, 2007. MILCOM 2007. IEEE Press, Oct. 2007, pp. 1 – 8, doi:10.1109/MILCOM 2007. 4454988.

[26] J. Jormakka, A TDMA-based MAC protocol for Ad Hoc Networks, *IUP Journal of Telecommunications*, in press, to appear Dec 2010.

[27] J. Jormakka and S. Ahvenainen, On Military Applications of IP-based Ad Hoc Networks, in *Technical Aspects of Network Centric Warfare*, National Defence College, Dept. of Techn., Series 1, No 17, Helsinki 2004, pp. 115 – 131.

[28] S. Singh, *The Code Book*, Fourth Estate, 2000, accessed on 22.12.2010 at 23:15.

[29] E. Haque, F. Wei, Y. Fukunaga, T. Gouda, X. Lu, and K. Mori, Autonomous Background Coordination Technology for Timely Sensor Connection in Wireless Sensor Networks, Proceedings of the IEEE International Symposium on Autonomous Decentralized Systems, 2011, pp. 10 – 16, doi 10.1109/ISADS.2011.8.