Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 11, Issue 2, June 2020: 538-544

Sustaining Battery Lifetime and Reliable Communication in Surveillance Applications of WSNs

Dr. S. Arif Abdul Rahuman [1], Dr. Babu Renga Rajan S.[2], Dr. R. Dinesh Kumar[3] & Dr. G. Uma Gowri [4]

[1]Professor, Department of CSE, Universal College of Engineering and Technology, Vallioor, Tirunelveli-627117, India.

[2]Professor, Department of CSE, PET Engineering College, Vallioor, Tirunelveli-627117, India.

[3]Associate Professor, Department of ECE, Kings Engineering College, Chennai-602117, Tamilnadu, India.

[4]Professor & Principal, Department of ECE, Madha Institute of Engineering and Technology, Chennai-600122, India.

Email: jnellai@gmail.com[1], babusbr7@gmail.com[2], mail2rdinesh@gmail.com[3], umagowri.g@gmail.com[4]

Abstract: System of system common operating environment supports the system. SOSCOE provides reusable software architecture for platform and battlecommand application via low bandwidth Adhoc network. Since,mostofthesystemoperatesinremoteenvironmentwithbatterysupport,powerconsumptionis aseriousissue.Systemwithmany nodal points has to be encrypted strictly to prevent the network from attacks (simply hacking). Use of instruments with less powerconsumption, particularlycustomdesignhardwareandwirelesssensors orsensorswill helptotacklethisproblem. This paper gives a detailed analysis on sustaining battery lifetime and reliable communication in surveillance and medical applications of WSNs.

Keywords: Battery lifetime, Reliable communication, Wireless sensor networks.

1. Introduction

Thisisourtimetochange ourbasic strategy from the 20th century, cold war model that relied on massive logistics buildup, heavybrigades,sequentialoperations,linearwarfareandintelligencegainedbydirectobservation/contact.FCSsupportsus against the current irregular warfare by providing light, agile Brigade Combat Teams with a small logisticsfootprintthatisnetworkedandcapableofconductingsimultaneousoperationstodirectlyattacktheenemycentersofcontrol andexploitstheintelligencegainedviaremotereconnaissanceandsurveillancesystems[1].

At the heart of the FCS, BCT is the network which will allow every FCS system from unmanned vehicles toprecision weapons to share the information and work together. The network will offer decision-making not just atthe brigade level, but all the way down to the battalion and company levels. The FCS allows the army to achievegreatersituationalawareness,improvedsurvivability,lethality,efficiencyandjointoperability.Ontoday‘sbattlefield, the availability of real-time information is vital for success.

FCS technology will allow the soldiers tosee first and understand first: from a position far away. Systems such as the Unattended Ground Sensor(UGS), Unmanned Ground Vehicles (UGVs) and Unmanned Aerial Vehicles (UAVs) will provide informationabout the enemy‘s position in individual buildings and neighborhoods, as well as over the bunkers. Wirelesssensors can be used in case of unattended war environments. This information will be fed into the network andimmediatelysharedwithbrigade,battalionandcompanycommanders,eventotheplatoonleaders.Thisnetworkedsurveillanceincreasesthereliabilityofinformationandreducestacticalrisktothesoldiers.Inshort,FCSprovidesenhancedsituationalawareness.Ontoday‘sbattlefield,precisionweaponsarenecessarytodefeatenemieswhoareoftenmixedwithcivilianpopulationsorhiddeninrestrictiveterrainsuchasmountainousregions.

FCSsystemssuchastheMountedCombatSystem(MCS),Non-LineofSight-Cannon(NLOS-C)andNon-LineofSight-Mortar(NLOS-M)combinedwithFCS‘sunmannedsystemsandthesoldiers,providetheabilitytodestroyenemyand increases the ability to identify targets and to engage with precision munitions that reduce the risk of collateraldamage. On today‘s battlefield, soldiers in complex environments are at risk within vehicles, due to the enemy‘suse of Improvised Explosive Devices (IEDs), Rocket-

Propelled Grenades (RPGs) and Anti-Tank Missiles. As thesoldiers move into complex terrain (urban areas) where the enemy is well hidden and traditional fighting vehiclesarelargelyineffective. Figure 1 shows the schematic diagram of border surveillance using sensor network.

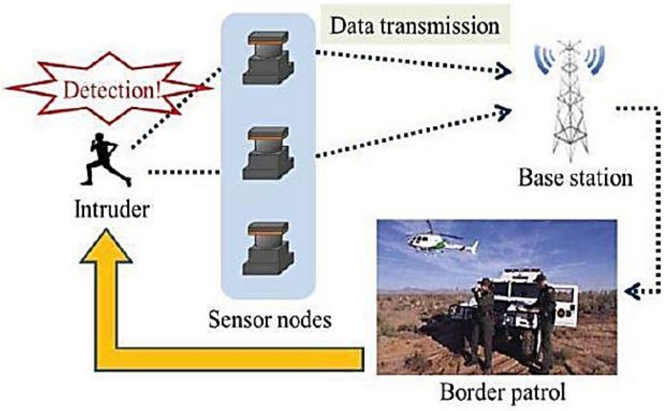

Figure 1. Border surveillance using sensor network [2]

2. Networking Architecture

The Army‘s FCS (BCT) network allows the FCS Family-of-Systems to operate as a system-of-systems in whichthecapabilitiesofallthesystemsaregreaterthanthesumofitsparts.Thenetworkenablestheinfantrysoldierstobetter understand and dominate the future battlefield at greater level. The network consists of five layers, whencombinedprovidesveryhighspeeddataflowwithinthenetwork.TheFCSnetworkpossessestheadaptabilityandmanagementfunctionalityrequiredtomaintainstandardservices,whiletheFCS(BCT)fightsonarapidlyshiftingbattlespacegivingthemthe advantageto seefirst, understandfirst,actfirstandfinishdecisively.

The Standards Layer is the foundation of the network. It provides the governance for which the other layers areshapedandformed.TheFCS(BCT)network conformstothestandardsdocumentationtoensurethatthenet-centric attributes like flexibility and adaptability on distributed computing environment. Information needs,information timeliness, information source and networked capabilities provide enhanced guidance to ensure thetechnicalexchangeofinformationandend-to-endoperationaleffectiveness.Uniformstandardallowsinteroperabilitywith othernetworks.

TheFCS(BCT)Family-of-

Systemsisconnectedtothecommand,control,communications,computers,intelligence, surveillance and reconnaissance (C4ISR) network by a multilayered transport layer with extremerange, capability and dependability. The primary function of the transport layer is to provide secure and reliabledata transfer over complex terrain. The network supports advanced functions like integrated network managementcapability, information assurance and information dissemination management to ensure dissemination of criticalinformation among sensors, processors and war fighters both within and external to the FCS (BCT)-equippedorganization.Figure 2 shows the cluster formation in the current scenario.

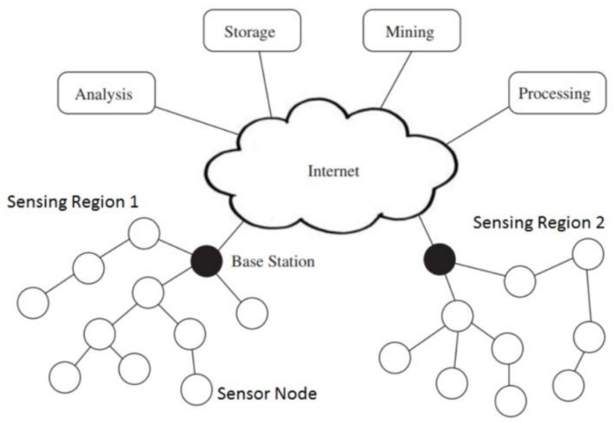

Figure 2. Cluster formation in the Current Scenario [3]

Heart of FCS (BCT) network is the Services Layer, commonly referred to as System-of-Systems CommonOperating Environment (SOSCOE) which supports multi mission-critical applications both independently andsimultaneously.Itisdesignedsothat,atanyspecificinstant,onecanincorporateonlythecomponentsthatareneeded for that particular instant. It enables advanced integration of separate software packages, independent oftheirlocation, connectivitymechanismandthetechnologyused fordevelopingthem.

TheApplicationsLayerisresponsibleforprovidingtheintegratedabilitytoassess,planandexecutethenetwork-centric mission operations by using a common interface and a set of non-overlapping functional servicesthat provides the full range of FCS (BCT) war-fighter capabilities. This layer combines ten software packages toenablefull interaction, integration andinteroperability between thesystemswith no hardware,softwareorinformation bank. It also allows cross Battlefield Functional Area (BFA)problem-solving, decision aiding,adaptable doctrine, tactics, techniques and procedures, reconfiguration of roles and levels of automation duringexecutiondevelopment,thebasicefficienciespromotion, technologyrefreshandinsertion.

3. ThePlatformandSensors

The Sensors and Platforms Layer is comprised of a distributed and networked array of multi-spectral sensors thatprovidestheFCS(BCT)withtheabilityto–seefirst.‖Intelligence,SurveillanceandReconnaissance(ISR)sensors are integrated onto all manned ground vehicles, all unmanned ground vehicles and all four classes of unmannedaerial vehicles within the FCS (BCT). To provide war fighters with current, accurate and actionable information,thedatafromthevariousdistributedISRandotherexternalsensorassetsaresubjectedto complexdataprocessing,filtering, correlation, aided target recognition and fusion. The 18 networked systems consist of eight mannedgroundvehicles,threeunmanned groundvehicles,fourunmanned aerial vehiclesandthreespecializeddevices.

AllSoldiersintheBrigadeCombatTeam(BCT)arepartoftheSoldierasaSystem(SaaS)overarchingrequirementthat encompasses everything the soldier wears, carries and consumes to include unit radios, crew served weaponsand unit specific equipment in the execution of tasks and the duties. All soldiers systems will be treated as anintegrated System of Systems (SoS). The soldier, as defined by Soldier as a System (SaaS) meets the need to perkupthecurrentcapabilityofallthesoldiers,regardlessofMilitaryOccupationalSpecialty(MOS)tocarryoutarmywarriortasksandfunctionsmoreproficientlyandeffectively.SoldierasaSystem(SaaS)establishesabaselineforcore soldier requirements and establishes the foundation for specific or mission unique soldier programs (Ground,Mounted and Air). It presents a fully integrated modular soldier that provides a balance of tasks and missionequipment in support of the soldier team: the current and the future force. FCS also enhances the SaaS withadditional benefits like joint embedded training: allowing the soldier to train anywhere, at any time, includingenroot to the battlefield [4]-[5].

4. MajorProblems

(1) One of the somber issues is the lifetime of the battery. Longer the lifetime of the battery, longer is the life ofthe soldier. Since the soldiers depend only on the system to identify and eliminate threads which affects hissurvivability,longlastingfastrechargeablebatteriesarerequired.Onesolutionforthisissueistoreplacethesensors with wireless sensors with novel distributed clustering algorithms embedded in it.

(2) It is very tricky toestablishcommunicationrelaysnearthebattlefield,asitbecomesatargettoenemyforces.Ifreliable communication could not be established, soldier can‘t obtain real-time war picture. For real-time situationalawareness, secure and reliable communication is the foremost criterion. More the number of node points, more isthe possibility for hacking and as a result providing reliable communication link in non-line of sight is a severeissue. The problem could be overcome by clustering all the nodes in distributed manner.

(3) When the battle fieldhastocoverwiderarea,signalstrengthbecomesweakerandthispavesawayforlosingthecollectedinformation.ThiscreatesaSNRproblemthathastobetakenintoaccount.Thiscanbeeliminatedcompletelybyincreasingthenumber of nodes in the network.

5. Conclusion

Supportingthesoldierwithrealtimesituationalawarenessandcooperativeoperability among forces to entire a mission successfully with low mortality rate is the fundamental thought,thereby enabling the soldier to see first, understand first and take action decisively. Fusing the data collected fromdissimilar reconnaissance vehicle, unattended ground sensors, unmanned aerial vehicles and live assets has to bemade successfully. After thecomprehensive study on the problems and issues concerning FCS, two foremost criterions have to be accountedprincipally: battery lifetime and reliable communication over disrupted terrains. This paper gives a detailed analysis on sustaining battery lifetime and reliable communication in surveillance and medical applications of WSNs.

References

[1] Huang, YM., Hsieh, MY., Sandnes, F.E. (2008). Wireless Sensor Networks and Applications. In: Mukhopadhyay, S., Huang, R. (eds) Sensors. Lecture Notes Electrical Engineering, vol 21. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-69033-7_10.

[2] D. Arjun, P. K. Indukala and K. A. U. Menon, "Border surveillance and intruder detection using wireless sensor networks: A brief survey," 2017 International Conference on Communication and Signal Processing (ICCSP), 2017, pp. 1125-1130, doi: 10.1109/ICCSP.2017.8286552.

[3] https://iot4beginners.com/basics-of-wireless-sensors-networks-topologies-and-application

[4] Hua, G., Li, YX., Yan, XM. (2011). Research on the Wireless Sensor Networks Applied in the Battlefield Situation Awareness System. In: Shen, G., Huang, X. (eds) Advanced Research on Electronic Commerce, Web Application, and Communication. ECWAC 2011. Communications in Computer and Information Science, vol 144. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-20370-1_73.

[5] Juneja, D., Sharma, A., Sharma, A.K. (2011). Wireless Sensor Network Security Research and Challenges: A Backdrop. In: Mantri, A., Nandi, S., Kumar, G., Kumar, S. (eds) High Performance Architecture and Grid Computing. HPAGC 2011. Communications in Computer and Information Science, vol 169. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-22577-2_55.