

Networked Intelligent Munitions and Sensor Systems

Michael I. Brownfield, Scott D. Lathrop, Sally A. Brownfield, Mongi Bellili

Electrical Engineering and Computer Science

United States Military Academy

West Point, New York

{[michael.brownfield](mailto:michael.brownfield@us.army.mil), [scott.lathrop](mailto:scott.lathrop@us.army.mil), [sally.brownfield](mailto:sally.brownfield@us.army.mil)}@us.army.mil

Abstract - This paper presents a networked intelligent munitions and sensor system (SUREFire) that provides a key decision-making tool for military command and control. Based on fundamental principles of network science, SUREFire employs collaboration between minefield sensors to improve the resolution of data collection and the corresponding application of lethal effects on an enemy force. SUREFire extends medium access control (MAC) protocol algorithms with energy-efficient, fault-tolerant, distributed communication protocols. The resulting system extends the munitions system lifetime; fuses data from multiple sensors to maximize target signature and trajectory; facilitates off-line collaboration to optimize the number of enemy targets in the engagement area; and offers positive munitions control mechanisms to meet the U.S. Mine Use policy goals set for 2010. Consequently, the overall intent of this paper is to describe the system prototypes and multi-modal sensor network experiments that validate the enabling technologies for a system which increases situational awareness to battlefield commanders.

I. INTRODUCTION

The application of network science to real-world challenges requires identifying and exploiting relevant, inter-connected actions occurring within and across the physical, information, social, and cognitive domains. Over the past decade, the United States Department of Defense (DoD) has intensified the research and development of highly technical weapons designed using the principles of network science. Intelligent sensor and weapon systems enable the military to attain information superiority and battlefield dominance at the strategic, operational, and tactical levels [1]. Network centric warfare (NCW) applies the principles of network science towards military operations by linking sensor data, intelligence tools, data distribution networks, and human experience. NCW capitalizes on the advantages of information superiority to create a multi-tiered common operating picture of the battlespace. With timely dissemination, this shared situational awareness allows units of varying sizes and missions to self-synchronize their actions and achieve desired battlefield effects [2].

The SUREFire networked intelligent munitions and sensor system provides valuable sensor and response mechanisms that enhance NCW operations. This paper provides the motivation and system description of SUREFire and details the aspects of network science that such a system leverages to achieve significant political, social, and military advantages.

II. APPLIED NETWORK SCIENCE PRINCIPLES

Network science describes mechanisms to categorize and relate seemingly random data into useful, relational information. SUREFire realizes these mechanisms by gathering raw data, predicting future enemy behavior, and controlling battlefield effects. These mechanisms provide an information advantage to the decision maker.

Understanding enemy intent and the location of both friendly and enemy forces on the battlefield allows

commanders to maximize the lethality of munitions systems directed at the enemy and away from friendly forces or innocent civilians. Once forces engage in combat action, the situational awareness of enemy forces and adjacent friendly units quickly dissolves to chaotic, segmented reports filtering to higher headquarters. Clausewitz describes this phenomenon as “the fog of war” [3]. The force that gathers and processes live battlefield data more efficiently brings order to this chaos, effectively achieving information superiority and enabling commanders to exploit enemy vulnerabilities while protecting their own force.

From a network science perspective, a networked configuration can achieve such order by classifying the domain entities, their behaviors, and inter-relationships—otherwise known as network knowledge. A network may be described as “the interaction between two or more entities regardless of domain, or level of abstraction” [4]. The entire universe is interwoven in a vast array of network domains with such examples as biological, social, physical, cognitive, and information domains. The Moxley Network Science Methodology, $M[d, b] = N_K$, relates network knowledge (N_K) as a function of behaviors (b) and domains (d) [5]. Figure 1 shows a graphical representation of how SUREFire applies network knowledge to detect the enemy in the physical domain, creates and applies predictive models of future behavior in the social and information domains, and provides the commander situational awareness and battlefield agility in the cognitive domain.

Physical Domain: The physical domain defines *entities* and their fundamental capabilities. For example, a military force contains quantifiable levels of raw combat power. Analysts consider the number of soldiers, the level of training, the availability of weapon systems, and the location of the force to calculate the effective combat power at a specific place and time in the physical domain. Sensors in the physical domain gather key behaviors of enemy forces that other domains use to assess enemy intent and to increase situational awareness. Available battlefield sensors include acoustic, radio intercept, radar, infrared, magnetic, and seismic sensors. Battlefield entity behaviors include enemy weapon platform

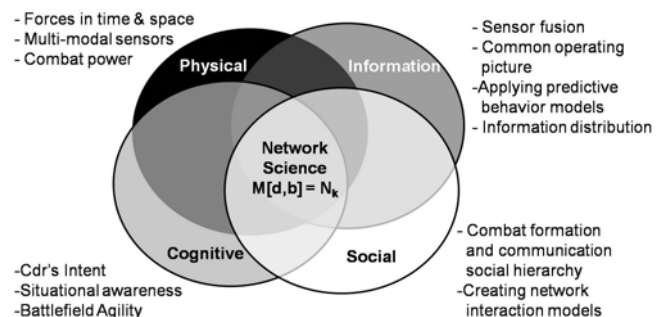


Figure 1. SUREFire Applied Network Science

employment, current enemy locations, enemy speed and direction of travel, physical interaction between enemy units, and the associated inter- and intra-unit communications patterns. In the physical domain, SUREFire incorporates sensors to gather data on the enemy behavior and provides additional networked control features to increase the ability of munitions systems to shape desired battlefield effects. Recognizing the tremendous value added by this combination, the Army's future combat systems are developed with the intention of making every possible munitions system into a networked sensor platform.

Information Domain: The information domain assimilates the collected data into relevant information and provides the infrastructure to distribute the information. SUREFire fuses enemy location and orientation to provide relational information useful for predicting organizational hierarchy and future behavior models relevant to the social domain. Figure 2 shows a depiction of raw battlefield data: unit battlefield location, vehicle type (acoustic signature), and direction of travel. The formation indicates that it is a company that is probably part of a battalion-sized task force [6]. The tank company will respond to the unit's center of gravity – typically the commander's (CDR) vehicle. The unit formation signifies that the force is alert with a heightened defensive protective posture in anticipation of a possible enemy attack, but it is not deployed to attack. The information domain uses social models similar to the unit tank formation to predict future enemy behavior and disseminates the predictions to other domains. The U.S. military command and control system which distributes a common operating picture to the operational units is the Force XXI Battlefield Command Brigade and Below (FBCB2). Providing the commander enhanced situational awareness in the cognitive domain allows him to redirect assets in the physical domain for increased combat power. SUREFire creates network information by collecting and fusing enemy vehicle locations, trajectories, and seismic and acoustic signatures that can be used in the cognitive domain to infer enemy vehicle types.

Social Domain: The social domain applies tools such as the Moxley Methodology to create intra- and inter-network relational models for use in developing network knowledge in the information domain. Analysts use battlefield unit movements and radio communications patterns to detect and identify enemy formations, create predictive models of future

behavior, and target enemy centers of gravity. Grouping units like the tank company in Figure 2 into higher echelon formations creates a social hierarchy of multi-tiered units. Identified command vehicles can be tracked as priority intelligence requests (PIRs) to filter raw data noise and clearly monitor the center of gravity for each unit. Additionally, units self-organize to conduct specific missions. Army units task-organize into task force units at battalion level and above. Analyzing a history of the seemingly random behaviors of vehicles and units on the battlefield produces probability clustering coefficients on the edges between entities based upon the frequency of interaction. These clustering coefficients dissipate the randomness to distinguish social interaction patterns common to a typical military unit hierarchy. Units with high clustering coefficients and small average path lengths between elements form into Small World Networks [7]. Formulating interrelations of seemingly random behaviors and developing behavioral templates based upon previous actions on the battlefield provides the cognitive domain the ability to predict future entity behavior.

Cognitive Domain: In the cognitive domain, commanders apply network knowledge from the social and information domains to gain situational awareness and provide predictability of future behaviors. Units at all levels self-synchronize their actions by applying their commander's intent to the common operating picture of current blue force (friendly) and red force (enemy) behaviors. As friendly neighboring units respond to enemy actions in their engagement areas according to a shared higher commander's intent, unit commanders autonomously adjust their actions and work towards common objectives. Unit self-synchronization allows the commander to increase the value of his physical entities, soldiers and weapons towards meeting the objectives of higher command levels.

Figure 3 summarizes the SUREFire culmination of these network science concepts in translating domain behaviors into network knowledge. Figure 3a represents raw data collected by SUREFire in the physical domain. Note that the individual entities appear random in nature. Figure 3b represents the transformation from the physical domain to the information and social domains. SUREFire leverages the raw data in the physical domain to aid in establishing inter- and intra-network relationships via clustering coefficients. Integrating this data with other sensor information, such as electronic communications interception, terrain characteristics, situation-based tactical behavior, and doctrinal templates, facilitates the development of social hierarchies as shown in Figure 3c. The cognitive domain, or commander, can use the hypothesized enemy red force template to anticipate the enemy's intentions and attain information superiority.

The progression of raw data from the physical domain to network knowledge developed from multiple interactions among other domains increases the situational awareness for the individual commanders on the battlefield and allows them to self-synchronize to meet common objectives. Clausewitz's "fog of war" begins to clear.

III. SUREFIRE DESIGN CONSIDERATIONS

SUREFire implements network science by combining sensor inputs from the physical domain, disseminating the

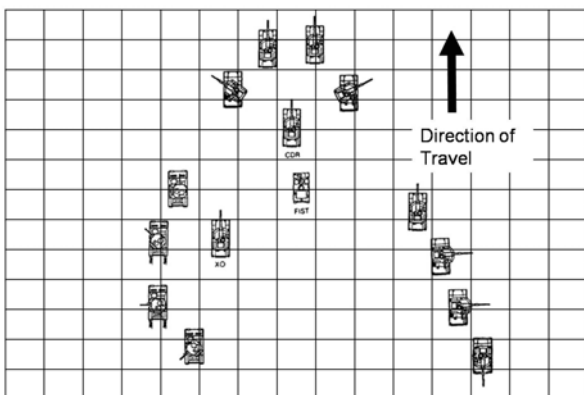


Figure 2. Armor Company Formation [6]



Figure 3a. Random Data

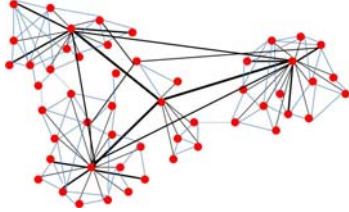


Figure 3b. Social Clustering Coefficients

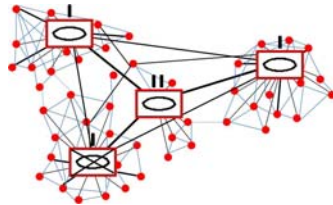


Figure 3c. Small World Networking

data in the information domain, developing network knowledge in both the information and social domains, and providing situational awareness for a commander or munitions control system to optimize the deployment of weapons systems in the cognitive domain. Advancing technology permits this intelligent munitions system to meet many of the needs of a modern day battlefield.

Relevant to the physical and social domains, international pressure has outlawed persistent minefields of the past. The U.S. has committed to develop intelligent, non-persistent munitions systems that safely retain the combat effects of defensive minefields and join the world in seeking safer solutions to unintentional collateral damage. The systems must respond immediately to the threat, yet consume power at a rate to operate unattended for more than 30 days without recharging. Additionally, these systems must be flexible with remote reprogramming capability to dynamically create maneuver space for friendly forces and lethal obstacles for the enemy. When the battle is complete, the systems must have a mechanism to disarm or destroy the munitions to protect the innocent civilians and the environment. The SUREFire intelligent munitions system addresses all of these design requirements.

A. Minefield International Treaty Agreements

For years, unexploded mines were a hazard which endangered innocent lives in war-ravaged societies. The mapping and marking of minefields has become increasingly difficult with modern aerial-delivered, scatterable mines. In 1999, concerned international parties of the Ottawa Treaty committed to not use, produce, or transfer anti-personnel landmines. However, the U.S. did not sign this treaty since it

considers the deployment of land mines a vital part of its military strategy in Korea. In 2004, the U.S. committed to several humanitarian landmine policies that protect against this unintended collateral damage. By 2010, the U.S. will no longer use persistent anti-personnel (AP) or anti-tank (AT) land mines. Future developed intelligent munitions systems must have a combination of self-destruction (SD) and/or self-deactivation (SDA) mechanisms [8]. Not only does SUREFire have these mechanisms, it can also retrofit the existing stockpile of “illegal” persistent mines by adding an intelligent triggering system. SUREFire’s positive control triggering mechanism upgrades the persistent mines to non-persistent as the electronic trigger mechanism is inert after the battery discharges. Additionally, SUREFire’s over-the-air reprogramming (OTAR) feature reduces the risks to innocent lives by enabling the combatants to actively control the mode and duration of the minefield from remote locations before, during, and after the battle. The U.S. Army remains committed to protecting innocent lives, and SUREFire offers a viable, technologically-sound option for meeting that commitment.

B. Maximum Lethality Algorithm

Networked munitions fields are technologically-enhanced minefields that wirelessly communicate to increase their effectiveness. SUREFire integrates an intelligent multimodal sensor array with a wireless communications platform for a conventional land mine or an advanced area munitions system. The U.S. Army’s Intelligent Munitions System (IMS) is an example of an advanced, ground-based weapon that provides area coverage by launching anti-tank munitions into the air to seek multiple targets out to a radius of 100m. Global positioning system (GPS), acoustic, passive infrared (PIR), and magnetic sensors allow a networked munitions system to determine a target’s type, proximity, and direction of travel. SUREFire uses this information to allow deeper penetration by an enemy formation prior to triggering an ambush. This ambush is an extension of a basic minefield deployment technique called *Daisy Chaining*, first introduced in Finland in 1939 [9]. Once the enemy sets off one of the mines, all others linked to it detonate and destroy the rest of the unit which had unknowingly entered the minefield.

Similarly, the munitions in SUREFire exchange location and orientation information upon deployment to establish relative spatial awareness of their neighbors and employ a maximum lethality algorithm. With this algorithm, each munitions system makes “silent decisions” to engage or defer targets to a neighbor if the predicted trajectory falls into the coverage of a neighboring mine. Once an enemy lead vehicle gets to the farthest edge of the munitions field based upon direction of travel and is not on a trajectory for a follow-on munitions system, the last mine breaks radio silence, broadcasts a *goodbye* message to neighboring mines, and self-detonates. Depending on the SUREFire programmed operational mode, the other mines will then either arm for immediate sensor-activated detonation or remove the exploded mine from their neighbor lookup tables and continue with a maximum lethality handoff algorithm.

Enemy vehicles remaining in the munitions field would be unable to retreat back across the mines they have already *safely* crossed. The software implementation section in this paper presents these operational modes in more detail.

C. Minimize Risk to Friendly Forces and Civilians

SUREFire minimizes the risk of friendly and civilian casualties by integrating an anti-fratricide beacon called Identify Friend or Foe (IFF), by providing the ability to remotely reprogram the system to a neutral *check-fire* state when civilians are temporarily in the area, or by triggering a *deactivation/detonation* mode when the battle is over. The IFF beacon provides a temporary, short-range deactivation for munitions in close proximity of a beacon transmitter. A system timeout rearms the system when the IFF message GPS location field indicates a safe, pre-defined distance or the SUREFire IFF trigger deactivation subsystem times out.

D. Battlefield Flexibility

SUREFire provides many capabilities to enhance a commander's flexibility on the battlefield. For instance, the SUREFire sensor fields provide the battlefield leaders with increased situational awareness, and the self-synchronizing maximum lethality detonation system automatically adjusts the munitions field to maximize the destruction of the enemy formation. Additionally, the OTAR capabilities provide the leader with the ability to dynamically adjust the munitions detonation schemes to match the approaching threat, suspend detonation of munitions to expand friendly forces' maneuver space during a counterattack, or neutralize the munitions when the battle is complete. SUREFire integrates intelligent sensor, processor, and communications platforms whose operational mode can be manually or remotely configured to respond dynamically to changing battlefield conditions.

E. Energy-Efficient Sentinel-MAC Protocol Design

SUREFire employs an energy-efficient wireless sensor network (WSN) medium access control (MAC) protocol called Sentinel-MAC (Sentry-MAC) that increases the sensor network lifetime by self-synchronizing the individual nodes in the network. Sentry-MAC establishes a sensor-field sleep rhythm, as shown in Figure 4, which allows all sensor platforms except for the sentinel sensor platform, or sensor node, to transition to a sleep state when no sensors in the network are triggered. Periodically rotating the point coordination function (PCF) distributes sentinel responsibilities among all eligible nodes to extend network lifetime. Both the SUREFire networked munitions system and the sensor field can capitalize on Sentry-MAC, but the SUREFire munitions system would have to give up radio silence to take full advantage of this network lifetime extension protocol. Studies have shown that implementing similar sleep algorithms can increase network lifetime by more than 800% [10].

Sentry-MAC Sleeping Scheme: Sentry-MAC self-elects a sensor field cluster head called the Sentinel to serve as the sensor network sentry while the other nodes cycle to sleep. Figure 4 shows a cyclic beacon and sleep period that creates

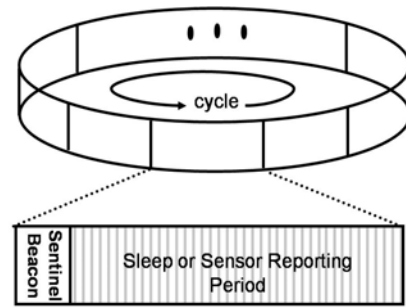


Figure 4. Sentinel "All's Well" Beacon Cycle

sleep opportunities to optimize the network lifetime. Given sensor ranges of 200 meters, the Sentinel can broadcast an "All's Well" message beacon with a sleep duration proportional to the maximum closure rate of an enemy vehicle, the longest diagonal across the sensor network, and the system re-initialization requirements.

When the Sentinel senses a target during a sleep cycle, it broadcasts a "Sentinel Alarm" beacon along with a node reporting sequence at the next scheduled beacon time. Each sensor platform will then transmit its latest sensor readings following the Sentinel's broadcasted schedule. The munitions platform intelligence data collection system matches the received sensor readings with the sender's existing GPS coordinates to determine target signature, location, direction of travel, and speed. Once the network sensor reports cycle through several iterations without positive sensor trigger reports, the Sentinel broadcasts an "All's Well" to send the sensor platforms back to sleep to conserve vital network energy. In effect, the sensor network self-synchronizes in the physical and information domains.

The significant energy savings provided by Sentry-MAC are a result of the reduction in the amount of time all nodes must monitor their sensors and their radios. Receiving the beacon is the only time that all nodes will be awake unless the beacon contains an "Alarm" or "Sentinel Election" message.

Sentry-MAC Rotation Scheme: Sentry-MAC periodically elects a new Sentinel node to distribute energy requirements equally among all of the nodes using a resource adaptive voluntary election (RAVE) scheme [11]. RAVE is a passive cluster coordinator election scheme similar to Low-energy Adaptive Clustering Hierarchy (LEACH) [12], but the RAVE algorithm allows for a self-election based on each node's available battery resources, not a strict probability-based calculation. Power-aware clustering TDMA (PACT) [13] is another passive election scheme which addresses battery resources as a discriminator for cluster head eligibility, but again, the election is based on probability.

Sentry-MAC's resource levels, shown in Table 1, facilitate the rotation of the Sentinel duties among the nodes with the most available resources. The associated voltage levels can be selected to achieve a duty rotation period based upon battery characteristics and minimum system voltage requirements. The critical resource level algorithm assigns a node's resource level (RL) according to the most critical

resource and provides graceful network degradation until all nodes' energy levels are exhausted.

To reduce the overhead of exchanging available power resource updates (an $\Theta(n^2)$ algorithm), the distributed RAVE algorithm establishes the next Sentinel by having each node calculate an individual election MAC contention backoff period based upon the node's available resources using the equation:

$$ElectionBackoff = Random(2^7) + (RL * 128). \quad (1)$$

$Random(2^7)$ is a random number between 0 and 127, RL is the node's available resource level multiplied by 128 to offset the random number into an eligibility band, and $ElectionBackoff$ is the number of contention slots a node will back off before sending a self-election packet (Table 2). A Sentinel node signals for a new election whenever it transitions to a lower energy state or approaches a default changeover frequency. Nodes immediately calculate an election contention backoff when they encounter a periodic or signaled election. The new Sentinel is the *volunteer* node that successfully transmits a self-election message after the election beacon message.

The distributed system's fault tolerance mechanism works by requiring a three-way confirmation handshake between the outgoing and incoming Sentinels. In the event of a Sentinel node failure, the sensor nodes will automatically conduct an election with a peer confirmation mechanism after waiting for three consecutive missed Sentinel beacons. RAVE also uses this timeout driven peer-election method to initially self-configure the cluster.

F. Sensor Field Design

A SUREFire sensor field complements the SUREFire IMS network to determine the target type, speed, and direction. The nine sensor network prototype, shown in Figure 5, brackets the enemy target using passive infrared (PIR) sensors and collaborates to calculate vehicle location. This system also validates the energy-efficient Sentry-MAC.

IV. SUREFIRE DESIGN IMPLEMENTATION

A team of cadets and faculty in the U.S. Military Academy

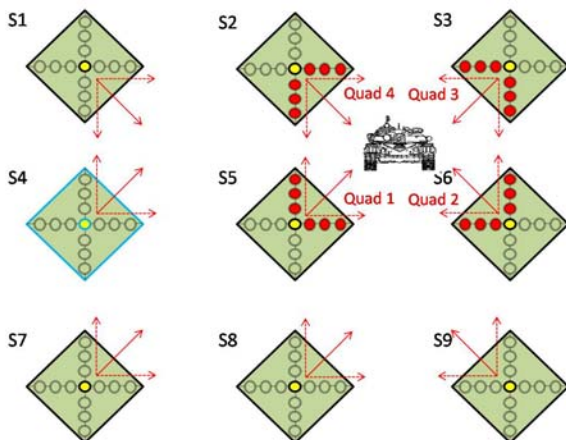


Figure 5. SUREFire Sensor Field

Table 1. Battery Resource Level

Battery Pwr Level	Power Level Nomenclature	Voltage Range (volts)
0	High	$2.6 < Pwr \leq (3.0-3.6)$
1	Med	$2.4 < Pwr \leq 2.6$
2	Low	$2.1 < Pwr \leq 2.4$
3	Min	$Pwr \leq 2.1$

Table 2. RAVE Election Contention Backoff

Resource Level (RL)	Election Contention Backoff Random(2⁷) + (RL * 128)
0 High	0 to 127 slots (0ms to 2ms)
1 Med	128 to 255 slots (2ms to 4ms)
2 Low	256 to 383 slots (4ms to 6ms)
3 Min	384 to 512 slots (6ms to 8ms)

Department of Electrical Engineering and Computer Science implemented both the networked intelligent munitions system and the accompanying networked sensor field as a proof of concept prototype. SUREFire won the 2008 Secretary of Defense Network Science Award for an innovative application of network science.

A. Hardware Design

SUREFire's networked intelligent munitions system was designed to demonstrate the effectiveness of the maximum lethality algorithm and to test the feasibility of SUREFire's enabling technology. The system must be able to determine the direction of travel for a vehicle using a small magnetometer, and the *localized relative* GPS accuracy must be less than 3m to assure that each node is aware of its neighbor's location. The absolute GPS accuracy is normally 10m, but the system might be able to achieve $\pm 3m$ when considering relative GPS data. The results of the enabling technology testing are presented in Section V.

MICAz Mote Platform: Figure 6 illustrates the SUREFire munitions subsystems. The base component for the wireless sensor network prototype was the Crossbow MICAz. The MICAz mote complies with the IEEE/ZigBee 802.15.4 wireless personal area network-low rate (WPLAN-LR) standards and communicates 250kbps at 2.4GHz [14]. The MICAz also provides the capability for hardware accelerated AES-128 encryption. The encryption coupled with a GPS-enabled timestamp provides security protection against a replay attack. The system also employs three Crossbow daughter boards to ease integration and provide competitive system specifications for their size and cost:

GPS: The MTS420CC GPS Weather Sensor Board uses a Leadtek 9546 GPS integrated circuit to provide an absolute location accuracy of 5m with a 50% confidence and 10m with a 95% confidence interval. SUREFire uses this feature to attain an improved location accuracy using relative location data [14][15].

Magnetometer: The MTS-310 sensor daughter board provides a dual-axis magnetometer to determine the vehicle direction of travel. The magnetometer has a 27 micro gauss resolution and can detect a vehicle at a radius of 5m [14].

Infrared Emitter/Detector Pair: The SUREFire indoor demonstration uses four Sharp IR sensor pairs to determine the direction of travel for non-ferrous model tanks. Figure 6 shows the key components of the demonstration prototype.

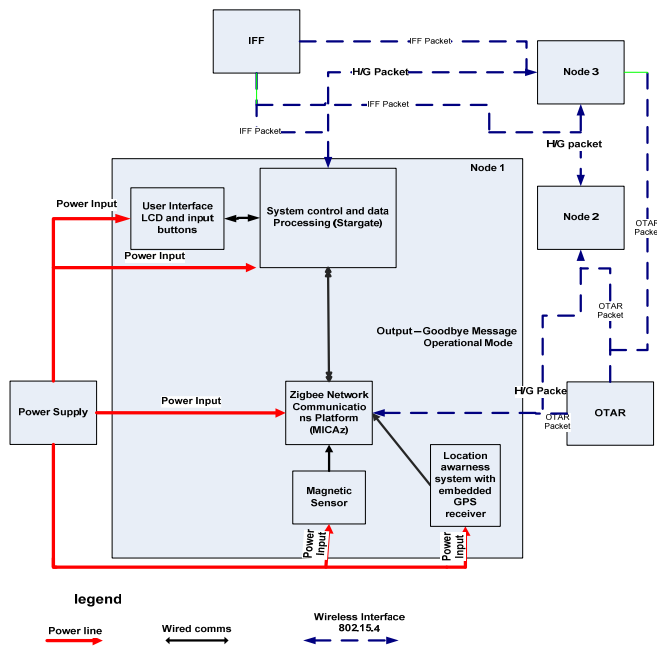


Figure 6. SUREFire System Block Diagram

Passive Infrared (PIR) Sensors: The area sensor field prototype employs a set of four Parallax PIR (555-28027) sensors to collaborate and determine the location of a target traversing a grid of nine sensor nodes.

System Menu LCD and Data Fusion Processor: The LCD screen system menu for a soldier manually programming a ground munitions system is controlled by a 400 CA STARGATE. The STARGATE has a diverse array of system interface ports and a 32-bit, 400 MHz Intel PXA255 XScale RISC processor for additional processing power while fusing multiple sensor data to provide better resolution for a target's type, speed, and direction of travel [14].

The team integrated these components to build three working intelligent munitions system (IMS) prototypes, nine PIR sensor nodes, an IFF transponder, an OTAR transceiver, and a static, full system display mounted on an inert training mine.

B. Software Design

The operating system for the MICAz mote is TinyOS. TinyOS provides a primitive operating system for wireless sensor networks with limited memory and processing resources. The SUREFire software program is written in NES-C, a C-like, concurrent programming language.

SUREFire Intelligent Munitions System: This software component samples sensors and determines whether to fire the munitions depending on one of the following operational states:

- Idle: System powered with sensors and trigger off-line.
- Standby: System and sensors powered on and able to exchange GPS data to initialize neighborhood lookup table. Munitions trigger off-line.
- Sensor Fire: System armed and automatically fires upon positive sensor reading.

- Max Lethality: System armed and will follow the algorithm to draw the maximum number of enemy into the munitions field.
- System Detonate: Automatically triggers for individual activation control or post-battle destruction.
- System Inert: Automatically destroys key electronic components to render the mine unusable.
- System Shutdown: Powers down the mine.

SUREFire Over-the-Air Reprogramming (OTAR): This human operator interface samples a thumbwheel 0-9 mode corresponding to the munitions operational mode/state. It securely broadcasts this code to the deployed intelligent munitions systems.

SUREFire Identify Friend or Foe (IFF): IFF periodically transmits a secure packet from a transmitter on a soldier or vehicle. This software allows a friendly node to broadcast an AES-128 bit encrypted code to set a *Friendly Check Fire* state and temporarily transform the intelligent munitions network into a friendly forces maneuver space. Current minefields indiscriminately detonate; however, with the use of the IFF by a friendly unit, mines are set to a check-fire mode. Once the IFF transceiver is out of range, the SUREFire node times out and resumes its previous operational mode. Thus, friendly units can use known minefields as escape routes that can quickly return to a deadly weapon system against the enemy.

V. SUREFIRE TESTING

The SUREFire intelligent munitions system requires two enabling technologies to operate. First, the GPS must be able to give a 5.3 meter neighbor-relative accuracy to provide the required resolution for a minimum 15m spaced munitions field [16]. Second, the magnetic sensor must be able to determine the direction of travel of the target. This section explains the tests and results for these enabling technologies.

A. Relative GPS Test

The first absolute accuracy GPS test established the need for the SUREFire network to consider gaining additional accuracy with relative vs. absolute GPS locations. Table 3 shows an initial absolute accuracy test for one location previously benchmarked by Geographic Information Systems (GIS). Comparing the GIS value and the GPS sensor reading produced a 5.805m error. Table 4 shows a subsequent GPS relative accuracy test between that point and another point at a distance of 11m apart reduced the relative error down to 1.70m. These two tests validate that the system does not meet the required 5.3m accuracy requirement using absolute GPS measurements, but the relative GPS measurements may be able to reduce the error sufficiently.

The third GPS experiment tested the relative GPS accuracy for eight points spaced approximately 15m apart. The eight pairs had an average relative location accuracy error of 1.68m with a standard deviation of 1.54m. The largest error was 4.4m which is within the required error tolerance. Since error is cumulative with distance, the system eliminates error accumulation of multi-hop neighbors by placing a higher confidence in the relative location of immediate neighbors.

Table 3. Absolute GPS Accuracy

Coordinates	Longitude	Latitude	Error Distance
GIS	73.953958 W	41.39121 N	5.805 m
GPS Measured	73.953968 W	41.39115 N	

Table 4. Two-point Relative GPS Accuracy

Longitude	Latitude	Distance	Error
73.9539683 W	41.3911583N	10.84 m	1.70 m
73.953985 W	41.391255 N		

B. Sensor Trajectory Magnetometer Experiment

The laboratory magnetometer experiment established that the 2-axis magnetometer was able to determine the direction of travel in four cardinal directions. To conduct the indoor experiment, we first established baseline x-axis and y-axis readings. Next, a 5kg ferrous transformer was placed adjacent to the sensor in the north, south, east, and west directions to determine changes in sensor readings based upon the orientation. The results in Table 5 clearly show that an overhead trajectory can be determined by identifying the positive and negative changes in the x and y readings. For instance, a northerly trajectory would first indicate that the vehicle is approaching from the south. The sensor would read a $+\Delta x$ and a $-\Delta y$ reading when compared to the baseline. As the target departs in a northern direction, the sensor would read a $-\Delta x$ and a $+\Delta y$ reading. Each direction of travel in five separate trials clearly shows a unique transition for each of the four directions of travel. This experiment validated that SUREFire can establish the direction of travel for an overhead vehicle using a 2-axis magnetometer.

VI. FUTURE WORK AND CONCLUSION

This research makes two significant contributions to network science and intelligent munitions systems. The first contribution is the deliberate network linkage of the physical domain to social and information domain processes and cognitive domain requirements to the initial phases of a systems development life-cycle. This linkage, in turn, enables the designer to leverage available resources and

Table 5. Magnetometer Directionality Results

Target Heading	Trial 1 of 5	
	x-axis	y-axis
Base line	7.7	3.4
South	10.7	1.1
	$+\Delta x$	$-\Delta y$
East	5.4	2.2
	$-\Delta x$	$-\Delta y$
West	12.3	7.7
	$+\Delta x$	$+\Delta y$
North	5.9	5.9
	$-\Delta x$	$+\Delta y$

integrate entities that can provide extended capabilities and self-synchronized behavior in a highly effective manner. The second contribution is the application of location and trajectory knowledge in a networked munitions system to increase the global situational awareness thereby making smarter detonation decisions and increasing overall combat power. Future work for SUREFire includes integrating more sensor types to provide greater accuracy in target signature, location, speed, and trajectory. In processing the sensor data, this work includes creating social templates to establish enemy formations (small world networks) and using behavioral models to relate past actions to future options.

REFERENCES

- [1] Committee on Network Science for Future Army Applications, National Research Council, Network Science, National Academies Press, Washington DC, 2006.
- [2] D. Alberts, J. Garstka, and F. Stein, Network Centric Warfare: Developing and Leveraging Information Superiority. CCRP Publication Series, April 2005.
- [3] Clausewitz, General Carl von. On War. Translated by Colonel J.J. Graham, Wilder Publications, LLC, Radford VA, 2008.
- [4] Moxley, Frederick I. (2005). Network Science Lectures, United States Military Academy, West Point, NY.
- [5] Moxley, Frederick I. (2006). The Art of Network Science in Network Science at the U.S. Military Academy, West Point, New York: [Brochure], 500.
- [6] U.S. Army Field Manual 71-123, Tactics and Techniques for Combined Arms Heavy Forces: Armored Brigade, Battalion/Task Force, and Company/Team, September 1992.
- [7] Atkinson S. and J. Moffat, The Agile Organization: From Informal Networks to Complex Effects and Agility, The Command and Control Research Program (CCRP), July 2005.
- [8] U.S. Department of State, Landmine Policy White Paper, February 2004, http://www.fas.org/asmp/campaigns/landmines/FactSheet_LandminePolicyWhitePaper_2-27-04.htm, accessed 29 March 2009.
- [9] Daisy Chaining. <http://www.fas.org/man/dod-101/sys/land/docs/981100-schneck.htm>, accessed 26 February 2009.
- [10] M. Brownfield, "Energy-efficient Wireless Sensor Network MAC Protocol," Ph.D. Dissertation, Virginia Polytechnic Institute and State University, March 2006.
- [11] M. Brownfield, K. Mehrjoo, A. Favez, and N. Davis, "Wireless Sensor Network Energy-Adaptive MAC Protocol," IEEE Consumer Communications and Networking Conference (CCNC 2006), January 2006.
- [12] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," In Proc. Intl. Conf. on System Sciences, January 2000.
- [13] G. Pei and C. Chien, "Low power TDMA in large wireless sensor networks," In MILCOM 2001, 2001.
- [14] <http://www.xbow.com>, accessed 23 March 2009.
- [15] <http://www.leadtek.com>, accessed 23 March 2009
- [16] Belleli, Mongi, IMS Enabling Technologies, Technical Paper, Dept. of Electrical Engineering and Computer Science United States Military Academy, West Point, NY, May 2008.