국방통신 … 편집위원 : 이종명 (명지대), 엄의석 (KAIST)

Key Technology Issues for Military Sensor Networks

Mohd. Noor Islam | Yeong Min Jang | Sunwoong Choi | Sangjoon Park*
Kookmin University, ETRI*

1. Introduction

Over a few decades a vast amount of research have been undertaken in the area of ad-hoc and wireless sensor network due to the fastest growth of Micro-Electro-Mechanical Systems (MEMS) and a significant success has been achieved by this time. It is possible now to deploy the sensors for civilian cases like industrial safety, medical health care (IT based treatment), smart building, volcanic surveillance and etc. It attracts in all areas for its low power, small device size, small size of network, less complexity and longer life characteristics.

With the success of application of sensor network in civil cases, nowadays the application of wireless sensor network is getting popularity in military because of many attractive applications of sensor networks in military like monitoring friendly forces, equipment and ammunition, battlefield surveillance, reconnaissance of opposing forces, targeting, battle damage assessment, nuclear, biological and chemical attack detection reconnaissance. Military Sensor Network includes appropriate protocols and organization for military applications. However, in military sensor network some challenges such as appropriate sensor technology, security, real time data streaming, audio and video services with data service, mobility management, fastest multi hop communication, coordination for large number of nodes, interoperability with other networks and coverage and connection assurance of the region of interest comes in front to apply sensor network for military applications successfully. Accuracy of sensors; low power audio and video compression technology; self-configurable, self-healing and self organized network; low latency and fast reconfigurable routing; transport protocol with high reliability, energy efficient and collision free MAC protocol; proper authentication, encryption, error detection and correction of data are necessary to make the military sensor network true.

A simple comparison of wireless sensor network for the civil and military applications is shown in Table1.

Table 1. A simple comparison of wireless sensor network and military sensor network

Characteristics	Civil Sensor Networks	Military Sensor Networks
Network Size	Small number of nodes	Large number of nodes (hundreds and thousands)
Coordination among nodes	Easy to coordinate due small number of nodes	Difficult to coordinate due to dense nodes
Mobility	Generally static	Static and mobile
Self -X (organization, configuration, healing)	Self-X protocols is not so necessary.	Self-X protocols should be adapted due to swift change of network condition, mobility and for different adverse conditions.
Security	Security is not prominent	Security is essential for reliable data and to protect malicious interfering.
Data type	Usually data is send through sensor network	Data, voice and video services are necessary to send, so real time protocol is necessary.
Sensors	Sensor mote equipped with humidity, temperature, light sensors	Sensor mote equipped with radar, acoustic, magnetic and electro-optic sensors, GPS, Infrared sensor
QoS	QoS is important	QoS is prominent

II. Military Sensor Network

2.1 Architecture of Military Sensor Network

There is no particular architecture of military sensor network. Figure 1 shows the total architecture and interconnection combines Air, Navy and Army forces. In army sensors are deployed in the battle field with air plane or helicopter. Some sensors are mobile such as robots and some are static. In the sea, some sensors are floating and some are underwater robots equipped with sensor. Sensors are equipped with radar sensors or electro-optic (camera), acoustic (microphone), magnetic, GPS and etc. The sensors detect the troops, calculate exact poison, track the moving objects and send those data to Sink. Data from the battle field may come hierarchical way using cluster head. After that the sink transmits the data to the control room via existing network (CDMA or Backhaul). In control room the data is analyzed and command or information is sent to the Air Fighter plane or to the War ship via Satellite. The tanks or other solders in the battle field can also get information from the sensor nodes.

In Figure 1, the total network architecture is dvided into different parts to show different applications. one part is shown as mountain area where the direct communication may be blocked by the mountain. So the sensors can help to find out the snipers or to communicate each other. In Urban case also same scenario happens for buildings when the solders can not find out the enemy snipers then they use sensors information to locate out and take necessary action. The tanks may use Wi-Fi to make mobile mesh network among them and they can also get sensors information through sink. Another portion is shown as plain area where the sensors are used to track the enemy vehicle. The data is

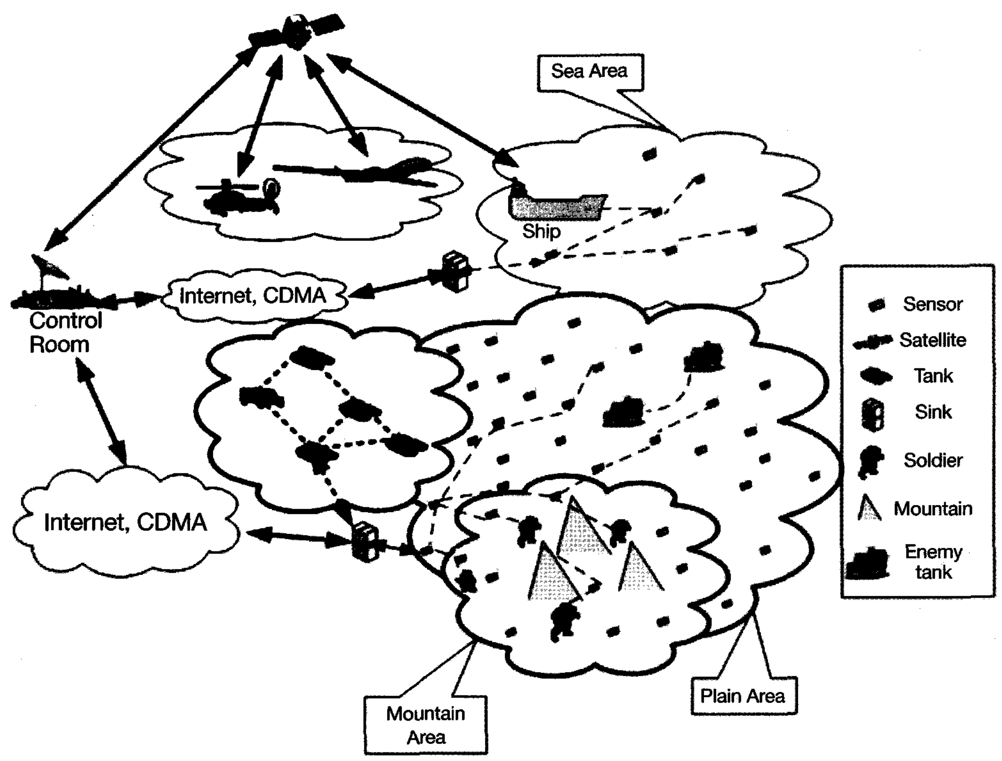


Figure 1: Future military sensor network architecture

sent to the control room and then the control room decides the necessary actions. Weapon may be equipped with some sensors and deployed in, when the sensor can detect enemy, the correct position, accurate speed then the weapon can take necessary action to destroy the enemy troops or vehicle without human intervention.

2.2 Applications of Military Sensor Network

Military sensor network can be used for different purposes in the battlefield.

A. Monitoring Equipments and Commanding Forces

Military Sensor Network can be used to gather data of troop' s position, the amount of equipment and weapons at hand, troop' s strength. This report can be sent to the higher levels at control room or troop leaders, where an appropriate command can be taken depending on the current state of affairs. The health condition of the soldiers can also be known using the sensor data.

B. Battlefield Surveillance

Sensors can be randomly deployed in inaccessible regions and critical areas to track the opposite forces and to conform about the presence of them. Furthermore, these networks can also be deployed to discover ways and paths to make plan for attack intelligently without human intervention.

C. Targeting and Localization

Military Sensor Networks can be used to track the path of enemy troops. The analyzed data can be fed to an intelligent ammunition system that can take an aggressive stance on order. Using the sensor network data the exact position of enemy troop or enemy tank can be localized.

D. Battle Damage Assessment

To analyze data before attack and after attack the battle damage can be assessed. In that case after the attack news sensors are needed to deploy.

E. Nuclear, Biological and Chemical Attack Detection

In military sensor network, sensors can be used to detect the chemical, biological or nuclear attack with appropriate sensor technology. This kind of sensors may include the ability to take counter measures against such attacks as well.

III. Challenges and Research Issues for Military Sensor Networks

To make an appropriate military sensor network there are a lot of challenges and an extensive research and development are needed. To provide the mobility, self-configuration, security and coverage the sensor nodes as well as sensor network protocol should be intelligent. Due to the limitation of power existing protocols for other network are not appropriate for the sensor network, so low power protocols are needed. The development for sensing accuracy and the advancement of sensing technology for military sensors are also important. The challenges for the future military sensor network are discussed below:

3.1 Sensor Technologies

Sensor technology provides the "eyes and ears" for nearly all army tactical and strategic weapon systems as well as the intelligence community. Sensors are integral and fundamental to achieve situational awareness on the battlefield to win the information war. Because of their pervasiveness, sensors have multiple transition opportunities, including the 21st century soldier, and sensors are vital to the survivability of soldiers and the weapon platforms on the battlefield.

In military sensor network, the research area of sensor technologies is developing in five subareas: Radar Sensors; Electro-optic Sensors; Acoustic, Magnetic, and Seismic Sensors; Automatic Target Recognition; and Integrated Platform Electronics. Significant effort is necessary for proper integration into larger-scale sensor networks, and one of the greatest challenges is improving sensor accuracy to keep the false alarm rate to a minimum. The need for a reliable detection of critical incidents has led to the use of multi-modal sensors. The intelligent combination of sensors and their joint accuracy are essential for future robust sensor applications. Furthermore, multi-modal sensors can minimize the power consumption as well as the generated traffic, e.g., if a video camera is enabled by an acoustic sensor or an infrared sensor [1]. In military, sensor encompasses self-organizing, flexible and scalable networks. Sensors communicate with one another for two purposes, communications services (e.g., automatic relaying of messages to a network gateway) and in-network processing (data aggregation and data fusion).

Companies such as SenTech, Textron and Lockheed Martin have systems with a variety of sensors (including seismic, acoustic, infrared) which transfer their data directly to a ground station over a number of long-range non-line of sight bearers (including satcom, very high frequency and high frequency bearers). But these nodes are equipped with own backhaul system. Recently Terrain Commander and Future Combat System (FCS) from Textron Systems or the Falcon Watch System from Harris which will provide processed information from a number of sensors (including acoustic, seismic, magnetic, electro-optical and passive infrared). However, there are very few systems on the market. Still those systems are not truly ad hoc multi-hop in nature requiring either a direct link back to a remote ground station or a direct link back to a gateway node. There are a few ad hoc systems advertised although many of these appear to be immature and still at proof-of-concept stage.

3.2 Coverage and Connectivity

In military sensor network coverage and connectivity are two vital measures to provide surveillance assurance and data reliability. In the battlefield, sensors are deployed from the helicopter or airplane randomly. For the wind the sensors may not be distributed uniformly so some place will be out of coverage or some place will have dense sensors. Two challenges arise for military sensor network. These are (a) Coverage and (b) Connectivity. Boolean and general sensing models are used to analyze coverage problems. If any point is inside of sensing range of a sensor then the point is covered. So, an event can be detected by the sensor network if and only the region is covered by the sensor network. If two sensors are inside the communication range of each other then the sensors are connected. As it is unpredictable about the situation after deployment, it may happen some part of the region of interest may stay out of coverage. In military sensor network, assurance of coverage and connectivity are most essential for reliability and faithful monitoring. Some researchers are proposed to use mobile sensor to make the area full of coverage. Some sensors may be damaged also during the battle. Another factor is lifetime of sensor. Sometime the sensor is needed for few weeks, sometimes it needs the coverage for the few months. So, there should need some research on deployment issues and how to make the region full of coverage. As the sensors are battery powered so appropriate self-organization and intelligent algorithms are needed to coordinate themselves and to share the sleeping schedule to save power compromising the coverage and power.

3.3 Mobility Management

Military sensor network comprises both mobile and static sensors due to accomplish different jobs. In military sensor network deploying of sensor network over the battlefield using advanced tools like airplane but various factors such as winds and obstacles are very likely to introduce coverage holes, regardless of how many sensor nodes are dropped. Taking one step further, even if a perfect coverage can be achieved initially, events such as node failures and malicious attacks will certainly degrade the network coverage as time evolves. As a result, there is an urgent need for sensor nodes to be equipped with mobility so that they can autonomously discover and repair coverage holes. Another scenario in which mobile sensor nodes are desired is the application of monitoring a moving object that travels over a large area. Lastly if the sensor nodes are equipped with moving vehicle or with human to sense his blood pressure that time the sensor also will move. So mobility management is a vital factor for military sensor network. High performance must be maintained in motion, which includes the rapid configuration of network topology as units and individuals reorganize themselves in pursuit of battlefield objectives. To achieve this, networking handoffs between communicating devices must be coordinated to minimize data outages and/or a reduction in performance while in motion. These hand-offs must be transparent to communicating units, maintaining session connectivity while in motion. Location awareness, both in relation to other communicating devices and space (such as GPS) may also be the key to high performance in motion.

As the radio range is very small and in battle field it is necessary to consider fast moving of nodes, it creates problem for association and dissociation quickly. This breaks the connectivity, loss of coverage and loosing of data is happened which degrades the network performance. Note that, for wireless sensor networks with scarce energy resources, it is not always favorable for nodes to move during field operation because the energy required for locomotion energy is often much higher than that for sensing and communication [6], [7]. However, as shown in [5], [8], when nodes can afford the energy cost associated with mobility, it is important to have a network management scheme that can make effective use of mobility to facilitate application objectives. For example, multiple mobile robots can be deployed in a battlefield for target tracking without human intervention [6]. These mobile robots can form an ad hoc sensor network for monitoring the region of interest. To ensure better tracking quality for a moving target, it is beneficial to deploy dynamically moving nodes. In [4], the solution for mobility management is shown using Bayesian estimation theory that can be implemented in a fully distributed manner. Mobility management is yet a hard issue for the military sensor network and more research is needed for the sensor network to make it appropriate for the military application.

3.4 Multimedia Services

In existing wireless sensor network only data is transmitted from different sensors to the sink. But in military sensor network, streaming and stored of video and audio data becomes an important part of modern command, communications, and control. The ability to deliver high bandwidth streams with low latency and low jitter is also critical. In many cases, these video streams must be delivered expeditiously across multiple hops (node-to-node connections) without loss of performance. Similarly, voice communications across many hops and in motion with high performance is a challenge demanding low delay and jitter at each network device.

More recently, the availability of inexpensive hardware such as CMOS cameras and microphones that are able to ubiquitously capture multimedia contents from the environment has fostered the development of Wireless Multimedia Sensor Networks (WMSNs) [11], [12], i.e., networks of wirelessly interconnected devices that allow retrieving video and audio streams, still images, and scalar sensor data. With rapid improvements and miniaturization in hardware, a single sensor device can be equipped with audio and visual information collection modules. As an example, the Cyclops image capturing and inference module [13], is designed for extremely light-weight imaging and can be interfaced with a host mote such as Crossbow' s MICA2 [9] or MICAz [10]. In addition to the ability to retrieve multimedia data, WMSNs will also be able to store, process in real-time, correlate and fuse multimedia data originated from heterogeneous sources. In [14], the survey shows the possible solution for the WMSN. They pointed out how recent work undertaken in Wyner-Ziv [15], [16] coding at the application layer, specialized spatio-temporal transport layer solutions, delay bounded routing, multi-channel MAC protocols, and MIMO, UWB technology, amongst others, seem most promising research directions in developing practical WMSNs. This multimedia WSN is still in theoretical stage. In military sensor network, research on multimedia application is important and we need much more research and practical advancement in that field.

3.5 Frequency Hopping

The dynamic and unpredictable nature of modern warfare and the peculiarities of the Radio Frequency (RF) spectrum environment place a high premium on the capability of individual devices to independently choose frequencies, locate and connect with peer devices, and rapidly shift frequencies in an automated, coordinated fashion without centralized oversight. This capability permits units to be brought on-line quickly in a hastily-formed network as well as to deal with inadvertent or malicious interfering and jamming signals in a deployed situation. Ideally, communicating devices will choose and manage frequencies and channels independently, for maximum flexibility in responding to mobility or interfering sources. In addition, these devices should continuously monitor the RF environment to allow for ongoing automated and coordinated optimization of the available RF spectrum.

3.6 Self-organization

Relationships between organizational units, vehicles, and individual war fighters may change rapidly, but in terms of command and control and in terms of physical proximity. In earlier eras, battlefield superiority depended on masses of contiguous units, but today the focus is on efficiency in achieving mission objectives. In order to deal with these changing relationships, communications devices must dynamically monitor and reconfigure network topologies. With thousands or hundreds of thousands of devices deployed in a single operation, it would be physically and logically impossible for network topologies to be defined and managed centrally. Instead, each device must independently find the best path for interconnection, choosing from available connections based on rules-based criteria. Self-X (configuration, healing, and organization) is the solution for Military sensor network. Every node should have self-configurable characteristics to adapt with the topology changing.

3.7 Security

The solution for sensor network security is public-key cryptography which distributes intelligence in the network, giving each node the ability to validate the identity of other participating nodes. This enables improved node mobility and flexible topologies for sensor networks that are scalable, fluid and easily reconfigurable, setting the stage for an array of new and innovative applications. In [1], [2], [3], they discussed on security challenges, key issues, security threats and solutions of the security for the wireless sensor network. Different layers of sensor are responsible for different attacks. Physical layer is responsible for Jamming, tampering and sybil attack though sybil is prompt in higher layer. The solutions of the attacks are spread-spectrum, lower duty cycle, tamper proofing and efficient key management. Link layer is responsible for collision, exhaustion, interrogating attack and sybil attack. Good encryption mechanism, authentication mechanism and error correcting techniques are required to defense these attacks. Network layer is also face some attacks like Manipulating routing information, Selective forwarding attack, Sinkhole (black hole) attack, Wormhole attack, Hello flood attack. So authentication, two-way authentication, three-way handshake, encryption, redundancy, probing, monitoring, flexible route selection is necessary to tackle those attacks. For transport layer Flooding is important where it needs limiting connection numbers, client puzzles. In application layer clone attack is prominent. So, unique pair wise keys are the solution for it. To provide the security in wireless sensor network there needs some messages and it increases the overhead where the data size in the network is so small. To use in the military network the security protocols need to be energy efficient and should be limited with few messages and robust.

Elliptic Curve Cryptography (ECC) delivers more security per bit than other public-key schemes; it is the only public-key scheme capable of meeting the footprint and power limitations of sensor devices. Certicom Security for Sensor Networks enables developers of low power sensor devices to build secure, reliable operation into sensor networks from design and development through to manufacturing, deployment and upgrade. In military sensor network it' s a great challenge yet to find out security for the sensor network compromising with the power constraint and bandwidth and robust security for the network.

3.8 Scalability

Scalability is the property of a sensor network means the applicability of sensor network would not be limited by the growing size of the network. As in the battle field thousands of nodes are deployed in order to provide the coverage assurance. So scalability for the military sensor network is evidently indispensable requirement. Scalability is ill served by any construct that requires globally consistent state, such as address or routing table entities that have to be maintained. In this case centralized control approach is not a good solution; rather the nodes should cooperatively organize the network, using distributed algorithm protocols. Self organization or self configuration is commonly used term for this principle. In network processing such as aggregation, distributed source coding and distributed compression, distributed and collaborative signal processing is necessary solution for the dense military sensor network.

3.9 Seamless Interoperability

Interoperability is a property referring to the ability of diverse systems and organizations to work together. Military sensor network is a heterogeneous network. Military sensor network may consist of Cellular network, Wi-Fi, WPAN, Satellite, and IP network. Protocols needed for military sensor network to provide seamless interoperability among those networks.

3.10 Target Classification, Localization and Querying Ability

Localization of target and query of any region is very essential task in military. In military sensor network, to locate target' s exact position, to monitor the friendly forces and to know the condition about any region of the battlefield without human intervention, localization and querying is the great challenge for military sensor network. Using different sensors in a mote and collecting data from different sensors the target can be classified exactly; for an example using acoustic and radar the object is determined and by magnetic sensor the object can be classified. And GPS or RSSI (Received Signal Strength Indicator) of signal can be used to determine the position.

IV. Protocols for Different Layer of MSN

In wireless sensor network, a vast research has been done for each layer of the network to make efficient individually. As there is no standardization for military sensor network, according to the application necessity in military sensor network some of those protocols can be used or some protocols need more development and research to make appropriate for military application. As in military sensor network, the node will face many difficulties, it will be far where human may not access and the data from the sensor network is most important to understand the exact situation in the battlefield. So the protocols should be certainly robust, energy efficient and intelligent. In this section we are focusing on the different layers protocols that can be proposed for the military wireless sensor network.

4.1 PHY Layer

In military sensor network, in case of other signals being transmitted within the same frequency band from other users or jamming the transmission, technology should provide some robustness against narrowband interference. Combined with the desire to achieve inconspicuous operation, some transmission technologies can subsequently be seen as prominent for use in military wireless sensor networks such as direct sequence spread spectrum (DS-SS), frequency hopping spread spectrum (FH-SS), pulsed ultra-wideband (UWB). In many prototype networks, "Commercial off the Shelf" COTS chipsets are being used providing transmission based on Bluetooth (FH-SS), ZigBee (IEEE 802.15.4/WPAN, DS-SS) or WLAN (IEEE 802.11b using DS-SS as well). Using of IEEE 802.15.4 specified multi-channel with narrow bands can be a solution for avoiding interference, collision. Virtual MIMO or UWB may come as a solution to provide higher bandwidth for multimedia services in military sensor network.

4.2 MAC Layer

In wireless sensor network, the existing MAC protocols are S-MAC, T-MAC, B-MAC which are trying to minimizing idle listening as much as possible to make energy efficient. To avoid the collision TDMA is the best solution but it doesn' t provide much scalability and doesn' t listen channel condition. CSMA can adapt with network changes. And Scheduled based protocols like TRAMA, which are combined with TDMA and CSMA. For military sensor network S-MAC, T-MAC, B-MAC, TRAMA can be used where TRAMA is best suitable to detect shot. Recently proposed Multichannel MAC like MMSN [17] can also be the candidate for military sensor network MAC. In [18] they present the virtual TDMA for sensors (VTS) MAC protocol, which intends to support the previous features, focusing particularly on real-time operation. VTS adaptively creates a TDMA arrangement with a number of timeslots equal to the actual number of nodes in range.

In military sensor network, we need real time, energy efficient, interference aware, and multi-channel MAC. So, combination of CSMA, TDMA and multichannel assignment MAC can be used for the military sensor network. Error correction codes are also necessary to include for tackling some attacks.

4.3 Routing Layer

In military sensor network, sensors are destroying, re-deploying and moving. So, the routing path is always changing. Routing protocols needs to be auto-reconfigurable. Routing protocols have influence on traffic latency, on networking overhead, on energy efficiency, on the speed of network recovery in case of failures, on traffic assurance. Three main classes of routing protocols for energy-efficient wireless sensor networks have been identified. (a) Hierarchical/node-centric, this kind protocol aim at clustering the nodes so that "cluster heads" can perform some aggregation. (b) Location based/position-centric, this kind of routing class is based on the exact (GPS) or relative (triangulation, analysis of neighbor dependencies) position of the single nodes. The distance between sensor nodes can be used to estimate the required transmission power which facilitates energy efficient routing. (c) Data-centric where the routing is driven by the query of the application, not on the identity of the involved nodes or sensors. Routing used for MANETs are AODV, DSR, OLSR, TORA, ZRP and etc. In military sensor network AODV can be used but some modification is necessary for supporting the continuity when the sensors are moving. In the future, disruption tolerant networking (DTN) techniques [19], [20] may receive further attention. These help to provide end-to-end communications in networks with large delays and/or frequent interruptions. Also the connection of the sensor network through the network gateways to the end application might profit from this approach - especially if this reach-back capability is not always present as in the case of the unmanned aerial vehicles (UAV) relay.

4.4 Transport Layer

Transport layer is responsible for end to end reliable data transfer. Standard protocols for transport layer are TCP and UDP. TCP provides complete reliability, The TCP protocol stack is complex to be implemented in a resource constrained sensor node. The overhead from headers can be quite large, particularly for small messages. UDP is a best-effort service and does not guarantee reliable delivery of information. Sensor Transmission Control Protocol (STCP): a generic, scalable and reliable transport layer protocol for sensor networks where a majority of the functionalities are implemented at the base station. STCP offers controlled variable reliability, congestion detection and avoidance, and supports multiple applications in the same network. In military sensor network STCP is prominent.

4.5 Application Layer

The services provided by application layer include traffic management and admission control functionalities, multimedia encoding techniques, flexible and efficient applications and middleware techniques. Admission control has to be based on QoS requirements of the overlying application. In military sensor network for multimedia application it need to provide differentiated service between real-time and delay tolerant applications and loss-tolerant and loss-intolerant applications. As far we know there is no admission control algorithm particularly for wireless sensor network. So in military sensor network for multimedia application, energy efficient admission control algorithm is necessary in application layer. The design objectives of a coder for multimedia application in military sensor networks are (a) high compression efficiency (b) low complexity and (c) error resiliency. Compared to the predictive coding such as MPEG or H.26X, pixel-domain Wyner-Ziv encoding is much simpler and can be used for multimedia application in military sensor network. But there is still a lack of practical solutions in Wyner-Ziv and it is a open research issue. The development of efficient and flexible system software to make functional abstractions and information gathered by scalar and multimedia sensors are available to higher layer applications is one of the most important challenges faced by researchers to manage complexity and heterogeneity of sensor system in military sensor network.

In military sensor network, resource constrained, low power scalar sensors can be used for simpler tasks such as detecting scalar physical measurements, while some resource-rich and high power devices are responsible for more complex tasks as audio or video signals. Data processing and storage can be performed in distributed fashion.

4.6 Cross Layer Design

Military sensor network consists of mobile sensors as well as with static sensors, multimedia services are included and different networks are interworked. So, end to end QoS, adaptation with the changing of channel characteristics due to adverse condition in the battle field, interoperability are great requirements for military sensor network. Cross layer design can be a good solution to design reconfigurable and adaptive network with optimization of constrain of sensor network like energy, bandwidth. A variety of adaptive cross-layer technologies already exist that have been developed and deployed within the commercial domain. However, most deployed techniques are singularly-adaptive and do not typically address the complete problem space of (1) adaptation in support of application QoS requirements, (2) adaptation in reaction to harsh, time-varying channel conditions, and (3) adaptation of technology to support seamless interoperability in a heterogeneous network. So, the interworking among PHY, Data Link, MAC, Network, Transport and Application layers will be a next challenging cross layer design for military sensor network.

V. Conclusion

Realizing all the challenges discussed above and the barriers such as bandwidth, energy, processing capability, bit error rate, latency, and mobility constraint limited modeling capability for scaling distributed algorithms, if it is possible to compromise among them then military sensor network will come in true in near future. Currently, much research effort is focused on developing 'simple' sensors, such as acoustic, temperature, and moisture detectors. But during the coming years, the research and development community will continue to make significant strides in sensor design, wireless communication, and signal processing to develop large-scale, low-cost, and more sophisticated sensor networks for intelligent information gathering.

As most of the elemental knowledge of sensor networks is basic on the defense application at the beginning, especially two important programs the Distributed Sensor Networks (DSN) and the Sensor Information Technology (SenIT) form the Defense Advanced Research Project Agency (DARPA), sensor networks are applied very successfully in the military sensing. The US Department of Defense, the Defense Advanced Research Projects Agency (DARPA), and the US Air Force Research Laboratory have envisioned rapidly deployable and self-assembling wireless sensor networks on a cooperative micro unmanned air vehicle (UAV) team that will offer unprecedented capability in battlefield intelligence and information dominance. Mercury Computer Systems introduced sensor network architecture for use by the military on the "next-generation" battlefield. The company says its Converged Sensor Network Architecture connects sensors, embedded computing systems; data storage and image display units, and sends the sensor data over an IP-based network.

References

[1] Michael Winkler and et al., "Theoretical and practical aspects of military wireless sensor networks," Journal of Telecommunication and Information Technology, February 2008.

[2] Xiaojiang Du and Hsiao-hwa Chen, "Security on wireless sensor network," IEEE Wireless Communications, August 2008.

[3] Hiren Kumar, Deva Sarma and Avijit Kar, "Security threats in wireless sensor networks," IEEE A&E System Magazine, June 2008.

[4] Yi Zou and Krishnendu Chakrabarty, "Distributed mobility management for target tracking in Mobile Sensor Networks," IEEE Tran. on Mobile Computing, August 2007.

[5] B.Y. Liu, P. Brass, O. Dousse, P. Nain, and D. Towsley, "Mobility improves coverage of sensor network," Proc. of MobiHoc, 2005.

[6] Y. G. Mei and et al., "Deployment strategy for mobile robots with energy and timing constraints," Proc. IEEE International Conference on Intelligent Robots and Systems, 2005.

[7] R. Rao and G. Kesidis, "Purposeful mobility for relaying and surveillance in mobile ad-hoc sensors networks," IEEE Trans. on Mobile Computing, 2004.

[8] G. Wang, G. Cao, and T. La Porta, "Movement-assisted sensor deployment," IEEE Trans. on Mobile Computing, 2006.

[9] Crossbow MICA2 Mote Specifications. 〈http://www.xbow.com〉.

[10] Crossbow MICAz Mote Specifications.

〈http://www.xbow.com〉.

[11] E. Gurses, O.B.Akan, "Multimedia communication in wireless sensor networks," Annals of Telecommunications, July-August 2005

[12] S. Misra, M. Reisslein, G. Xue, "A survey of multimedia streaming in wireless sensor networks," IEEE Communication Surveys & Tutorials, 2008.

[13] M. Rahimi and et al., "Cyclops: In Situ Image sensing and interpretation in wireless sensor networks," ACM Conference on Embedded Networked Sensor Systems (SenSys), November 2005.

[14] Ian F. Akyildiz and et al., "A survey on wireless multimedia sensor networks," Computer Networks, March 2007.

[15] A. Aaron and et al., "Coding for video: applications to compression and error resilience," IEEE Data Compression Conference(DCC), March 2003

[16] A. Aaron, E. Setton, B. Girod, "Towards practical Wyner- Ziv coding of video," IEEE International Conference on Image Processing (ICIP), September 2003.

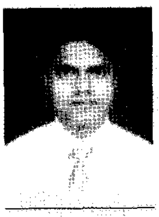
[17] G. Zhou and et al., "MMSN: Multi-frequency media access control for wireless sensor networks," IEEE INFOCOM, 2006.

[18] E. Egea-Lo′pez and et al., "A wireless sensor networks MAC protocol for real-time Applications," Journal Personal and Ubiquitous Computing, Feb., 2008

[19] Delay tolerant networking research group of the IRTF, http://www.dtnrg.org and http://www.irtf.org/

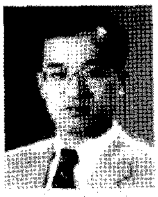
[20] V. Cerf and et al., "Delay-tolerant networking," RFC 4838, April. 2007.

약 력



Mohd. Noor Islam

2003년 B.Sc in Electrical and Electronic Engineering from Khulna University of Engineering and Technology (KUET), Khulna, Bangladesh
2004년 ~ 2007년 Lecturer, EEE Dept, KUET, Khulna, Bangladesh.
2007년 ~ till now Assistant professor, EEE Dept. KUET, Khulna, Bangladesh.
2007년 ~ till now M.Sc. in Electronics Engineering Department, Kookmin University, Seoul, South Korea.
Interests : Self-organization, Coverage and connectivity analysis for dense wireless sensor network, Multi-channel assignment, and Cross-layer design for wireless sensor network



장 영 민

1985년 경북대학교 전자공학과 학사
1987년 경북대학교 전자공학과 석사
1999년 Univ. of Massachusetts 컴퓨터과학과 박사
1987년 ~ 2000년 한국전자통신연구원(ETRI) 이동통신연구단 선임연구원
2002년 ~ 현재 국민대학교 전자공학부 교수
관심분야 : 4G 통신 네트워크 및 IT 융합

최 선 웅

1998년 서울대학교 전산과학과 학사
2000년 서울대학교 전산과학과 석사
2005년 서울대학교 전기, 컴퓨터 공학부 박사
2005년 ~ 2007년 삼성전자 정보통신총괄 책임연구원
2007년 ~ 현재 국민대학교 전자공학부 조교수
관심분야 : 무선 네트워크, 네트워크 자원관리, 시스템 성능 평가

박 상 준

1988년 경북대학교 전자공학과 학사
1991년 경북대학교 전자공학과 석사
2006년 North Carolina State University 컴퓨터과학과 박사
1990년 ~ 2001년 국방과학연구소 선임연구원
2006년 ~ 현재 한국전자통신연구원(ETRI) 팀장
관심분야 : 센서네트워크, Multi-sensor data fusion 및 target tracking, Hardware-In-The-Loop Simulator for Wireless Sensor Network