AUTONOMIC WIRELESS SENSOR NETWORK PROTOCOLS

C. Hari Kishan[1], Dr. P. BalaKrishna Prasad[2]
1. Scholar in Computer Science and Engineering Department, Acharya Nagarjuna University
2.Principal, Eluru College of Engineering & Technology ,Eluru

Abstract: *Wireless ad hoc networks of sensor nodes are envisioned to be deployed in the physical environment to monitor a wide variety of real-world phenomena. Wireless sensor networks (WSN's) are becoming popular in military and civilian applications such as surveillance, monitoring, disaster recovery, home automation and many others. Almost any sensor network application requires some form of self-configuration and autonomic functionality. Following IBM's initiatives towards Autonomic computing many architectures and protocols for network self-organization and management have been proposed and being implemented.*

The paper presents concept of Autonomic Computing with respect to Wireless Sensor Network. The paper introduces Wireless sensor network basics, design goals and challenges along with current and future applications. It articulates basic needs of incorporating autonomic computing principles into the design of Wireless Sensor Networks. The paper also outlines recent contributions to Autonomic network architectures, research projects, proposed architectures and routing protocols for Autonomic Wireless Sensor Networks.

1. INTRODUCTION

Wireless sensor networks have critical applications in the scientific, medical, commercial, and military domains. Examples of these applications include environmental monitoring, smart homes and offices, surveillance, and intelligent transportation systems. It also has significant usages in biomedical field. As social reliance on wireless sensor network technology increases, we can expect the size and complexity of individual networks as well as the number of networks to increase dramatically.

Wireless sensor networks are typically used in highly dynamic, and hostile environments with no human existence (unlike conventional data networks), and therefore, they must be tolerant to the failure and loss of connectivity of individual nodes. The sensor nodes should be intelligent to recover from failures with minimum human involvement. Networks should support process of autonomous formation of connectivity, addressing, and routing structures. Recent researches on Autonomic Networking can serve as basis for design of *Autonomic Wireless Sensor Networks*.

The paper introduces Autonomic computing and wireless sensor network concepts. Discusses how the fundamental properties of Autonomic computing comply with the basic design requirements for wireless sensor networks. Proposed protocols for Wireless Sensor Network and their applicability and suitability to Autonomic Wireless Sensor

Networks and required improvements. The paper gives brief overview of research projects and architectures for autonomic communication and networking which can be applied to WSNs. The last section focuses on the current and possible future applications of Autonomic Wireless Sensor Networks.

**** C. Hari Kishan***
Scholar in Computer Science and Engineering Department, Acharya Nagarjuna University

2 Autonomic Computing

2.1 Background

The dramatic increase in computing devices, increased computing capacity and complexity combined with popularity of internet resulted in phenomenal growth in heterogeneous networks and network applications. With this increasing system complexity, network management issues and communication protocols are reaching a level beyond human ability to manage and secure so the stability of current infrastructure, systems, and data is at an increasingly greater risk to suffer outages and general disrepair. Future network algorithms need to be adaptive, robust, and scalable with fully distributed and self-organizing architectures. Automation, self-protection and self management of wide spread networks may solve the problem till some extent.

As the concept of self management rooted up, the most direct inspiration one can think of was the *autonomic function of the human central nervous system,* where autonomic controls use motor neurons to send indirect messages to organs at a sub-conscious level. These messages regulate temperature, breathing, and heart rate without conscious thought. Observation and analysis of these complex adaptive systems found in nature became a major source of inspiration to design algorithms for self-managed, self-organized, self-configuring and self-protecting systems.

Taking inspiration from autonomic nervous system of the human body IBM created a foundation for autonomic systems by taking initiatives towards Autonomic Computing for relieving humans from the burden of managing computer systems which is growing enormously till the extent of unmanageability. [01]

2.2 Autonomic System

Autonomic System is a system which works independently on predefined policies and rules without any human interaction, manage and configure itself on its own based on predefined rules and gained knowledgs over the time. IBM has defined the following four functional areas for self management of Autonomic System: (Ref [03]) Self-Configuration: Automatic configuration of components.

Self-Healing:Automatic discovery, and correction of faults.
Self-Optimization: Automatic monitoring and control of resources to ensure the optimal functioning with respect to the defined requirements.
Self-Protection: Proactive identification and protection from arbitrary attacks.

2.3 IBM Autonomic Computing architecture

IBM Autonomic Computing Architecture [02] defines an abstract information framework for self-managing IT systems. In the information framework, an autonomic system is a collection of autonomic elements. Each autonomic element consists of an autonomic manager (AM) and the managed resource (MR). The communication between the AM and the MR is done through the MR's management interfaces, which exposes two types of hooks, sensors and effectors. The sensors are used by the AM to obtain the internal state of the MR, and the effectors are used by the AM to change the behavior of the MR. The AM enables self-management of the resource using a "monitoring, analysis, planning, and execution" control loop, with supporting knowledge of the computing environment, management policies, and some other related considerations.

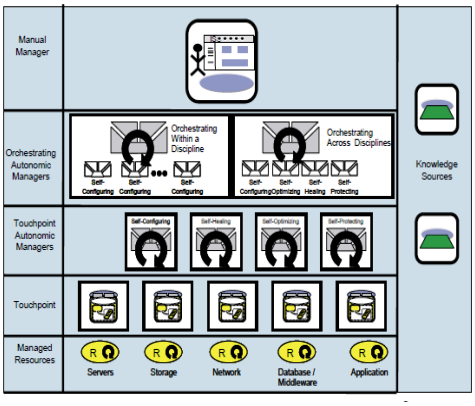

Figure 1. Basic Autonomic Computing Reference Architecture

The autonomic computing information model only provides the conceptual guidance on designing self-managed systems; in practice, the information model needs to be mapped to an implementable management and control architecture for Autonomic Networks. Specifically, measurement techniques, rule engines, planning methodologies, dynamic resource allocation techniques, security and management schemes need to be developed for autonomic elements, and a scalable management platform is required to coordinate the autonomic elements into a self-managing system.

3 Wireless Sensor Network

A wireless sensor network (WSN) is a network that is made of hundreds or thousands of sensor nodes which are densely deployed in an unattended environment with the capabilities of sensing, wireless communications and computations (i.e. collecting and disseminating environmental data). These spatially distributed autonomous devices cooperatively monitor physical and environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. The basic archetecture of Wireless sensor Network is shown in Figure2.

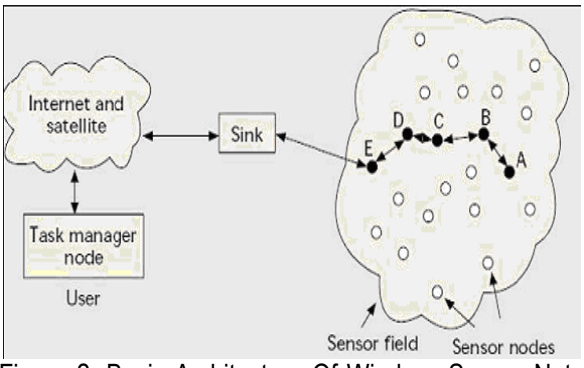

Figure 2. Basic Architecture Of Wireless Sensor Network. (Ref [04])

Each autonomic node in a sensor network is typically equipped with a radio transceiver or other wireless communications device, a processing unit which can be a small micro-controller, sensing unit, and an energy source, usually an alkaline battery. Sometimes, a mobilizer is needed to move sensor node from current position and carry out the assigned tasks. Since the sensor may be mobile, the base station may require accurate location of the node which is done by location finding system. The size of a single sensor node can vary from shoebox-sized nodes down to devices the size of grain of dust. [04]

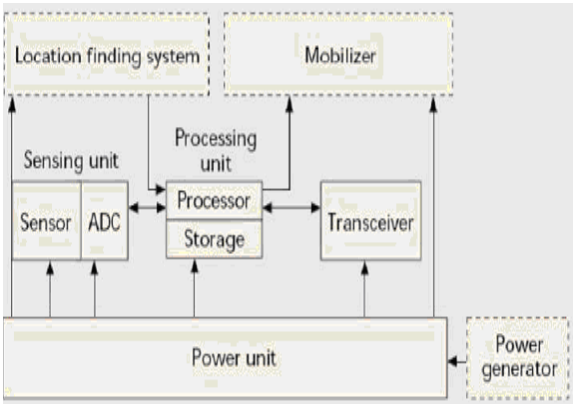

Fig 3. Components of a Sensor Node (Ref [04])

3.1 Requirements and Design factors in Wireless Sensor Network

Following are some of the basic requirements and design factors of wireless sensor network which serve as guidelines for development of protocols and algorithms for WSN communication architecture.

1. Fault Tolerance, Adaptability and Reliability: Sensor networks are required to operate through adapting to the environmental changes that sensors monitor. The networks should be *self-learning.* Reliability is the ability to maintain the sensor network functionalities without any interruption due to sensor node failure. Sensor node may fail due to lack of energy, physical damage, communications problem, inactivity, or environmental interference. The network should be able to detect failure of a node and *organize* itself, *reconfigure* and *recover* from node failures without loosing any information. [05]

2. Power Consumption and Power management: One of the components of sensor nodes is the power source which can be a battery. The wireless sensor node being a microelectronic device, can only be equipped with a limited power source [04]. Over the remote inaccessible place with less human control and existence, power sources play critical role in survival of sensor nodes. Power source should be intelligently divided over sensing, computation, and communications phases as per requirement. Sensors can be hibernated when inactive. Lots of current researches are focusing on designing power-aware protocols and algorithms for wireless sensor networks. Recently, solar energy is also considered as an option for empowering remote sensor nodes which are exposed environment.

3. Network Efficiency and Data Aggregation: Flooding raw sensed data over the network can easily congest the network. Some critical applications like *intruder detectors* require urgent transmission and faster processing of data which may degrade performance and loose reliability due to congestion or latency in the network. Intelligent aggregation of sensed data and elimination of unwanted and redundant information and data compression can be a solution for efficient resource and energy utilization and congestion avoidance. Many algorithms like directed diffusion [06] are proposed to facilitate data aggregation and dissemination within the context of WSNs.

4. Intelligent Routing: In many applications, sensor nodes are moving nodes and can change place dynamically. Routing protocols must be adaptive to these changes and should be *self-healing* and *self-configuring*. The information should be persistent in spite of changes in network nodes. Low processing capacity of a node creates many challenges for routing packets throughout the

neighbouring nodes intelligently. As discussed above, some applications may require a faster communication and instant response. Routing algorithms should be intelligent to choose minimum hop and minimum distance paths for data transfer. [07]

5. Management challenge – Managing the communication over heterogeneous networks is basic challenge in self-managed system because policies and communication protocols plan an important role in network communication. Also, it is necessary to balance the level of detail the network is providing to the client against the rate at which energy is being consumed while gathering the data. Clearly, it is preferable to have the network automatically do this tuning, rather than requiring manual intervention.

These basic requirements and design goals serve as challenge for current technology. Though current IP routing protocol exist and have significant applications in current networks and Internet, they do not satisfy complete design requirements in Wireless sensor networks because WSN nodes typically has limited computing capacities and less power. So WSN's require a different infrastructure and protocol stack which can be implemented using autonomic computing concept as we will discuss in next section.

4. Wireless Sensor Networks and Autonomic Computing -

To clarify the contribution that autonomic computing can bring to Wireless Sensor Networks (WSN), let's examine how WSN design requirements and operations can be tackled using autonomic principles.

As discussed above, there can be sensor nodes which are moving and can change their position dynamically or even leave the network coverage area. Therefore, a pre-programmed configuration for the network will not work. **Self-configuring** nodes can set up network connections, evaluate if there are any gaps in the WSN and replace a moved or dead node in the network. Since sensors can be deployed in an unattended area (e.g., forest and ocean) or physically unreachable area (e.g., inside a building wall), they are required to operate with the minimum aid from base stations or human administrators. Although majority of current sensor application have already considered this in their network design, there is still a need for WSN to have the ability to reconfigure and recover itself without too much human intervene, especially in inaccessible environment. [04, 05]

Sensor reading usually contains some noises; it may be a false positive due to malfunction of sensors. Sensors are required to collectively **self-heal** (i.e., detect and eliminate) false positives in their sensor readings instead of transmitting them to base stations. This can also reduce power consumption of sensors because data processing within the sensor incurs much less power consumption than data transmission does [10].

Sensor nodes are generally exposed to much harsher conditions than standard computing equipment, and are thus subject to energy depletion and incidental damage. Battery failure can result in lost sensor node. This leads to a gradual degradation of the network as individual nodes are lost. Network paths break and gaps appear in the coverage area. A WSN needs to adapt to the changes, recover from losses and be **self-protected**. This can be achieved by renegotiating network routes, monitoring voltage levels within sensor node, controlling each node by an agent or base station and upon failure activating redundant nodes to replace damaged ones, or by informing some higher-level entity which can provide assistance.

As discussed in requirements, maximum efficiency needs to be gained from the available energy as the available energy at each sensor node is limited. Sensing, Processing and data transfer phases require lot of energy so each node should be able to sense process and transfer data intelligently hence **self-optimization** is an important trait for WSN protocols. Energy savings can be achieved by putting the nodes into a low power sleep mode, ready to be reactivated when the need arises. For example, sensors may decrease their duty cycles when there is no significant change in their sensor readings. This results in less power consumption in the sensors. Also, when neighboring sensors report environmental changes, a sensor may draw inference from the reports and increase its duty cycle to be more watchful for a potential local environmental change in the future. However, there exists a trade-off in that the computational cost of a globally-

optimal solution such as this is often computationally intractable, whether by 8-bit nodes or 64-bit base-stations.

All basic WSN self-management principles comply with the concept of autonomic computing. So IBM autonomic computing principles can be applied to wireless sensor networks to get the desired functionality in vastly growing sensor network applications.

5. Autonomic Wireless Sensor Network Management Architectures -

As discussed in section 2.3, the basic Autonomic Computing model only provides the conceptual guidance on designing self-managed systems and needs to be mapped to an implementable management and control architecture for Autonomic Networks. An architecture for Autonomic communication and networking is an area of research lately and many architectures are proposed and being developed. All these architectures aim to produce an architectural design that enables flexible, dynamic and fully autonomic formation of large-scale networks in which the functionalities of each constituent network node are also composed in an autonomic fashion. Moreover, these architectures also support mobile nodes and multiple administrative domains so these can be applied to wireless sensor networks for achieving desired goals and meet above mention challenges.

Following is the brief discussion of some visions for the design of an efficient management architecture for WSNs based on top of the basic autonomic computing architecture.

5.1. Service-Oriented Architecture

Service-oriented architecture (SOA Ref [21]) is an approach to build distributed systems that deliver application functionality as services to end-user applications or to build other services. It decomposes the design of large complex application, and middleware architecture into various reusable services or function units. In SOA the service requester has no knowledge of the technical details of the provider's implementation, such as the programming language, deployment platform, and so forth. The service requester typically invokes operations by way of messages -- a request message and the response -- rather than through the use of APIs or file formats. Thus, the application developers only need to concern the operational description of the service which allows software on each side of the conversation to change without impacting the other.

So far, the implementation and design of SOA is mostly dependent on Web Services with standardized web technologies such as WSDL, OGSA. As a result, it is not directly applicable to all of those complex technologies on those resource-constrained sensor nodes. MANNA [19] has presented some initial ideas of using the concept of service semantics from SOA.

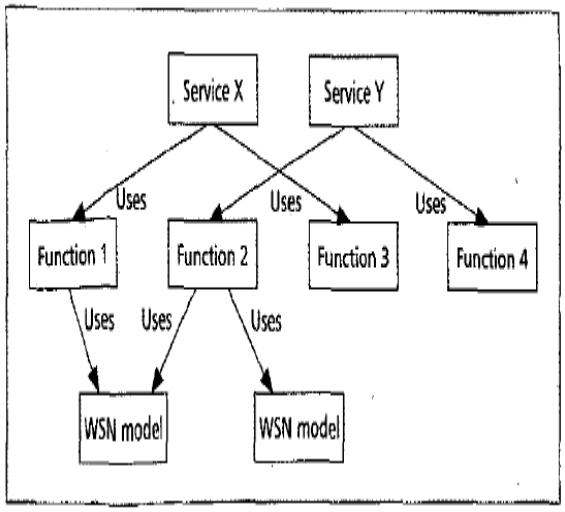

Figure 4. Basic Model of MANNA Architecture (Ref [19])

In MANNA, all the management function units sit at the lowest level of management architecture. They are designed with specific implementation for individual objectives in consideration of unique features of WSN. A service, at the top layer, can use one or more of those management functions. Different services can share the same functions, but still concern each individual given aspect based on the polices and network state obtained from WSN models. The basic model of MANNA architecture is as shown in figure 4 (Ref [19])

Furthermore, SOA can specially deal with WSN unique aspects such heterogeneity, mobility and adaptation, and offers seamless management integration in the wireless environments. Although the special features of SOA are marvellous, there is still a large amount of research

challenge needed to address before the concepts of SOA can be appropriately applied into WSNs.

5.2. Policy Based Architecture

Policy-based management has presented its robust ability to support designing of self-adaptive decentralized management service in WSNs. Davy S. et al. [20] proposed an autonomic communications architecture that manages complexity through policy-based management by incorporating a shared information model integrated with knowledge-based reasoning mechanisms to provide self-governing behavior.

The architecture is organized using four distinct architectural constructs i.e. *Shared Information, Virtual Software, Infrastructure and Policy* as shown in fig 5.

The shared information over the network is managed through a virtual software which support autonomic functionality for different heterogeneous networks and components combined with network infrastructure which include network elements and other computing devices. All these three modules are governed by policy module. [20]

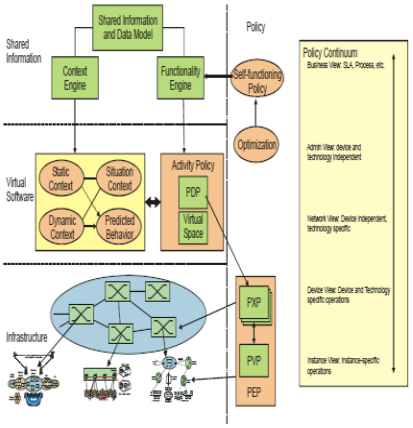

Figure 5. Proposed Policy Based Autonomic Architecture (Ref [20])

This model is based on three important concepts of autonomic computing: (1) the sharing and reusing of common information and knowledge, (2) the application of machine learning and knowledge-based reasoning to guide the changes in behavior of the system, and (3) an extensible and flexible governance model that forms a closed control loop that learns from its decisions.

Similarly, in MANNA [19], policies describe a set of desired behaviours of management components (e.g. manager and agent) for indicating the real-time operations. Based on polices, managers and agents can interact with each other in a cooperative fashion to achieve a desired overall management goal such as form groups of nodes, control network density, and keep the coverage of the WSN area.

6 Routing Protocols for Autonomic Wireless Sensor Networks

Now let's analyze few well-known routing protocols for wireless sensor networks and their suitability, pros and cons for Autonomic WSN's.

6.1 Flooding

Flooding [24] is an old routing mechanism used in wireless networks that may also be used in Autonomic wireless sensor networks. In flooding, a node sends out the received data or the management packets to its neighbors by broadcasting or flooding, unless a maximum number of hops for that packet are reached or the destination of the packets is arrived. This method guarantees the delivery of the packet to the destination. However; there are some deficiencies and disadvantages of flooding technique [24]:

- Implosion of Data packets: Flooding may cause the Implosion effect for data packets and also for ACK packets if used any. One packet takes multiple routes and multiple hosts can deliver the same packet to destination. Destination has to implement a separate mechanism for duplicate suppression also lot of bandwidth and resources are wasted in transmitting same packet through multiple hosts so this technique may not be suitable for large Wireless sensor networks.

- Overlap: if two sensor nodes cover an overlapping measuring region, both of them will sense/detect the same data. As a result, their neighbor nodes will receive duplicated data or messages. Overlapping is a function o both the network topology and the mapping of sensed data to sensor nodes.

- Resource utilization: In flooding, nodes do not take into account the amount of energy resource available to them

at a given time. An Autonomic WSN protocol must be energy resource-aware and adapts its sensing, communication and computation to the state of its energy.

6.2 Gossipi

Gossiping protocol is an alternative to flooding mechanism. In Gossiping [25], nodes forward incoming packets to a randomly selected neighbor node. Once a gossiping node receives the messages, it forwards the data back to that neighbor or to another one randomly selected neighbor node and in this way route from source to destination is created. This technique assists in energy conservation by randomization.

Although, gossiping can solve the implosion problem, it can not avoid the overlapping problem. On the other hand; gossiping distribute information slowly, this means it consumes energy at a slow rate, but the cost is long-time propagation is needed to send messages to all sensor nodes so it may not be the best suitable technique for Autonomic Wireless Sensor networks.

6.3 SPIN

Kulik et al. proposed a family of adaptive protocols for WSNs, called SPIN (Sensor Protocols for Information via Negotiation) [26]. Their design goal is to avoid the drawbacks of flooding protocols by utilizing data negotiation and resource-adaptive algorithms. Nodes running a SPIN communication protocol name their data using high-level data descriptors, called meta-data. They use meta-data negotiations to eliminate the transmission of redundant data throughout the network. In addition, SPIN nodes can base their communication decisions both upon application-specific knowledge of the data and upon knowledge of the resources that are available to them. This efficient distribution of data by sensors with limited energy supply complies with the Autonomic Sensor network requirements and can be very effective under small networks.

SPIN is designed based on two basic ideas; (1) to operate efficiently and to conserve energy by sending metadata (i.e., sending data about sensor data instead of sending the whole data that sensor nodes already have or need to obtain), and (2) nodes in a network must be aware of changes in their own energy resources and adapt to these changes to extend the operating lifetime of the system. SPIN has three types of messages, namely, ADV, REQ, and DATA.

- ADV: when a node has data to send, it advertises via broadcasting this message containing meta-data (i.e., descriptor) to all nodes in the network.

- REQ: an interested node sends this message when it wishes to receive some data.

- DATA: Data message contains the actual sensor data along with meta-data header.

SPIN is a data-centric routing protocol where the sensor nodes send ADV message via broadcasting for the data they have and wait for REQ messages from interested sinks or nodes. SPIN has some advantages in solving the problems associated with classic flooding protocols, and adaptive to topological changes, it has its own drawbacks like; (1) SPIN is not scalable, (2) if the sink is interested in too many events, this could make the sensor nodes around it deplete their energy, and (3) SPIN's data advertisement technique can not guarantee the delivery of data if the interested nodes are far away from the source node and the nodes in between are not interested in that data.

6.4 Directed Diffusion

Directed diffusion [27] is most effective data dissemination and aggregation protocol. It is a data-centric and application aware routing protocol for Wireless Sensor Networks. It aims at naming all data generated by sensor nodes by attribute-value pairs. Directed diffusion consists of several elements; first of all, naming; where task descriptors, sent out by the sink or Data receiver, are named by assigning attribute-value pairs. Secondly, interests and gradients; the named task description constitutes an interest that contains timestamp field and several gradient fields.

Each leaf node and intermediate nodes store the interest in their interest cache. As the interests propagate throughout the network, the gradients from the source back to the sink

are set up. Thirdly, data propagation, when the source has data for the interest, it sends out the data to the interest (i.e., sink) along the interest's gradient path which can be chosen as the shortest hop path or shortest time path derived from the request packet. Fourthly, after the interest (sink) starts receiving low rate data events, it reinforce one particular neighbor to draw down higher

quality (higher data rate) events. This feature of directed diffusion is achieved by data-driven local rules. Directed diffusion assists in saving sensors' energy by selecting good paths by caching and processing data in-network since each node has the ability for performing data aggregation and caching. On the other hand; Directed diffusion has its limitations such as; implementing data aggregation requires deployment of synchronization techniques which is not realizable in WSNs. Also, the overhead in data aggregation involves recording information.

These two drawbacks may contribute to the cost of sensor node hence cost is the tradeoff for performance in Directed diffusion technique, which may be acceptable for some autonomic wireless sensor networks.

6.5 LEACH

LEACH (Low Energy Adaptive Clustering Hierarchy) [28] is a self-organizing, adaptive clustering-based protocol that uses randomized rotation of cluster-heads to evenly distribute the energy load among the sensor nodes in the network. LEACH based on two basic assumptions: (a) base station is fixed and located far away from the sensors, and (b) all nodes in the network are homogeneous and energy-constrained. The idea behind LEACH is to form clusters of the sensor nodes depending on the received signal strength and use local cluster heads as routers to route data to the base station. The key features of LEACH are:

- Localized coordination and control for cluster set-up and operation.

- Randomized rotation of the cluster "base stations" or "cluster heads" and the corresponding clusters.

- Local compression to reduce global communication.

In LEACH, the operation is separated into fixed-length rounds, where each round starts with a setup phase followed by a steady-state phase. The duration of a round is determined priori.

Although, LEACH has shown good features to sensor networks, it suffers from the following drawbacks:

- It can not be applied to time-constrained application as it results in a long latency.

- The nodes on the route a hot spot to the sink could drain their power fast. This problem is known as "hot spot" problem.

- The number of clusters may not be fixed every round.

- It can not be applied to large sensor networks.

Therefore, for Autonomic wireless sensor networks with stable and fixed homogeneous nodes the LEACH protocol will give good performance. For a Autonomic Sensor Network with stationary, battery powered nodes it would be effective to use clustered based protocol like LEACH, the most obvious reason is, its advantages such as reduced control messages, bandwidth reusability, enhanced resource allocation, improved power control and lest wastage of energy.

6.6 PEGASIS

PEGASIS (Power-Efficient GAthering in Sensor Information Systems) is a greedy chain-based power efficient algorithm [29]. PEGASIS is based on two ideas i.e. Chaining, and Data Fusion. It uses same technique as LEACH (the scenario and the radio model in PEGASIS are the same as in LEACH).

In PEGASIS, each node can take turn of being a leader of the chain, where the chain can be constructed using greedy algorithms that are deployed by the sensor nodes. PEGASIS assumes that sensor nodes have a global knowledge of the network, nodes are stationary (no movement of sensor nodes), and nodes have location information about all other nodes. PEGASIS performs data

fusion except the end nodes in the chain. PEGASIS outperforms LEACH by eliminating the overhead of dynamic cluster formation, minimizing the sum of distances that non leader-nodes must transmit, limiting the number of transmissions and receives

among all nodes, and using only one transmission to the Base Station per round.

As it is similar as LEACH protocol, PEGASIS also suffers from same problems as LEACH.

Additionally, PEGASIS does not scale, so can not be applied to sensor network where global knowledge of the network is not easy to get.

6.7 GEAR

GEAR (Geographical and Energy Aware Routing) [30] is a recursive data dissemination protocol for WSNs. It uses energy aware and geographically informed neighbor selection heuristics to route a packet to the targeted region. Within that region, it uses a recursive a geographic informed mechanism to disseminate the packet. GEAR, like other sensor networks protocols, developed according to some assumptions in mind:

- Sensor nodes are static (i.e., immobile).
- There is an existence of a localization system that enables each node to know its current position.
- Sensor nodes are energy-constrained accompanied with location information about all other nodes (i.e., each node knows its location and its energy level, and its neighbor's location and remaining energy level.
- The link that connects nodes is bi-directional.

GEAR has two phases: (1) forwarding the packets toward the targeted region, and (2) forwarding the packets within the targeted region R.
Although GEAR reduces the energy consumption for the route set up. It is not scalable and does not support data diffusion.

Based on the analysis, compatibility survey of the existing protocols for Wireless Sensor Networks, we can conclude that some of the protocols can more or less be applied for routing in Autonomic Wireless Sensor Networks with few modifications depending upon the network structure and functionality. Overall, there are some key features, an efficient routing protocol for Autonomic Wireless Sensor Networks should have are: [31]

- Data Aggregation: Reducing the data size quickly using computation will play a key role in supporting efficient query processing, and reducing the overall network overhead. Hence saving the power.

- Dynamic clustering: Dynamic clustering architecture is very important because such architecture will preclude cluster heads from depleting their energy quickly. Hence, long network's lifetime.

- Threshold for sensor nodes on data transmission and dissemination: this will help in saving energy by reducing unnecessary transmissions (i.e., redundancy) and giving the network long lifetime.

- Randomized path selection: multi-path selection to destination could improve fault tolerance and handle the overhead of network load.

- Mobility: most of the current protocols assume that sensor nodes are static (i.e., immobile). However, for some applications, nodes need to be mobile. Hence, new routing algorithms are needed to handle the mobility and network topology changes.

- Self-configuration: since sensor nodes are prone to failure due to some factors or new sensor nodes may join the network, an update, self-configuration, self-healing, and adaptation to changes in network topology or environmental changes should be considered.

- Security: there is a desperate need to develop distributed security approaches for wireless sensor network. Hence, achieving secure routing.

- Quality-of-Service, dependability, and localization need to be considered and given more attention.

- Time synchronization.

7. Brief Overview of research projects on Autonomic Networks–

Here is a brief overview of the current research projects based on Architecture for Autonomic Network communication and Self-Management which will serve as guidelines for Autonomic WSN's and will bring revolution to WSN's and its applications.

7.1. Bison

BISON was a three-year project funded by the European Commission. BISON aimed confronting the complexity

explosion problem by building robust Network Information Systems that are self-organizing and self-repairing.

BISON developed techniques and tools for building robust, self-organizing and adaptive Network Information System as ensembles of autonomous agents by drawing inspiration from biological processes and mechanisms like ant colonies for routing in overlay networks using swarm intelligence, lifecycle of Dictyostelium for load balancing, epidemics for aggregation and immune system for search.

BISON explored the use of ideas derived from complex adaptive systems (CAS) to enable the construction of robust and self-organizing information systems for deployment in highly dynamic network environments. The project proposed solutions to important problems arising in overlay networks and mobile ad-hoc networks by developing algorithms for routing in mobile ad-hoc networks, topology control in sensor networks along with data aggregation and content search algorithms for peer to peer networks. [11]

7.2. ANA (Autonomic Network Architecture)

ANA framework is built on the objective to provide an architectural framework that allows the accommodation of and communication between various networks, ranging from small scale Personal Area Networks, through (Mobile) Ad hoc Networks and special purpose networks such as Sensor Networks, to global scale networks, in particular the Internet. ANA framework specifies how networks interact.

ANA introduces the core concept of "network compartments." The compartment abstraction allows atomization or decomposition of communication systems and networks into smaller and more easily manageable units. For example, compartments will allow decomposition of today's global IP network into appropriate sub-networks, which can be managed more autonomously from the overall network (e.g., a different addressing or routing scheme can be applied inside each compartment). [14]

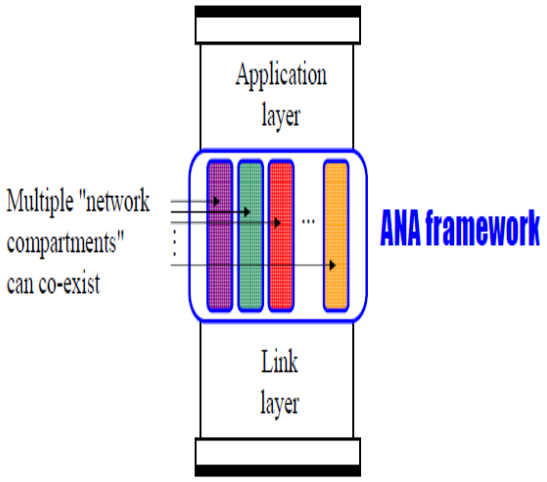

Figure 6. ANA Framework and Network compartments (Ref [14])

A (network) compartment implements the operational rules and administrative policies for a given communication context. Compartments typically perform functions like registration and degradation, policy enforcement, identifier management and resolution and Routing. [14]

Addressing and naming are left to compartments. The main advantages of this approach are:

No need to impose a unique way to resolve names and manage a unique global addressing scheme. It is open to future addressing and naming schemes.

7.3. Haggle

Haggle is a new autonomic networking architecture designed to enable communication in the presence of intermittent network connectivity, which exploits autonomic opportunistic communications (i.e., in the absence of end-to-end communication infrastructures). Haggle node architecture takes inspiration from human communication model. [15]

The main components of Haggle are:

- A **revolutionary paradigm for autonomic communication**, based on advanced local forwarding and sensitive to realistic human mobility
- A **simple and powerful architecture** oriented to opportunistic message relaying, and based on

privacy, authentication, trust and advanced data handling
- An open environment for the easy proliferation of applications and services.

7.4. CASCADAS

CASCADAS (Component-ware for Autonomic Situation-aware Communications, and Dynamically Adaptable Services) is an ongoing project like ANA and Haggle.

The overall goal of CASCADAS is identifying, developing, and evaluating architectures and solutions based on a general-purpose component model for autonomic communication services; specifically in such context autonomic service components autonomously achieve self-organization and self-adaptation towards the provision of adaptive and situated communication-intensive services.

CASACDAS approach is based on four key scientific principles i.e. situation awareness, semantic self organization, self similarity and Autonomic component awareness around which the future communication services infrastructures should be designed and built. [16]

8. Applications & future work –

The applications for WSNs are many and varied. They are used in commercial and industrial applications to monitor data that would be difficult or expensive to monitor using wired sensors. Typical applications of WSNs include monitoring, tracking, and controlling. Some of the specific applications are habitat monitoring, object tracking, nuclear reactor controlling, fire detection, traffic monitoring and so on.

1. Wireless sensor networks are currently being used for *intrusion detection* by forming a perimeter around a secure area and monitoring the progression of intruders (passing information from one node to the next). WSN's could be further deployed in Military applications such as hostile tracking and surveillance, spy monitoring.

2. Other major current application of WSN include environment monitoring and applications such as animal tracking, flood detection and weather prediction and forecasting and commercial applications like seismic activities monitoring and prediction. Many weather forecasting websites use WSN technology for retrieving weather details in remote inhibited areas. [23]

3. Significant amount of the technology and applications are already in existence for monitoring activities in home along with intrusion detection by equipping a home with a suitable sensor-laden infrastructure.

4. WSN's are used widely in automation and control and Artificial intelligence applications like Robotics.

5 Sensor networks are increasingly being used in Health applications for monitoring changes in patient's health, behaviour and heart rate.

By continuously monitoring the progressive disease, opportunities for actively intervening to aid the patient may be identified. The Ambient Assisted living technologies are in existence, which use WSN elements to assist the patient.

Resent research project at Wayne State University and the Kresge Eye Institute developed *artificial retina* using Wireless Biomedical sensors. The project aimed to build a chronically implanted artificial retina with sufficient visual functionality to allow persons without vision or with limited vision to "see" at an acceptable level. [17]

Moreover, this Wireless biomedical sensor technology can be effectively used to treat diabetes, by providing a more consistent, accurate, and less invasive method for monitoring glucose levels. Currently, to monitor blood glucose levels, a lancet is used to prick a finger; a drop of blood is placed on a test strip, which is analyzed either manually or electronically. This constant pricking several times a day over a period of years can damage the tissue and blood vessels in that area. As proposed by Schwiebert et al. [17], Wireless biomedical sensors could be implanted in the patient once. The sensor would monitor the glucose levels and transmit the results to a wristwatch display.

Wireless biomedical sensors may play a key role in early detection of Cancer. As discussed in [17], cancer cells exude nitric oxide, which affects the blood flow in the area surrounding a tumor. A sensor with the ability to detect these changes in the blood flow can be placed in suspect locations. It is likely that any abnormalities could be detected much sooner with the sensors than without.

RFID, video and various kinds of embedded sensors can be used to track and monitor the patient in their everyday activities. This information can be processed and relayed to medical personnel. Patient's routine can be assembled over the period of time and deviations from this may be recognized and analyzed.

9. Conclusion

Wireless Sensor Network technology offers significant potential in numerous application domains. Given the diverse nature of these domains, it is essential that WSNs perform in a reliable and robust fashion. I believe, wireless sensor network has proved its usage in the future distributed computing environment. However, there are significant amount of technical challenges and design issues those needs to be addressed. One of the biggest challenges is the designing of efficient network management architecture to continuously support WSNs for providing services for various sensor applications. The unique features of WSNs make the design and implementation of such management architecture different enough from the traditional networks which can be satisfied by concept of Autonomic Computing. There is still no particular generic network management architecture so taking inspiration from IBMs Autonomic Computing concept and Biological neural network system many different research projects are currently being executed.

In this paper, we discussed concepts of Autonomic computing, Wireless Sensor Networks (WSN's). Design criteria for WSN and how it matches basic Autonomic principles. Then we overviewed few architectures and routing protocols suitable for WSN and ongoing research work of Autonomic communication and network management architectures which can be applied to WSNs. Finally, we summarized some of the WSN applications along with future usages.

References

[01] P. Horn, "Autonomic Computing: IBMs Perspective on the State of Information Technology", Oct. 2001. Available from the World Wide Web (WWW): http://www.research.ibm.com/autonomic

[02] IBM and autonomic computing, "An architectural blueprint for autonomic computing," April 2003. Available from the WWW: http://www-03.ibm.com/autonomic/pdfs/ACwpFinal.pdf

[03] Kephart J, and Chess D, "The Vision of Autonomic Computing" Computer Magazine, IEEE, 2003. Available from WWW: http://www.research.ibm.com/autonomic/research/papers/AC_Vision_Computer_Jan_2003.pdf

[04] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on Sensor Networks," IEEE Communications Magazine, vol. 40, Issue: 8, pp. 102-114, August 2002. Available from WWW: http://citeseer.ist.psu.edu/akyildiz02survey.html

[05] Yu Mengjie, Mokhtar H., Merabti M., "A Survey of Network Management Architecture in Wireless Sensor Network" Available from WWW: www.cms.livjm.ac.uk/senman/Papers/2006-093.pdf

[06] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva, "Directed Diffusion for Wireless Sensor Networking," IEEE/ACM Transactions on Networking, vol. 11, pp. 2-16, Feb. 2003. Available from WWW: http://citeseer.ist.psu.edu/intanagonwiwat00directed.html

[07] O'Hare G.M.P., O'Grady M.J., D. Marsh, Ruzzelli A. G. and Tynan R. "Autonomic Wireless Sensor Networks: Intelligent. Ubiquitous Sensing" Available from WWW: www.cs.ucd.ie/csprism/publications/pub2006/ANIPLA06.pdf

[08] D. Marsh, R. Tynan, D. O'Kane and G. M. P. O'Hare, "Autonomic Wireless Sensor Networks," Engineering Applications of Artificial Intelligence, vol 17-7, pp. 741-748, October 2004. Available from WWW: http://tinyoside.ucd.ie/publications/retrieve.php?publication=tynanAutonomic05.pdf

[09] Yu Cheng et al., "A generic architecture for autonomic service and network management", Computer Communications (2006), doi:10.1016/j.comcom.2006.06.017. Available from WWW: http://www.ece.iit.edu/~yucheng/YCheng_CompCom.pdf

[10] P. Boonma, P. Champrasert and J. Suzuki, "BiSNET: A Biologically-Inspired Architecture for Wireless Sensor Networks," In Proc. of the 2nd IEEE/IARIA International Conference on Autonomic and Autonomous Systems (IEEE/IARIA ICAS), Santa Clara, CA, July 2006. Available from WWW: http://www.cs.umb.edu/~jxs/pub/icas-bisnet.pdf

[11] BISON: Biology-Inspired techniques for Self-Organization in dynamic Networks Project. http://www.cs.unibo.it/bison/index.shtml

[12] Shen C, Pesch D, Irvine J.,"A Framework for Self-Management of Hybrid Wireless Networks Using Autonomic Computing Principles" In proceedings of the 3rd Annual Communication Networks and Services Research Conference (CNSR'05) - Volume 00. Available from WWW: http://portal.acm.org/citation.cfm?id=1068503.1068711&coll=GUIDE&dl=GUIDE&CFID=9467744&CFTOKEN=44832813

[13] Colan, M. Service-Oriented Architecture expands the vision of Web services, Part 1. June, 2004

[14] ANA: Autonomic Network Architecture Project. http://www.ana-project.org/

[15] Haggle Project. http://www.haggleproject.org

[16] CASCADAS project. http://www.cascadas-project.org

[17] Schwiebert L., Gupta S., Weinmann J., "Research Challenges in Wireless Networks of Biomedical Sensors" in proceedings of the 7th annual international conference on Mobile computing and networking. Available from WWW: http://portal.acm.org/citation.cfm?id=381692

[18] Autonomic Computing Wiki. http://en.wikipedia.org/wiki/Autonomic_computing

[19] Linnyer Beatrys Ruiz, J.M.S.N., Antonio A.F. Loureiro, "MANNA: A Management Architecture for Wireless Sensor Networks." IEEE Communications Magazine, 2003. 41(2): p. 116-125. Available from WWW: http://www.lisha.ufsc.br/~lucas/docs/Ruiz-2003.pd

[20] Davy S. et al. “Policy-Based Architecture to Enable Autonomic Communications”. Available from WWW: http://techpubs.motorola.com/download/IPCOM000141400D/IPCOM000141400D.pdf
[21] Colan, M. Service-Oriented Architecture expands the vision of Web services, Part 1. June, 2004 Available from WWW: http://www-128.ibm.com/developerworks/library/ws-soaintro.html
[22] Gianni A., Di Caro, Frederick Ducatelle, Luca M. Gambardella, “BISON: Biology-Inspired techniques for Self-Organization in dynamic Networks” Available from WWW: http://www.idsia.ch/~frederick/bison.pdf
[23] Wireless Sensor Networks Wiki. http://en.wikipedia.org/wiki/Wireless_sensor_network
[24] W. R. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive Protocols for Informatio Dissemination in Wireless Sensor Networks," in proc. ACM MobiCom '99, Seattle, WA, 1999. Available from WWW: http://www.cs.huji.ac.il/labs/danss/sensor/sensors/kulik_99adaptiveprotocols.pdf
[25] S. M. Hedetniemi, S. H. Hedetniemi, and A. Liestman, "A Survey of Gossiping and Broadcasting in Communication Networks," Networks, vol. 18, 1988.
[26] J. Kulik, W. R. Heinzelman, and H. Balakrishnan, "Negotiation base protocols for Disseminating Information in Wireless Sensor Networks," Wireless Networks, vol. 8, pp. 169-185, 2002. Available from WWW: http://citeseer.ist.psu.edu/kulik99negotiationased.html
[27] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva, "Directed Diffusion for Wireless Sensor Networking," IEEE/ACM Transactions on Networking, vol. 11, pp. 2-16, Feb. 2003. Available from WWW: http://www.isi.edu/~johnh/PAPERS/Intanagonwiwat03a.pdf
[28] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Micro-Sensor Networks," in Proc. of the 33rd Annual Hawaii International Conf. on System Sciences, pp. 3005- 3014, 2000. Available from WWW: http://pdos.csail.mit.edu/decouto/papers/heinzelman00.pdf
[29] S. Lindsey, C. S. Raghavendra, "PEGASIS: Power-Efficient Gathering in Sensor Information Systems," presented at Proc. of IEEE Aerospace Conference, Montana, 2002. Available from WWW: http://ceng.usc.edu/~raghu/pegasisrev.pdf
[30] Y. Yu, R. Govindan, D. Estrin, "Geographical and Energy Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks," UCLA Computer Science Department UCLA-CSD TR-01-0023, May, 2001. Available from WWW:http://www.parc.com/zhao/stanford-cs428/readings/Networking/Estrin_geo-routing01.pdf
[31] Al-Obaisat Y, Braun R “On Wireless Sensor Networks: Architectures, Protocols, Applications, and Management” Auswireless Conference 2006. Available from WWW: http://epress.lib.uts.edu.au/dspace/bitstream/2100/160/2/59_Al-Obaisat.pd
TURE IN HETEROGENEOUS WIRELESS NETWORKS ENVIRONMENT