I.J.Computer Network and Information Security, **2012, 3,54-61**
Published Online April 2012 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2012.03.07

Intelligent Wireless Sensor Network System to shrink Suspected Terror from Militants

SanjeevPuri, Reviewer member IACSIT-IJCEE, Elsevier,
Research Scholar, Singhania University, Jhunjhunu, India purispuri_2005@rediffmail.com

***Abstract*—**In current scenario, there are always impending threats from militants and terrorists within and out of a country. The sensor networks play a vital role in minimizing the loss of human lives in the event of usual calamity and artificial sabotage created by terrorists. The sensor networks can be successfully deployed in any difficult geographical terrains where manual round-the-clock surveillance is highly impossible. Energy aware routing is immensely helpful to sensor networks in the aspect of extending the life span of the WSNs. In this paper, an automatic suspected terror system based on wireless sensor networks is developed, which is designed for high-rise metro structure. In order to provide early extinguish of impending threats by putting any bomb, large numbers of detectors which periodically measure noise, smell, infringement, vibration, temperature concentration, unidentified stranger photo are deployed from major streets. Those scattered detectors report their monitoring information to the surveillance center via the self-organizing hierarchical intelligent wireless sensor networks (IWSN). Test results from it show that the automatic suspected terror system achieves the design requirements.

Index Terms— Sensor Networks, Suspected Terror System, Impending Threats, Scattered Detectors, IWSN, Energy aware routing

I. INTRODUCTION

A Wireless Sensor Network (WSN) is a network of wireless computing devices with spatially distributed autonomous devices to cooperatively monitor physical or environmental conditions using sensors. WSNs are used to collect data from physically challenging environments. The information of events can be detected, collected, processed and sent to control room or sink by the sensors deployed in WSNs. The tiny nodes (sensors) in WSNs are equipped with substantial processing capabilities of combining the data with adjacent nodes, compressing the data, intelligent gathering and processing of sensed data, understanding and controlling the processes inherent to the system. The applications include monitoring the disasters events or elements, detection of cross border terrorism, sensing the intrusion of enemies through land or sea, battlefield surveillance, offering logistics in urban warfare and reconnaissance.

The sensor network is the network of a large number of sensor nodes which are densely deployed either inside the field or very close to it. The sensing electronics measure ambient conditions related to the environment surrounding the sensor and transform them into an electric signal. Processing such a signal reveals some properties about objects located and/or events happening in the vicinity of the sensor [8].

Intelligent wireless sensor networks (IWSN) combine sensing, signal processing, decision capability, and wireless networking capability in a compact, low power system. We need to develop the large scale, quality control low cost WSN structure. This requires that sensor information be conveyed to the user at low bit rate with low power transceivers. Continuous sensor signal processing must be provided to enable constant monitoring of events in an environment [1].

Nowadays computing devices have become cheaper, highly mobile, widely distributed and pervasive due to recent advancements in the fieldsof cellular technology, Global Positioning System (GPS), Radio Frequency Identification (RFID), Micro Electro Mechanical System (MEMS) and Advanced Electronics.Currently, most WSN designs concentrate on improving energy-efficiency leaving network delays to low priority [3]. This makes them unsuitable for time-critical applications. Still, several envisioned WSN applications should be able to handle scenarios requiring low delays. In personal security it is essential that alarm messages are delivered reliably and quickly. Other application areas requiring low communication latencies include surveillance applications and real-time localization.

After initial operation, sensors become responsible for self-organizing an appropriate network infrastructure with multi-hop connections among them and tend to communicate to their neighbors by finding their locations

and forming the topology of the network. The onboard sensors then start collecting acoustic, seismic or magnetic information of the environment through either continuous or event driven working mode. The location and positioning information of an object or event can also be obtained through the GPS or local positioning algorithms. This information can be gathered from the network and appropriately processed to construct a global view of monitoring phenomena.

A single node may cause a number of holes and shadows which can be effectively covered with a distributed deployment. Since the sensor nodes are used in large numbers, they are able to record an event with greater redundancy. In case of failure of one sensor to capture an event, others can keeptrack of it. The deployment of nodes in large numbers also offers robustness to point failures which is considered important in mission critical tasks. For instance, even when a large number of sensors are destroyed in natural or manmade disasters, the remaining sensors may keep on monitoring the event.

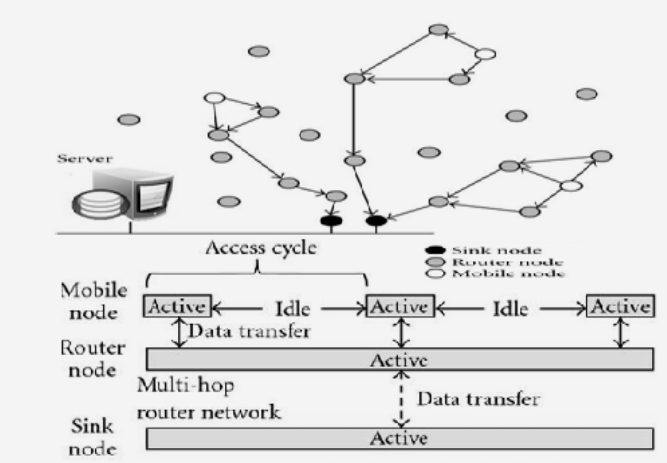

Figure1: Access Cycles of nodes in Multi-hop WSN

In this paper first I discuss the recent development of sensor networks, surveillance system and control system plane with cross layer WSN protocols are interfaced to form entire sensor system. After that I realize to propose multi-hop intelligent wireless sensor network surveillance system (IWSN) implementation in which localization level algorithm and protocol design parameters are discussed.Then I analyze the energy-aware shortest routing for IWSN and need for the alternative energy constraints with future scope to control suspected terror from militants.

II. DERIVED APPLICATIONS

WSNs can be used to make continuous monitoring for remote and inaccessible areas along border line of control where human patrolling is highly impossible. The sensors can be dropped from planes to sense the conditions of the critical area where human penetration is highly impossible. They can detect and differentiate the movement made by human beings and unidentified vehicles by continuously monitoring the vibrations in the environment. The WSN plays a crucial role in monitoring along borderline of control and reduce man power required to maintain the security.

Within a few minutes, the nodes start communicating amongst themselves, finding their positions, self organizing them, establishing a network, synchronizing clocks and lying in wait.

Some of the nodes organize themselves as active nodes while the remaining nodes slip into low power mode of sleepy state in the view of consuming less energy. When an activity is detected by any active node, it will wake up all the other nodes in the network. Thus the nodes then collaboratively track down the movements of intruders by aggregating information from various sensors to gather real-time information.

III. RECENT STUDY

Initially, the development of sensor networks has highly been driven by defense applications. Since early 1950s, a system of long-range acoustic sensors namely the Sound Surveillance System (SOSUS) had been deployed in the deep basins of the Atlantic and Pacific oceans for submarine surveillance. SOSUS has recently been replaced by the more sophisticated integrated undersea surveillance system. The network of air defense radars can be regarded as an example for networked large scale sensors. Both ground-based radar systems and airborne warning and control System planes are combined together to form a sophisticated network which provides all-weather surveillance, command, control and communications.

The Cooperative Engagement Capability (CEC) was developed in the period between 1980s and 1990s as a military sensor network in which information gathered by multiple radars was shared across the entire system to provide a consistent view of battle field. Another early example of wireless sensor device is the Air Delivered Seismic Intrusion Detector system launched by US Air Force in the Vietnam War. With the advent of digital packet radios for wireless communication networks developed by ALOHA net Project at Hawaii and DARPA's (Defense Advanced Research Projects Agency)

Packet Radio Project in 1970s, wireless communication within the same frequency band using MAC (Medium Access Control)techniques and packet-based multi hop communication became possible.

A.MAC protocols

WSN MAC protocols can be divided into three categories: random-access, scheduled contention access, and Time Division Multiple Access. The low duty-cycle random-access MAC protocols, such as B-MAC, are based on a technique called low-power listening. It includes the procedure of periodically polling the wireless channel to test for traffic. Typically, frames are transmitted with a preceding preamble that is longer than the channel poll interval. This ensures that the destination node is awake during the actual data transmission. Scheduled contention-access low duty-cycle MAC protocols, such as S-MAC and IEEE 802.15.4 Low-Rate Wireless Personal Area Network (LR-WPAN) standard used in Zigbee networks, utilize periodic active and sleep periods to achieve duty cycling. The start of the active period includes the transmission of synchronization frames to communicate own schedule information to neighboring nodes. TDMA-based low duty-cycle MAC protocols, such as SMACS [13] and TUTWSN MAC [5], exchange data only in predetermined synchronized time slots. Rest of the time is spent in sleep mode. This makes the protocols virtually collision-free and removes overhearing.

B. Low-Latency Routing Protocols

Multiple real-time routing protocols have been proposed for WSNs Furthermore, design decisions such as reactive/proactive routing and flat/hierarchical topology affect the network delays and energy-efficiency.

Geographic routing protocol SPEED [14] provides soft real-time latency guarantees proportional to path length. It maintains a desired packet delivery speed in the network by estimating one-hop delays from MAC level feedback. However, SPEED leaves reliability unattended, and the used reactive route discovery method increases latency of the data forwarding process. Multipath Multi-SPEED (MMSPEED) [15] extends SPEED by providing service differentiation and probabilistic multipath forwarding to support various reliability requirements and makes routing decisions reactively.

A location-aware design in [16] presents a heuristic solution to find energy-efficient path for delay-constrained data in WSNs. The design achieves balancing between latency and energy consumption. Real-time power-aware routing (RPAR) [17] protocol is a location-aware protocol proposed to achieve low communication delays and energy-efficiency by dynamically adjusting transmission powers and routing decisions. Applications can make tradeoffs between energy consumption, network capacity, and lower delays by specifypacked deadlines. The reactive broadcast method of RPAR appears to be challenging in larger networks due to neighbor table size and a great amount of traffic congesting replies.

In [18], Akkaya and Younis propose an energy-aware QoS routing protocol that searches for energy-efficient path which satisfies latency requirements. The delay requirements are converted into bandwidth requirements and traffic is divided into different priority queues for time-critical and delay unconstrained packets. However, the proposed method consists of too complex algorithms for resource-constrained nodes in large-scale networks [4].

A cost-based routing protocol called GRAdient Broadcast (GRAB) [19] forwards packets along an interleaved mesh. Nodes broadcast packets using a cost metric. Every packet is assigned a budget. The budget consists of the minimum path cost from source to sink and a credit, which is utilized to increase reliability by channeling data along multiple paths. Although duplicate packets are controlled by a cache of recently forwarded packets, the redundant packets degrade energy-efficiency and increase delay. Also, the packet cache size increases rapidly with network size and data transmit frequency.

The used costs minimize the multi-hop communication latency. The mobile nodes are relieved from doing routing. Thus, this does not hinder their energy-efficiency.

C. Low-Latency WSN

WSN designs for time-critical applications are relatively rare. Furthermore, their experimented performance is seldom documented very accurately.

In Simon et al. present a sniper detection and localization system for urban environments, which is further refined in [20]. The system is built on Mica product line, and the later version is extended with an external Field Programmable Gate Array (FPGA) sensor board. Routing is done with Directed Flood-Routing Framework (DFRF) [21].DFRF is a gradient-based, best-effort converge-cast protocol with data-aggregation. The directed broadcasts of DFRF provide fast message delivery, but result in high communication overhead. Thus, the design is only suit for one-shot type events and does not scale well.

IV. INTELLIGENT WIRELESS SENSOR NETWORK SYSTEM (IWSN)

Multi-hop IWSN communication, provides an immediate advance in capability for narrow bandwidth devices. However, Multi-hop Communication sensor networks permit large power reduction and the implementation of dense node distribution. IWSN enable continuous sensing, event detection, and event identification at low power. Since the event detection process must occur continuously, the sensor, data converter, data buffer, and spectrum analyzer must all operate at micro power levels. In the event that an event is detected, the spectrum analyzer output may trigger the microcontroller. The microcontroller may then issue commands for additional signal processing operations for identification of the event signal. Protocols for node operation then determine whether a remote user or neighboring WINS node should be alerted. The WINS node then supplies an attribute of the identified event.

Distributed network sensor devices must continuously monitor multiple sensor systems, process sensor signals, and adapt to changing environments and user requirements with take decisions on signals parameters measurements. IWSN user requirements are wireless devices with street-level localization, reliable low-latency alarming, long network lifetime, and ease of installation and maintenance.

A. Street-Level Localization: The alarming devices are continuously carried by the guard of street. This requires fully wireless small devices operating with small batteries. The alarms should be responded as quickly as possible by a security guard and other personnel on-site. Thus, the alarming devices should be localized within one to two streets.

B. *Consistent Low-Latency Alarming*: Alarms are triggered by a person in a threatening situation. Being critical for personal security, alarm messages should not be lost. Furthermore, to ensure fast reaction to alarms, the alarm message delay should be in the order of seconds.

C. Extended Network Lifetime: For easy maintenance, the network should have extended lifetime in the order of years. This includes all devices in the network whether they are mobile or static.

D. *Effortlessness Installation and Maintenance*: The alarm network can be installed and used in many locations. Thus, it should be possible to be installed and maintained by the personnel on-site without the need for rigorous guidance to the network operation.

The network consists of sink nodes, router nodes, and mobile nodes. The sink nodes act as data endpoints for the WSN and as gateways to other networks. The router nodes forward data via a wireless multi-hop network to one or multiple sinks. To achieve low delays, the duty cycle of the routers is configured to be high. Thus, they consume more power and should be main powered or equipped with large enough batteries. The mobile nodes have low duty cycles which can be configured according to application needs.The network consists of resource-constrained WSN nodes. The nodes communicate using a high-cost high-power 24 GHz radio that includes Received Signal Strength Indicator (RSSI) functionality.

The application layer consists of security, measurement, and actuator control applications. The routing protocol provides autonomous multi-hop data forwarding. The MAC protocol implements wireless communication between nodes. The physical layer consists of the security WSN node hardware which includes various sensors.

The hardware platform hosts multitude of sensors integrated to the circuit board or via an external connector. These sensors include temperature, luminance, air humidity, accelerometer, soil humidity, carbon dioxide, sound pressure, air flow, electrical measurements (current, voltage, resistance, and power), motion detectors (passive infrared), and magnetic switches. There is also support for on/off actuator control. We are also investigating the possibility of electrocardiogram and pulse measurements

With adaptation of local streets security WSN, personnel can send wireless alarms in threatening situations, receive acknowledgements telling that help is on its way, make various different kinds of measurements, and use actuators. The main contributions of the paper are (i) user requirement specification for the IWNS security, (ii) design and implementation meeting the presented requirements, (iii) real world pilot deployment and experiments.

To achieve these security requirements IWSN utilizes a heterogeneous architecture where variable duty cycling is used based on node responsibilities giving them different activity times. The network achieves reliable data forwarding and low delays whilst enabling the usage of fully wireless sensor nodes that can be also portable if needed. The mobile nodes are localized using a location resolver algorithm. Both the communication and localization are resilient against failed nodes and communication links.

Wireless Integrated Network Sensors now provide a new monitoring and control capability for monitoring the external and internal boundaries of the country. Using this concept we can easily identify a stranger or some terrorists entering from the border or any destination area. The destination area is divided into number of nodes. Each node is in contact with each other and with the main node. The noise produced by the foot-steps of the outsider or any suspected parameter is collected and recognized using the sensor. This sensed signal is then converted into power spectral density and the compared with reference value of our convenience.

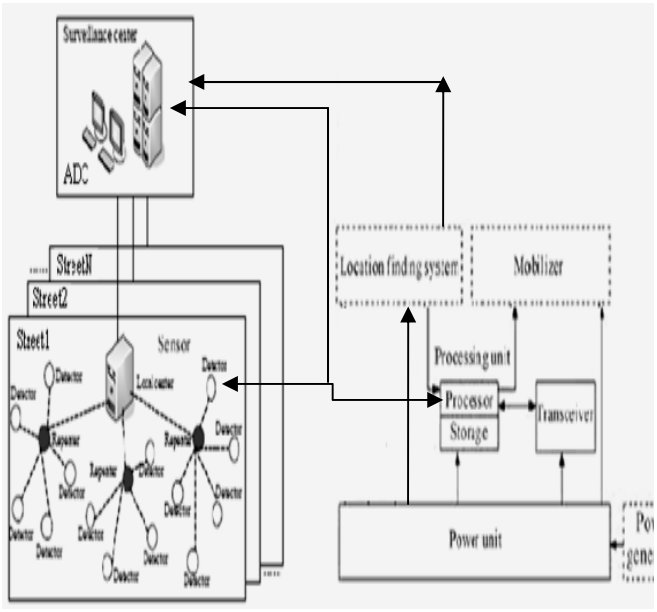

Figure2: Intelligent Wireless Sensor Network based Surveillance System

Accordingly the compared value is processed using a microprocessor, which sends appropriate signals to the main node. Thus the stranger is identified at the main node. A series of interface, signal processing, and communication systems have been implemented in micro power CMOS circuits. A micro power spectrum analyzer has been developed to enable low power operation of the entire system. On a global scale, Intelligent Wireless Sensor Network System (IWSNS) will permit monitoring of land, water, and air resources for environmental monitoring. On a national scale, transportation systems, local streets and borders will be monitored for efficiency, safety, and security.

On a metropolitan scale, new traffic, security, emergency, and disaster recovery services will be enabled by proposed system. On a local, enterprise scale, IWSNS will create a manufacturing information service for cost and quality control. The opportunities for IWSNS depend on the development of scalable, low cost, sensor network architecture. This requires that sensor information be conveyed to the user at low bit rate with low power transceivers. Distributed signal processing and decision making enables events to be identified at the remote sensor.

Self-organizing and self-healing are the remarkable characteristic of wireless sensor network. When wireless nodes startup, they can find and join the nearest network automatically. And when some node failure, they can reorganize the network as soon as possible. As shown in the
Figure2, the topological structure of our proposedIWNSsystem is Hybrid (Star + tree). The system is distributed in accordance with the deployed locations. In order to identify sensors based on their locations, addressing is required. In fact, a system involves no more than 10,000 detectors. So 2 bytes communication address is used in our system to indicate the source end and the destination end of a message. The high 8 bits represents network address, and the low 8 bits represents node address. Therefore, a network can accommodate up to 255 repeaters, each repeater can hold up to 255 detectors. Each repeater is allocated one network address by the surveillance center. And the repeater allocates node addresses for its detectors independently.

In our system, the messages are transported through wireless links up to two hops. So the networking operation is relatively simple. New node broadcasts a networking request message, declaring its serial number. Repeaters received the networking request will check whether the serial number it announced is permitted, and send back a response with the communication address allocated for the new node. To avoid confusion bring by more than one repeater responding, the detector transmits a networking confirm message to the repeater it chosen. And the repeater received the confirm message updates its neighbor table and report the topology change to the surveillance center. Other repeaters wait until waiting times up, and then cancel the address allocation operation.

V.WORKING OF PROTOCOL AND ITS DESIGN FOR IWSN

IWSN stack design consists of a MAC and a routing protocol. The MAC protocol uses random channel access to achieve low channel access delays. Thus, nodes can transmit data at any required time instant. Network beacons, used for neighbor discovery signaling among the router nodes, are transmitted on a different frequency channel. The routing protocol utilizes multiple cost-based, proactively constructed routing gradients to the sink nodes. The source routers randomize different back-off times for the initial transmissions. Thus, they both transmit their packets successfully to the destination router, who acknowledges the successful data exchanges.

The WSN server interprets the messages sent from the WSN and resolves the locations of the suspect alarming devices. It provides an interface for a third party alarm server. The interface is implemented using Simple Object Access Protocol (SOAP) [22]. The third party alarm server is responsible for forwarding the suspect detect alarms to designated UIs that can be, for example, in personal computers or cell phones. Via the SOAP interface, the alarm server can receive the alarming device ID, suspect alarm time, alarm location in textual format, and alarm location highlighted in a map image.

Location resolver algorithm shows resilience against failed nodesand communication links. First, both Anchor nodes 1 and 2 can hear the localized node. Thus, the unknown location is resolved by intersection of the two bounding boxes. Then, Anchor node 2 is lost but at least a rough location is still resolved.

The routing algorithm SPIN (Sensor Protocols for Information via Negotiation) uses concepts to eliminate redundant data transmission. It employs metadata to uniquely identify data items to prevent sending multiple copies of the same data. It also introduces energy awareness into the system which helps to increase the life of the network [5]. LEACH (Low-Energy Adaptive Clustering Hierarchy) is a cluster based protocol to evenly distribute energy load among various sensors in the network. It uses clustering to reduce the amount of global traffic and implement area level aggregation and compression. The changing the cluster heads randomly distributes the energy level gradually over the network and the probability of node failure is much more random which results in longer life for WSN.

In order to implement communications between equipments, messages format are defined carefully. All messages we defined are filled in the data field of CC1100 packet. The first bytes of all those messages are packet type field, which indicates the function of the message. Five packet type values we defined are:

Packet type Message

0x01 Networking request
0x02 Networking response
0x03 Networking confirm
0x11 Suspectedalarm reports
0x12 Parameter modify

The communication addresses are allocated in the networking communication process, and the sensor network is updated. The format of networking messages is shown in Figure3. The networking message involves 3 type messages: networking request, networking response and networking confirm. Networking request is a broadcast frame, whose source address and destination address are both set to 0xFFFF. The identification of node is 5 bytes serial number which is stored in EEPROM of each node. The serial number of each node is record before installing in the building, and the installation location of each node is pre-arranged. So the surveillance center is able to accurately locate the alarm source.

8bits8 bits 8bits 8bits 16bits16bits 8bits

Figure3: Suspected Concerned Message

Communication counter field records the successful communication times between the detector and the repeater. So that repeater can identify whether the message is a retransmitted one. Alarm type is shown in alarm status, including NORMAL, SUSPECT_ALARM, BATTERY_FAULT and DETECTOR_AGING. Suspect concentration field is the infringement concentration or temperature value measured by the detector. Battery energy field shows the voltage of the detector, so that the controller center knows the energy status of each detector. When repeater receives a suspected alarm message, it will forward the message to control center and send back a parameter modify message to confirm that it has received thesuspected alarm message. The parameter modify message is also sent by surveillance center to control detectors'status and modify their detect parameters.

VI. ENERGY-AWARE SHORTEST ROUTING

Shah et al. [21] proposed to use a set of sub-optimal paths occasionally to increase the lifetime of the network. These paths are chosen by means of a probability function, which depends on the energy consumption of each path. Network survivability is the main metric that the approach is concerned with. The approach argues that using the minimum energy path all the time will deplete the energy of nodes on that path. Instead, one of the multiple paths is used with a certain probability so that the whole network lifetime increases. The protocol assumes that each node is addressable through a class-based addressing which includes the location and types of the nodes. There are 3 phases in the protocol:

A. Setup phase: Localized flooding occurs to find the routes and create the routing tables. While doing this, the total energy cost is calculated in each node. For instance, if the request is sent from node *i N* to node *j N*,*j N* calculates the cost of the path as follows:

$$C_{Nj,Ni} = Cost\ (N_i) + Metric\ (N_j\ ,\ N_i) \quad (1)$$

Here, the energy metric used captures transmission and reception costs along with the residual energy of the nodes. Paths that have a very high cost are discarded. The node selection is done according to closeness to the destination. The node assigns a probability to each of its neighbors in routing (forwarding) table (FT)

corresponding to the formed paths. The probability is inversely proportional to the cost.

B. Data Communication Phase: Each node forwards the packet by randomly choosing a node from its forwarding table using the probabilities.

C. Route maintenance phase: Localized flooding is performed infrequently to keep all the paths alive. The mean delay time for the entire subnet is derived from weighted sum of all the lines. There are different flows to get new average delay. But we find the path, which has the smallest mean delay using program. Then we calculate the Waiting factor for each path. The path, which has low waiting factor, is the shortest path.

$$\textit{The waiting factor (W) = Mean packet flow in path}(\lambda_i) \,/\, \textit{Mean packet flow in subnet } (\lambda) \quad (2)$$

The routing protocol allows multiple sink nodes in the network. They can be either individuals or replicas. The sinks request data from the network using interests [7]. Individual sinks have unique addresses and separate interest information. Replicated sinks share the same address and interest information. Routing to the nearest sink lowers latency further by minimizing the amount of hops that a packet has to traverse. The routing protocol functionality is divided into route discovery, route calculation, and data forwarding.

The sink sequence number is used to resolve the latest sink information and reject old information. It is incremented by a sink when it disseminates new interests to the network. The route discovery process [12] is divided into sink-initiated route construction and router node-initiated route maintenance. Route construction is for sink interest diffusion and fast network build-up. Route maintenance allows adaptation to network dynamics. The route calculation uses only local information available in a router node and its neighborhood. As routes are proactively calculated, router nodes can forward data packets immediately on demand and transmit the packets forward in the hop chain.

VII. ALTERNATE ENERGY CONSTRAINTS

The various key design issues involved in WSNs are network dynamics and node deployment, transmission media and communication, data delivery models, node capabilities, power consumption, data aggregation, fault tolerance, scalability and sensor network topology. Energy consumption is a dominant factor in the design of large scale sensor networks. Since, these constraints are highly specific to sensor networks, new improved power sources, wireless ad-hoc networking and efficient routing techniques are required [6]. By providing newly improved power sources like nature based renewable (solar) energy will solve many of the aforementioned constraints.

In the higher energy density batteries and very low power embedded platforms, the amount of available energy on board still severely limits the life span of distributed battery operated WSN systems. The low-level energy constraints of the sensor nodes combined with the data delivery requirements leave a clearly defined energy budget for all other services. The goal is to achieve a self-powered system without having necessary frequent maintenance for battery replacement or recharging [6].

VIII. CONCLUSION AND FUTURE SCOPE

The user requirements consisted of wireless devices with street-level localization, reliable low-latency alarming, long network lifetime, and ease of installation and maintenance. With using IWSN system, Personnel can send wireless suspected alarms in threatening situations, receive acknowledgements telling that help is on its way, and make various environmental and physiologicalmeasurements. Thesuspected terror security IWSN framework utilizes a heterogeneous communication hybrid topology including sink, router, and mobile nodes. The router nodes have a high-duty cycle, and they form a multi-hop network for low-latency data forwarding to sink nodes. The mobile nodes have low-duty cycles and are highly energy-efficient.

Sensor Networks are emerging as a great aid in improving the way data is gathered. This development is going to have a great impact on the environmental monitoring in the area of defense. By using energy aware efficient clustering and routing concepts the battery and computation overhead will be reduced. Energy aware routing within the clusters saves the energy of the battery powered nodes due to its routing capability only through the alternative powered nodes. The alternate energy based routing concepts increase the performance and life of WSNs compared to other conventional routing algorithms. The soft computing based approximation algorithms such as Fuzzy and Genetic algorithm concepts can be used to have better convergence of clustering and routing techniques.

REFERENCES

[1] Barrenetxea, M. Vetterli, 2008. Wireless sensor networks for environmental monitoring: the sensor scope experience. IEEE International Zurich Seminar on Communications, Zurich, pp: 98-101.

[2] Nallusamy, R., K. Duraiswamy and D.A. Muthukumar, 2010. Energy efficient clustering and shortest path routing in wireless ad hoc sensor networks using (WASN) approximation algorithms. J. Math. Technol., 1: 154-160.

[3] C.S., S. Lee, P. Mitra and S. Kumara, 2009. Distributed energy balanced routing for wireless sensor networks. Comput. Ind. Eng., 57: 125-135.
[4] Al-Karaki, J.N. and G.A. Al-Mashaqbeh, 2007. Energy-centric routing in wireless sensor Networks Microprocessors Microsyst., 31: 252-262.
[5] Lattanzi, E., E. Regini, A. Acquaviva and A. Bogliolo, 2007. Energetic sustainability of routing algorithms for energy-harvesting wireless sensor networks. Computing Comm.,30: 2976-2986.
[6] Minami, M., T. Morito, H. Morikawa, A battery-less wireless sensor network system for environmental monitoring applications 2nd International Workshop on Networked Sensing Systems, June 2005
[7] Yang, Y., R.S. Blum and B.M. Sadler, 2009. Energy-efficient routing for signal detection in wireless sensor networks. IEEE Trans. Signal Process, 57: 2050-2063.
[8] F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Communications Magazine, vol. 40, no. 8, pp. 102–114, 2002.
[9] J. Suhonen, M. Kohvakka, M. Hännikäinen, and Hämäläinen, "Design, implementation, and experiments on outdoor deployment of wireless sensor network for environmental monitoring," *6th International Workshop on Architectures, Modeling, and Simulation (SAMOS '06)*, vol. 4017 of *Lecture Notes in Computer Science*, pp. 109–121, Samos, Greece, July 2006.
[10] M. Kuorilehto, J. Suhonen, M. Hännikäinen, and Hämäläinen, "Tool-aided design and implementation of indoor surveillance wireless sensor network," in *7th International Workshop on Embedded Computer Systems: Architectures, Modeling, and Simulation (SAMOS '07)*, vol. 4599 of *Lecture Notes in Computer Science*, pp. 396–407, Samos, Greece, July 2007.
[11] V. A. Kaseva, M. Kohvakka, M. Kuorilehto, M. Hännikäinen, and T. D. Hämäläinen, "A wireless sensor network for RF-based indoor localization," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, Article ID 731835, 2008.
[12] M. Kohvakka, J. Suhonen, M. Kuorilehto, V. Kaseva, M. Hännikäinen, and T. D. Hämäläinen, Energy-efficient neighbor discovery protocol for mobile wireless sensor networks," *Ad Hoc Networks*, vol. 7, no. 1, pp. 24–41, 2009.
[13] K. Sohrabi, J. Gao, V. Ailawadhi, and G. J. Pottie, "Protocols for self-organization of a wireless sensor network," *IEEE Personal Communications*, vol. 7, no. 5, pp. 16–27, 2000.
[14] T. He, J. A. Stankovic, C. Lu, and T. Abdelzaher, "SPEED: a stateless protocol for real-time communication in sensor networks," in *Proceedings of the 23th IEEE International Conference on Distributed Computing Systems*, pp. 46–55, May 2003.
[15] E. Felemban, C.-G. Lee, and E. Ekici, "MMSPEED: multipath Multi-SPEED protocol for QoSguaranteeof reliability and timeliness in wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 5, no. 6, pp. 738–754, 2006.
[16] P. K. Pothuri, V. Sarangan, and J. P. Thomas, "Delay-constrained, energy-efficient routing in wireless sensor networks through topology control," in *Proceedings of IEEE International Conference on Networking, Sensing and Control (ICNSC '06)*, pp. 35–41, April 2006.
[17] O. Chipara, Z. He, and Z. He, "Real-time power-aware routing in sensor networks," in *Proceedings of the 14th IEEE International Workshop on Quality of Service (IWQoS '06)*
[18] F. Ye, G. Zhong, S. Lu, and L. Zhang, "GRAdient broadcast: a robust data delivery protocol for large scale sensor networks," *Wireless Networks*, vol. 11, no. 3, pp. 285–298, 2005.
[19] P. Volgyesi, G. Balogh, A. Nadas, C. B. Nash, and A. Ledeczi, "Shooter localization and weapon classification with soldier-wearable networked sensors," in *Proceedings of the 5th International Conference on Mobile Systems, Applications and Services (MobiSys '07)*, pp. 113–126, 2007.
[20] L. G. Roberts, "Aloha packet system with and without slots and capture," *ACM SIGCOMM—Computer Communication Review*, vol. 5, no. 2, pp. 28–42, 1975.
[21] J. Syrjarinne, *Studies of modern techniques for personal positioning*, Ph.D. dissertation, Tampere University of Technology, Tampere, Finland, March 2001.
[22] "SOAP Version 1.2 W3C Recommendation," 2007, http://www.w3.org/TR/soap12-part1

Prof. SanjeevPuriis the research scholar and pursued PhD (CS) fromSinghania University, Jhunjhunu. He is the Reviewer editorial member of IACSIT-IJCEE and Elsevier. He has received MPhil(Computer Sc.) from VMU, Salem in 2006. He has done Master of Science in Computer Science in 2003.He is working as Professor (Information Technology) at SRMCEM (Now SRM University), Lucknow, India. His research interests include techniques and related to wireless sensor networks security, grid security and protocols working deeds in communication of network system.