Performance Boost-Up by Using an Efficient Network Management Schemes in Wireless Sensor Network

Imran Khan Memon and Muhammad Khalid Khan

***Abstract*—Wireless Sensor Network (WSN) are becoming more challenging day by day; some of major challenges are security attacks, packet drops, high power consumptions, low battery backup and some connectivity problems, but the most significant problem is providing quality service under harsh environments, where sensor nodes, facing several problems such as batteries of sensor nodes not working properly, when temperature goes to very low in winter, reliability of monitoring system, energy and power losses etc, hence performance of network degrades greatly. By applying an Efficient Network Management Scheme (ENMS), we can handle these major drawbacks thus our network working accurately even in harsh environments.**

In this paper we have discussed Security, Fault and Performance management related issues in Wireless Sensor Network.

***Index Terms*—Wireless sensor networks, security management, fault management, performance management.**

I. Introduction

Wireless sensor network is smart technology that used widely in many important fields, such as Military, Traffic surveillance, Medical application etc, due to outstanding performance. In past few years, WSN have deployed in many small as well as large networks, because of higher needs for deploying in hostile environments or over large geographical areas. In this paper we have discussed basic uses and architecture of WSNs along with certain issues regarding Security, Fault, and Performance management.

A. Uses of Wireless Sensor Networks

Sensor networks can be used to monitor environmental changes. An example could be water pollution detection in a lake that is located near a factory that uses chemical substances. Sensor nodes could be randomly deployed in unknown and hostile areas and transmit the exact origin of an impurity to a centralized authority to take appropriate measures to limit the spreading of pollution. Such as forest fire detection, air pollution and rainfall observation in agriculture. Military uses sensor networks for battlefield surveillance; sensors could monitor track the position of the enemy or even safeguard the equipment of the side deploying sensors.

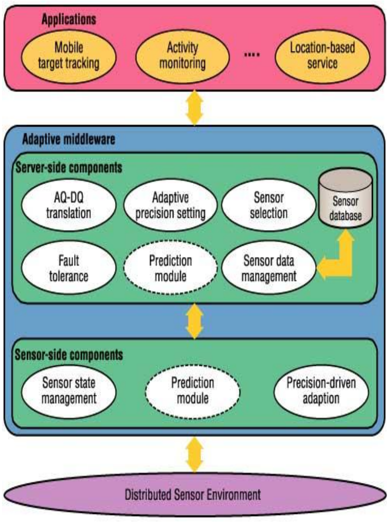

Fig. 1. Architecture of wsns. [16]

Sensors can also be used in large buildings or factories monitoring weather changes. Thermostats and temperature sensor nodes are deployed all over the building's area. In addition, sensors could be used to monitor vibration of earthquake that could damage the structure of a building.

Sensors can be used in biomedical applications to improve the quality of the provided care. Sensors are fixed in the human body to monitor medical problems like cancer and help patients maintain their health.

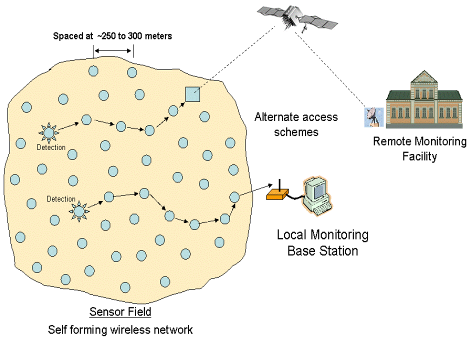
Spaced at ~250 to 300 meters
Detection
Detection
Alternate access schemes
Remote Monitoring Facility
Local Monitoring Base Station
Sensor Field
Self forming wireless network

Fig. 2. Wireless sensor network. [17]

The goal of this paper is resolve issues regarding Security, Fault and Performance Management in WSNS, to provide guaranteed and reliable service in dynamical situations.

II. Problems and Issues

A. Security Management Issues

In wireless sensor network security is major requirements of network infrastructure, some sufficient policies must be

Manuscript received July 15, 2012; revised September 10, 2012.

I. K. Memon is with the Department of Data Communication, National Telecommunication Corporation Karachi, Pakistan (e-mail: dr.imranmemon@gmailcom).

M. K. Khan is with the Department of Computer Science, Karachi Institute of Economics & Technology, (PAF KIET), Karachi, Pakistan (e-mail: khalid.khan@pafkiet.edu.pk).

adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access and the effectiveness or lack of these measures combined together, there are many securities issues in WSNs which are discussed below.

WSN is usually suffered from several kinds of security attack such as, Interruption, Interception, Modification, and Fabrication. [1]. these attacks are involving to breach all kinds of WSNs security.

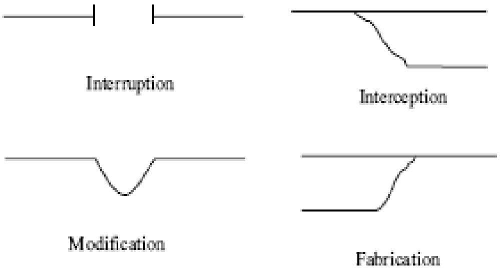

Fig. 3. Security issues in wsns [1]

In certain cases some networks becomes very risky because network of compromised nodes, in that case security will be more challenging to detect internal compromised nodes, through these nodes intruder can reaches at internal network.. Some sensor nodes are designed the goals of being small, in order to be utilized in different environments and relatively cheap so that many nodes can be deployed in the testing environments. This has lead to these sensors having constraints in terms of low computation, memory, and power available by the base stations and sensor nodes of the wireless sensor network [2]. Typically, the wireless sensor networks (WSNs) consisting of a large number of tiny sensors with limited resources are deployed in open, hostile, unattended environments, for a wide variety of applications, including object tracking, environment monitoring, smart environments, and so on. For efficiency, the sensor nodes usually form into groups clusters and perform in-network processing according to the inherently collaborative nature of wireless sensor networks, consequently, create needs for efficient and secure group communications. In certain cases key distribution centre doesn’t providing massive security during key sharing. [3]

B. *Fault Management Issues*

Fault management is a key part of WSNs, it covers operation functions such as detect, isolate, determine the cause and correct functions in a network. The objectives of doing fault management are to increase network availability, reduce network downtime and restore network failure quickly; WSNs are suffered from several fault management related issues which are listed below.

Basically, the latency time of ZigBee hardly becomes a problem in monitoring applications; Generally ZigBee is quite difficult to handle High-speed control applications. Specially, the control cycle in 1 second. In particular case of very low temperature in winter, mostly sensor nodes became challenging to manage because some time battery not working properly in very low temperature, also Cable based network infrastructure may creates some problems because of high electricity consumption and high cost [4].

In enterprise environments fault management does not fulfill all requirements of fault tolerance systems [5], thus performance of system highly degrades. Usually faults occur through malfunctioning hardware, software errors or by external causes such as fire and flood. In business applications where WSNs are applied, failures in essential parts of the sensor network must be efficiently detected and automatically recovered.

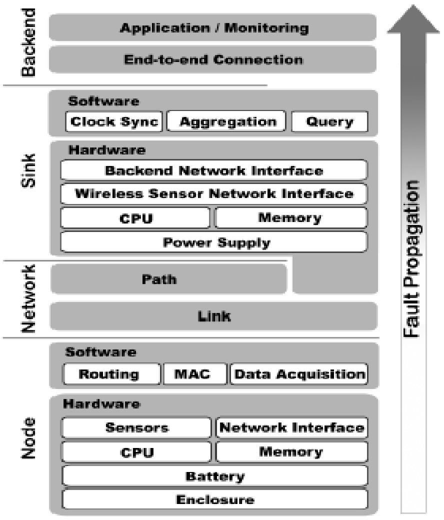

Fig. 4. Fault classification and propagation [5]

In some cases sensor nodes may suffered by limited range of connectivity to monitor any application [6], and a traditional monitor system doesn’t fulfill all the requirement of WSNs. Variations in applications, and avoid reinventing the wheel every time we are presented with a new problem.

Typically WSNs are suffered from limited bandwidth and limited energy, thus communication becomes more challenging, hence lifetime reduced greatly [7]. Mostly sensor nodes have limited energy and communication bandwidth, managing the utilization of these resources is a vital key in the design of wireless sensor network protocols. Inefficient use of energy can drastically reduce the network lifetime. In addition, inaccurate utilization of bandwidth may lead to more collision during data transmission and, therefore, more waste of energy.

In case of performance monitoring WSNs facing monitor operation failure, devices problems, batteries issues, and many other issues of environments, so it become more challenging for fault management [8]. Packet losses play an important role to degrading the quality and the quantity of collected data, due to the dependency of WSNs on neighbor’s node measurements in controlling and configuring network functionality. The random loss of received neighbor’s measurements may increase the Effect of the deviation of individual node operations and with this, non-ideal data gathering paths and data routing occurs.

Bluetooth based sensor network for short-range network is less powerful then traditional network, thus it cannot deals quickly to large amount of data [9]. WSN force many requirements on nodes, such as power expenditure, lake of maintenance for entire lifetime; or functional, such as automatic network assembly, scalability, high throughput etc. In order to meet all these requirements, it is necessary that the nodes be so small as to be able to be fabricated on a single chip. The radio access technique that the nodes use to communicate with each other should have a number of characteristics such as resistance to interference, fairly good throughput, and possibly some inbuilt security.

C. Performance Management Issues

Network performance management is essential part of WSNs, it provides planning, and usage based billing, understanding Quality of Service (QOS) of traffic, providing reports to customers/users to fulfill Service level and through performance management network administrator gets information about their networks.

Performance of WSNs is also one of the core issues, several performance degrading factors such as energy and power loses, sensing holes etc are involving to degrade the overall performance of WSNs, couples of more issues are discussed below.

Wireless sensor networks are susceptible to various types of security threats such as eavesdropping, message replay, and fabrication of messages. These threats can be avoided by introducing various safety mechanisms such as authentication, confidentiality, and message integrity.

far away from the node. Totally distributed approaches are also not suitable because each node has limited memory and computation power. In a distributed approach, each node needs to maintain the up-to-date.

On other hands Traditional trust management schemes which were developed for wired and wireless ad-hoc networks are not suitable for wireless sensor networks, because of their higher utilization of memory and power resources [10].

Routing problem for sensor networks differs from that of traditional ad hoc wireless networks because sensor nodes can be constrained by limited battery power, communication bandwidth and processing power. [11].

Generally Wireless sensor network are suffered from coverage and connectivity problems [12]. Typically in WSN, energy source provided for sensors is usually battery type, which has not yet reached the stage for sensors to operate for a long time without recharging. Moreover, sensors are often intended to deploy in remote or hostile environment, such as a battlefield or desert; it is undesirable or impossible to recharge or replace the battery power of all sensors. Therefore, the design for energy efficient Guarantees for the coverage and connectivity of wireless sensor networks problem, by using with minimum available information.

Single-path-based distributed TCP caching is not suitable for Wireless Sensor networks because of high packet drop ratio [12]. Some other drawbacks of sensor node, such as restricted telecommunication, computing and storing capability, limited energy without supplement; energy efficiency becomes the most prior consideration. Moreover, applying conventional TCP protocol into wireless networks with high packet drop rate cannot utilize its performance.

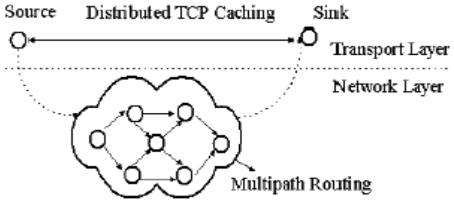

Fig. 5. MPDTC implementation on network layer and transport layer [12]

Energy conservation is obviously a core issue when designing a WSN since most nodes will be expected to be battery-powered. Strategies to cut down power consumption, whether acting at battery, hardware or protocol stack levels, are heavily investigated by researchers in the field [13].

Processing of Virtual Machine (VM) under wireless sensor networks environment has certain challenges of high power consumption and insufficient battery lifetime for execution on the wireless sensor network's nodes [14].

Wireless sensor nodes typically operate with a limited power source such as batteries. In most applications, battery Replacement is difficult or impossible. Thus, energy efficient protocols are crucial to obtain maximum network lifetime. The Transmission and reception of packets consume most of the energy. At present, most MAC protocols in wireless sensor Networks reduce energy consumption by reducing the idle time of the sensor nodes, such as SMAC, B-MAC [15].

III. Methodology/Approaches

A. Efficient Network Management Schemes

EFMS provides comprehensive solution of many issues such as security attacks, packet drops, high power consumptions, low battery backup and some connectivity problems etc, especially Fault management related issues, which faced by sensor nodes and monitoring server, EFMS techniques provides reliability under hostile environment, our proposed solution covers entire areas of network management such as, security, fault and performance management.

B. Security Management

Several kinds of attacks are involving to breach security of WSNs, thus four security mechanisms such as confidentiality, integrity, authentication and availability security services are sufficient to provide reliable services to protect Wireless Sensor Networks from many attacks such as Interruption, Interception, Modification, Fabrications etc. [1].

Anomaly-based intrusion detection system is reliable to detect compromised nodes in wireless sensor networks [2], first of all this system trying to detect compromised nodes by localization based anomaly diction and then after Network/Neighbors Stability Based Anomaly Detection, after perforating both process, our system protected from compromised nodes.

Authenticated Combinatorial Key Distribution (ACKDs), based on Exclusion Basis System (EBS) are sufficient to provide efficiency, and one-way hash chain are sufficient for authentication [3].

C. Fault Management

ZigBee wireless sensor network which perform very well even in heavy industrial environments, because of low cost, low electricity consumption and low data rate [6]. Zigbee operates three states such as, sensor node, sink node and gateway node.

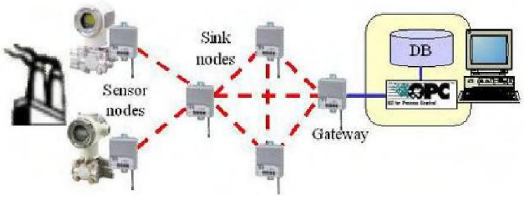

Fig. 6. Zigbee monitoring system [4]

Proposed FT-CoWiseNets framework is Efficient to improve the availability of Heterogeneous Wireless Sensor Networks through an efficient fault tolerance support which covers overall requirements and demonstrates to be more adequate to business scenarios than the current approaches [5]. It also prevent from isolate failure, Identify crash, omission, value and arbitrary failures and providing Provide automatic recovery techniques.

A General Purpose Framework is discussed for wireless sensor networks which are good enough to monitoring any application with a minimum amount of effort [6]. This framework performing several operations including, Design and testing of the basic functional block, Testing the functional blocks in different network configurations , Developing a general purpose network, Developing techniques for power conservation, Developing techniques to increase the overall system dependability

FTPASC (Fault Tolerant Power Aware protocol with Static Clustering), which holds high power sensor nodes to stop more power consuming tasks, to extend network lifetime [7]. FTPASC divided into two phases such as Setup Phase and Steady State Phase, in these phases controls high power consumption issues.

Distributed performance algorithm that ensure to detect problems and reduces the impact on network functionality [8]. It alerts for many warning such as neighbors warnings, testing packets warnings etc.

This paper considering Bluetooth Network is only best solution for short range and personal area sensor networks [9]. Currently peoples require wireless connectivity on their PC/LAPTOP/PALMTOP/SERVER without installation any equipment or devices, so Bluetooth will be good solution for providing setup/installation less communication, nowadays every laptop have built-in Bluetooth facility.

D. Performance Management

This paper proposes a group based trust management scheme (GTMS) for distributed wireless sensor networks which results is minimum resource utilization[10]. Three elements have to calculate in GTMS scheme, Trust Calculation at Node, Trust Calculation at Cluster Head and Trust Calculation at Base Station, GTMS scheme performing all operation with minimum amount of energy consumption.

The paper proposes an Efficient Power Management Protocol with Limited Cluster Size (EPMPLCS), which limits the size of clusters and avoids high energy consumption to enhance the network life [11]. EPMPLCS scheme based on two phases, setup phase and steady-state phase, both of these phases is well supported to fix high energy consumption issue.

Node scheduling scheme applied to resolve coverage and connectivity problems in wireless sensor networks [11]. This scheme performing operation based on three scheduling scheme for individual node they are: sensing, routing, and sleeping.

This scheme based on nodes, which is define in four states: listen, collision sense, active and l-duty.

In this paper the author adopts a multi-path-based distributed TCP caching algorithm on transport layer, and multi-path routing algorithm on the network layer to enhance transport reliability and overall performance [12].

A Simple Synchronization Algorithm to face timing and power consumption issues in an Industrial automation environment [13]. This algorithm working in three phases, Timing Phase, Data Phase, Sleep Phase, Timing Phases used to establish or maintain synchronization, where a data phase use for transport data in the network, and sleep phase used where the nodes are in low-power mode.

Proposed generalized processor architecture which allows hardware acceleration to reduce the power consumption for execution of Virtual Machine on WSN nodes [14]. This architecture, allows the accelerator to interfere in the execution of VM applications. When inactive it is possible that the accelerator will be supply or implemented using low leakage transistors

This paper proposes a transmission power control Sensor MAC (PSMAC) scheme which consumes minimum amount of energy for communication, and Sensor MAC (SMAC) scheme to avoid the collisions of nodes [15].

Our scheme that applied in order to enhance the performance of WSNs also provides massive support for fault management related works especially in disasters conditions or in hostile environment.

IV. Conclusions

Wireless sensor networks possess the potential to revolutionize business in a similar way to the emergence of the internet by providing a large number of users with various forms of information. But WSNs are suffered from many issues of security, fault and performance managements, these issues may handle by using, an efficient network management scheme (ENMS) which provides comprehensive solution to fixing discussed issues.

Still some research is required on fair fault management to increase intensity of wireless signal under covered area, also in bad weather conditions such as rains, hot and cold environment.

References

[1] T. Zia and A. Zomaya, *Security Issues in Wireless Sensor Network*, vol. 1, 2006.

[2] M. Mathews, M. Song Shetty, and R. McKenzie, “D. Compromised Nodes in Wireless Sensor Networks,” *Eighth ACIS International Conference on software Engineering, Artificial Intelligence*, Network and Parallel/Distributed Computing, vol. 1, 2007.

[3] L. Li, J. Li, L. Tie, and J. Pan, “ACKDs: An Authenticated Combinatorial Key Distribution Scheme for Wireless Sensor Networks,” *Eighth ACIS International Conference on software Engineering*, Artificial Intelligence, Network and Parallel/Distributed Computing, vol. 1, 2007.

[4] L. Zheng and ZigBee, “Wireless Sensor Network in Industrial Applications,” *SICE-ICASE International Joint Conference* 2006.

[5] L. M. S. D. Souza, “FT-CoWiseNets: A Fault Tolerance Framework for Wireless Sensor Networks,” in *Proc. of International Conference on Sensor Technologies and Applications*, vol.1, 2007.

[6] A. Z. Faza and S. Sedigh-Ali, “A general purpose framework for wireless sensor network applications,” in *Proc. of 30th Annual International Computer Software and Applications Conference (COMPSAC'06)*,vol. 1

[7] A. Khadivi and M. Shiva, in *Proc. of A Fault Tolerant Power Aware Protocol with Static Clustering for Wireless Sensor Networks*, vol. 1

[8] Y. J. Al-raisi and D. J. Parish, “Wireless Sensor Network Performance Monitoring,” in *Proc. of International Conference on Sensor Technologies and Applications*, vol. 1, 2007

[9] C. Dethe, D. Wakde, and C. Jaybhaye, “Bluetooth based Sensor Networks Issues and Techniques,” in *Proc. of First Asia International Conference on Modeling and Simulation (AMS’07)*, vol. 1, 2007.

[10] R. Ahmed, H. Jameel, S. Lee, S. Rajput, and Y. Jae S., “Trust Management Problem in Distributed Wireless Sensor Networks,” in *Proceedings of the 12th IEEE International Conference on Embeded and Real- Time Computing*, vol. 1, 2006.

[11] T.-Y. Byun, “An Efficient Energy Consumption Scheme Considering Coverage and Connectivity Problem in Wireless Sensor Networks,” in *Proc. of Fifth International Conference on Software Engineering Research, Management and Applications*, vol. 1

[12] Y. Liu, H. Huang, and K. Xu, “Multi-path-based Distributed TCP Caching for Wireless Sensor Networks,” in *Proc. of Eighth ACIS International Conference on Software Engineering*, Artificial Intelligence, Networking, and Parallel/Distributed, vol. 1

[13] N. Aakvaag M. Mtheesen, and G. Thonest, “ABB Corporate Research, Billingstad, Norway,” Timing and Power Issues in Wireless Sensor Networks an Industrial Test Cse; *Proceedings of the International Conference on Parallel Processing Workshops*, vol. 1, 2005.

[14] H. Oi and C. J. Bleakley, *Towards a Low Power Virtual Machine for Wireless Sensor Networks Motes*.

[15] Z. Zhao, X. Zhang, P. Sun, and P. Liu, “A transmission power control Mac protocol for wireless sensor networks,” in *Proceedings of the sixth International Conference on Networking*, vol. 1, 2007.

[16] International Seabed Authority. [Online]. Available: http://www.isa.org

[17] Alico Systems Home Page. [Online]. Available: http://www.alicosystems.com

Imran Khan Memon was born in Nawabshah, Pakistan on 15-03-1984, I have done MS (Computer Science) Specialization in Networks & Telecom from PAF KIET Karachi, Pakistan, in 2009. Currently He is working as ASSISTANT MANAGER (NETWORKS) in National Telecommunication Corporation, Karachi, Pakistan. Mr. Memon is member of PSQCA and WMO and Many other organizations related to my area.

Muhammad Khalid Khan was born in Karachi, Pakistan, He have done MS (Computer Science) from SZABIST Karachi, Pakistan. Currently He is working as DIRECTOR OF SCIENCE AND ENGINEERING DEPT AT PAF KIET, Karachi, Pakistan. Mr. Khalid is cooperate training of voirous banks such as State Bank, ABL, HBL.