Ingredients of Wireless Sensor Network Technique Using Artificial Intelligence and Virtualization

Reshmi. S[1], Ahamed Johnsha Ali. S[2], Suganya.V[3]

[1,2]Assistant Professor, [3]Student
[1,3]Department of Computer Science and Application, Sri Krishna Arts and Science College
[2]Department of Information and Computer Technology, Sri Krishna Adithya College of Arts and Science

***Abstract*: Next generation wireless sensor network must support ultra-reliable, low latency communication and intelligently accomplish a massive number of internet of things devices in real time, within a highly dynamic environment. The goal is to introduce computational intelligence competence for the wireless sensor networks to become adaptive to changes within a variety of functioning contexts and to exhibit intelligent behaviour. The characteristics of wireless sensor networks bring many challenges, such as the ultra large number of sensor nodes, dense distribution, changing topology structure, storage and communication competence. The employment of artificial network techniques to develop in network "intelligent computation" and "adaption" ability for wireless sensor networks to improve their functionality and survival aspects. Wireless sensor networks are gaining incredible importance of commercial application such as in smart phone automation, health care and industrial automation. Virtualization in sensor network may provide elasticity, cost effective solutions and rise manageability. This paper presents a wide array of state-of-the-art projects related to sensor network virtualization.**

Index Terms: Artificial Intelligence; Adaption; Intelligent Computation; Wireless Sensor Networks; Virtualization; Industrial automation.

1. INTRODUCTION

The main objective of Artificial Intelligence is to develop systems that rival the intellectual and interaction capabilities of a human being of the dispersed Artificial Intelligence pursues the same objective but focusing on human being societies. A paradigm is the current use for the development of dispersed Artificial Intelligence is based on the notion of multi-agent systems [1] [3]. A multi-agent system is formed by a number of interrelating smart systems called agents, and can be executed as a software program, as an enthusiastic computer, or as a robot. Intelligent agents in a multi-agent system interact among each other to organize their structure, assign tasks, and transaction knowledge [4] [5].

Recent advances in wireless communications and electronics have enabled the development of low-cost, low-power, multifunctional sensor nodes that are small in size and communicate untied over short distances [6] [7]. A sensor network consists of a large number of sensor nodes that are compactly organized either inside the phenomenon of interest or very close to it [8]. The WSN virtualization has been caused mainly from the realization that most of the sensor nodes in a WSN remain idle for most of the time. Sensor network virtualization is one of the best ways to exploit the physical sensor node. Virtualization of sensor networks can provide a platform upon which novel sensor network architectures can be built, investigated and evaluated. The importance of sensor virtualization is manifold at the age of worldwide monetary recession. VSN can provide cost effective and green technology resolutions to design smart houses and cities [9] [10].

2. WIRELESS SENSOR NETWORKS AND ARTIFICIAL INTELLIGENCE

An intelligent sensor is one that modifies its interior behaviour to enhance its capability to collect data from the corporal world and interrelates it in a receptive manner, to a base station or to a host system [11]. The functionality of intellectual sensor includes: self-calibration, self-validation, and compensation. The self- calibration means that the sensor can monitor the computing condition to decide whether a new standardization is needed or not. Self-validation applies accurate modelling error broadcast and error isolation or knowledge-based techniques [12] [13].

The use of Artificial intelligence techniques plays a key role in construction of intellectual sensor structures. Main research issues of the WSNs are absorbed on the coverage, connectivity network lifetime, and data fidelity. In the recent years, there has been a cumulative interest in the area of the Artificial Intelligence and distributed Artificial Intelligence and their methods for solving WSNs constrains, create new algorithms and new applications for WSNs [14] [15]. In this particular case Distributed Independent Reinforcement Learning proposed the use of communal intelligence in resource management within WSNs.

3. INGREDIENTS OF WIRELESS SENSOR NETWORK IN ARTIFICIAL INTELLIGENCE

3.1. *The Ability to Collect Data for Insight*

Just as all great wines start with great grapes, any meaningful AI solution begins with enormous amounts of excellence data. AI continually builds its intelligence over time through data collection and investigation, so the more diverse data that is collected, the smarter it gets [16]. Thus, it's crucial to be able to collect data in the Wi-Fi/BLE area from every device in real time, then send the evidence to the cloud where AI algorithms can investigate it promptly.

3.2. *Contextual Services*

Enterprises that are approval BLE and mobile apps in their wireless strategy are also fetching data from the mobile device to deliver on high-accuracy location services to enable related services. They need to be able to aggregate global meta data across customers [17]. That means not only collecting data for insight into specific client behaviour and location evidence but gaining insights and analytics across device types, operating systems, applications and more. This is key for baselining and monitoring trends, and recognizing macro issues early so they can be addressed pro-actively [18].

3.3. *Domain-Specific Design Intent Metrics*

Whether trying to build a system that can play Jeopardy, help a doctor analyze cancer or permit an IT administrator to diagnose wireless problems, AI resolutions need labelled data based on domain-specific knowledge to break the problem down into small sectors that can be used to train the AI models [19] [20]. This can be accomplished using design intent metrics, which are structured data categories for classifying and monitoring the wireless user experience.

3.4. *A Data Science Toolbox*

Now that the problem is divided into domain-specific chunks of metadata, this metadata is ready to be nursed into the powerful world of machine learning and big data [14] [16]. Various techniques, such as supervised or unsupervised machine learning and neural networks, should be labouring to analyze data and provide actionable perception.

3.5. *Security Anomaly Detection*

By detecting infrequent network activity at every level of the network, an AI-enabled stage can accurately detect prevailing and day-zero threats. In addition, location technology can be used to precisely locate accidental or spiteful rogue devices and provide location-based access to resources [18] [19].

3.6. *Virtual Wireless Assistant*

Most people experience concerted sifting when they pick a movie on Netflix or buy something from Amazon and receive references for other similar movies or items. Beyond approvals, collaborative filtering is also used to sort through large sets of data and put a face on an AI solution.

In wireless networking, this procedure can be used to turn all the data collection and enquiry into expressive insight or action. It is akin to a virtual wireless expert that helps to resolve complex problems.

4. VIRTUALIZATION OF WIRELESS SENSOR NETWORK

Virtualization of Sensor Network (VSN) is a brand-new investigation method in the field of Wireless Sensor Network (WSN). Before proceeding further, we need to clarify few basic insights and the difference between traditional WSN, conservative Virtual Sensor Network, Overlay Sensor Network and VSN.

In brief, a traditional wireless sensor network consists of a large quantity of sensor nodes that are thickly ordered either inside the phenomenon of interest or very close to it. In this paper VSN means virtualization of wireless sensor network. The term VSN in this paper is synonymously used for the process of virtualization of sensor network and for the network that sustenance virtualization.

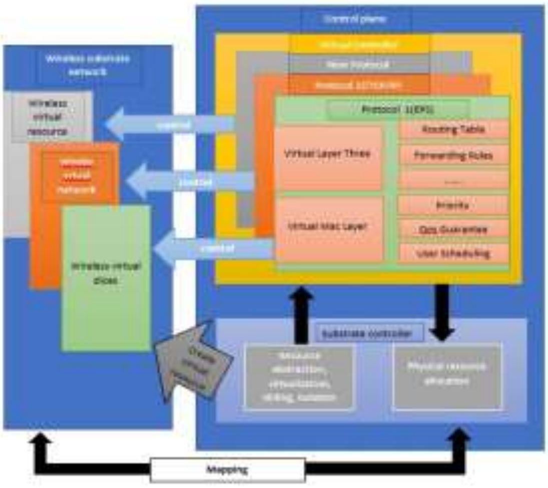

Fig 4.1 Mapping of wireless and physical resources

5. DESIGNING VIRTUALIZATION OF WIRELESS SENSOR NETWORK

5.1. *Design Goals Behind VSN*

The design goals for efficiently appreciating virtualization in sensor network have been lectured by dissimilar research groups. In order to appear the issues behind sensor network virtualization, each of these scheming principles should be satisfied.

5.2. *Flexibility*

Flexibility means designs that can adjust when peripheral changes occur. In designing VSNs we must pay courtesy to the given issue. Virtualization in sensor networks must provide freedom for every characteristic of sensor networking. Each sensor virtualization network service provider should be free to instrument chance for virtual sensor network topologies. It should also deliver flexibility in routing and encouraging functionalities, and modified control protocols that are self-determining of the fundamental physical sensor network and other coexisting SVNSPs. For example, organizing source routing in today's sensor network depends much on the compromise among the SInPs. In a virtualized environment, the owner of a SVNSP should be able to offer source routing without having to organize with any other parties. In short, source routing allows a sender of a packet to discreetly or entirely specify the route; the packet takes through the sensor network.

5.3. *Network Heterogeneity*

Heterogeneity is a significant issue in designing VSNs. Heterogeneity in the context of sensor network virtualization comes mainly from two perceptions: first, heterogeneity of the underlying sensor networking technologies i.e., sensor nodes of different vendors; second, each end-to-end SVNSP, created on top of that heterogeneous grouping of fundamental SInP, can also be heterogeneous. SVNSPs must be permitted to embrace and run cross field end-to-end VSNs without the need for any specific solutions. Fundamental infrastructures must also be talented of subsidiary mixed protocols and algorithms completed by different SVNSPs. The different types of sensor node concur in the same physical substrate sensor network. The heterogeneity is essential in the designing compound sensor network since it provides multiple types of services. The heterogeneity can be established in terms of sensor node disposition or the sensor network that is designed by the heterogeneous sensor nodes.

5.4. *Isolation*

Sensor Network virtualization must confirm separation between synchronized VSNs to recover fault-tolerance, safety, and discretion. Sensor network protocols are prone to misconfigurations and operation errors. Sensor virtualization must ensure that misconfigurations in one VSN are measured within itself and do not affect other co-existing VSNs.

Isolation allows logical parting of the VSNs although they overlap on same physical substrate sensor network. The device abstraction motivates strong software isolation: multiple diagrams of natural sensing applications use their virtual sensor as if it were an enthusiastic physical sensor. Strong isolation also varieties performance: each user's performance is a function of dispersal of device's resources. Sharing guarantees as a minimum fraction of a sensor's resources.

5.5. *Manageability*

Managing VSN requests has always been a key part of VSN design. In VSNs each SVNSP remains self-determining over a joined physical sensor network. By unravelling SVNSPs from SInPs, sensor network virtualization will modularize network management tasks and introduce accountability at every layer of networking architecture. It must provide complete, end to end control of the VSNs to the SVNSPs obviating the obligation of organization across administrative limitations as seen in the current WSN domain.

5.6. *Scalability*

Existence of multiple sensor networks is one of the essential principles of sensor network virtualization. Scalability comes as an essential part of this equation. SInPs obligation scale to sustenance an increasing number of coordinated VSNs without distressing their routine. For designing a large scale merged sensor network, it is essential to design the VSN scalable so that any type of alteration or addition of further physical sensor network can be easily done.

5.7. *Stability and Convergence*

Isolation confirms that faults in one VSN do not disturb other synchronized VSNs, but errors and misconfigurations in the fundamental physical network can also disrupt a sensor network virtualization environment. Moreover, uncertainty in the SInPs can lead to variability of all the hosted VSNs. VSNs must ensure the solidity of sensor virtualization environment and in case of any instability the affected VSNs must be able to successfully meet to their stable states.

5.8. *Programmability*

To ensure flexibility and manageability, programmability of the virtual sensor network rudiments is a necessary obligation. Only through programmability, SVNSPs can contrivance personalized protocols and arrange diverse services. Two pressing questions in this respect must have reasonable answers: how much programmability should be allowed? And how it should be exposed? A win-win situation must be found where programmability is easy, operative, and protected at the same time. For sharing the resources of the resource inhibited sensor node programmability may provide a chance to do further research activities in VSNs.

5.9. *Legacy Support*

Legacy provision or regressive compatibility has always been a stock of deep concern when establishing any new expertise. Theoretically, sensor network virtualization can simply integrate legacy support by seeing the prevailing WSN province as just another VSN into its congregation of sensor network.

6. EXPERIMENTAL AND DEPLOYMENT FACILITY

Before arrangement, any physically dispersed in sensor network service is naturally intended and estimated in test labs in a measured environment. Since it is very limited production of sensor network, tests are insufficient to simple topologies and traffic patterns that do not essentially characterize the real-world environment.

Moreover, migration of a sensor network to a dissimilar condition can also be extremely painstaking. By developing the service in a separate virtual sensor network from the very beginning can electively improve these problems. In addition, organizing new end-to-end services could not be easier than arranging it on a detached virtual sensor network of its own.

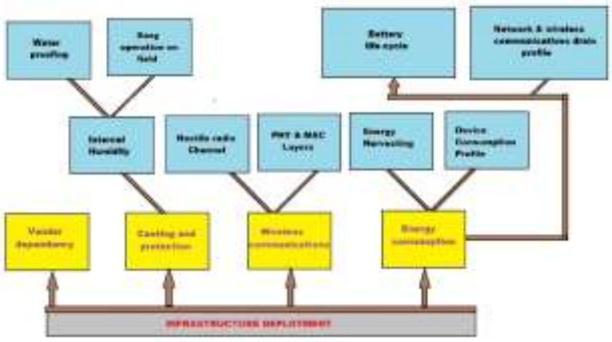

Fig 6.1: Communication Infrastructure Deployment

7. CONCLUSION

It is possible to contrivance a resolution that enables a sensor network to behave as an intellectual multi-agent system through the proposed model due to it exploits multi-agent systems together with layered architecture to simplify intelligence and pretend any

WSN, all needed is to know the final application, where the WSN is going to be deploy. Also, a layered architecture can provide modularity and structure for a WSN system.

Moreover, proposed model emphasizes about WSN works and to make it intelligent. Virtualization in sensor networks could be real in scenarios like smart home automation, patient monitoring, battlefield surveillance, rock slides and animal crossing in a mountainous terrain, among others.

Multivendor sensor network architecture could be organized for efficient utilization of physical sensor organization. By allowing multiple assorted wireless sensor network architectures to coexist on a shared physical substrate, virtualization of sensor networks might provide a new business model which could be cost in terms of deployment. For this purpose, we are working on the progress of a virtual machine which is suitable for tiny sensor nodes and will enable true virtualization of wireless sensor networks.

REFERENCES

[1] Cheong, E. (2007). Actor-oriented programming for wireless sensor networks. Conte, R., Gilbert, N. & Sichman, J. (1998). MAS and social simulation: A suitable commitment, Multi-Agent Systems and Agent-Based Simulation, Springer, pp. 1–9.

[2] CRULLER, D., Estrin, D. & Srivastava, M. (2004). Overview of sensor networks, Computer 37(8): 41–49. Davoudani, D., Hart, E. & Paechter, B. (2007). An immune-inspired approach to speckled computing, Artificial Immune Systems pp. 288–299.

[3] Egea-Lopez, E.,Vales-Alonso, J.,Martinez-Sala, A.,Pavon-Marino,P.& Garcia-Haro,J.(2006). Simulation scalability issues in wireless sensor networks,IEEECommunicationsMagazine 44(7): 64. Georgeff, M., Pell, B., Pollack, M., Tambe, M. & Wooldridge, M. (1998).

[4] The belief-desireintention model of agency, Intelligent Agents V. Agent Theories, Architectures, and Languages: 5th International Workshop, ATAL'98, Paris, France, July 1998. Proceedings, Springer, pp.

[5] Akyildiz, I.F.; Su, W.; Sankarasubramaniam, Y.; Cayirci, E. A survey on sensor networks. IEEE Commun. Mag. 2002, 40, 102-114.

[6] Akka, K.; Younis, M. A survey on routing protocols for wireless sensor networks. Ad. Hoc. Netw. 2005, 3, 325-349.

[7] Olariu, S.; Xu, Q. A simple and robust virtual infrastructure for massively deployed wireless sensor networks. J. Comput. Commun. 2005, 28, doi: 10.1016/j.comcom.2004.12.038.

[8] Shelby, Z.; Bormann, C. 6LoWPAN: The Wireless Embedded Internet; John Wiley & Sons Ltd: Hoboken, NJ, USA, 2009.

[9] Rodrigues, J.J.P.C.; Neves, P.A.C.S. A survey on IP-based wireless sensor network solutions. Int. J. Commun. Syst. 2010, 23, 963-998.

[10] Islam, M.M.; Huh, E.-N. Sensor proxy mobile IPv6 (SPMIPv6)—A novel scheme for mobility supported IP-WSNs. Sensors 2011, 11, 1865-1887.

[11] Islam, M.M.; Huh, E.-N. A novel addressing scheme for PMIPv6 based global IP-WSNs. Sensors 2011, 11, 8430-8455.

[12] Faghih, M.M.; Moghaddam, M.E. SOMM: A new service-oriented middleware for generic wireless multimedia sensor networks based on code mobility. Sensors 2011, 11, 10343-10371.

[13] Alam, S.; Chowdhury, M.M.R.; Noll, J. Virtualizing sensor for the enablement of semantic-aware internet of things ecosystem. Int. J. Des. Anal. Tools Circuits Syst. 2011, 2, 41-51.

[14] Reshmi. S, and M. Anand Kumar, "A REVIEW ON OBFUSCATION AND HEURISTICS ALGORITHM IN NETWORK VIRTUALIZATION", International Journal of Advanced Research in Computer Science, IJARCS & ISSN No. 0976-5697, Volume 8 (8), Sep-Oct 2017, Pg: 264-268, DOI: http://dx.doi.org/10.26483/ijarcs.v8i8.4651.

[15] Reshmi. S, Kirthika. B and Deepa. B, "SHIELDING NETWORK VIRTUALIZATION USING CBC-MAC FOR IMMINENT INTERCONNECTED NETWORKS", International Journal of Computer Science and Mobile Applications, IJCSMA & ISSN: 2321-8363, Impact Factor: 4.123, Volume 5 (10), Oct 2017, pg: 123-130.

[16] Reshmi. S, and M. Anand Kumar, "IMPLEMENTATION ON IDENTIFYING PACKET MISBEHAVIOR IN NETWORK VIRTUALIZATION", ARPN Journal of Engineering and Applied Sciences & ISSN 1819-6608, VOL. 13, NO. 4, 20th February 2018, Pg: 1284-1296.

[17] Vikash. S, Praveen. T, Anita. P, Suganya. V, Reshmi. S "HIGHLIGHTING THE VITAL CYPHER BY MEANS OF FORMING INSIGHT ABOUT CLOUD COMPUTING THROUGH VIRTUALIZATION", International Journal for Research in Applied Science & Engineering Technology, IJRASET & ISSN: 2321-9653, SJ Impact Factor: 6.887, Vol. Issue XII, Dec 2018, pg. 638-644.

[18] Reshmi. S, and M. Anand Kumar, "Survey on Identifying Packet Misbehaviour in Network Virtualization", Indian Journal of Science and Technology, INDJST & ISSN (Online): 0974-5645, Vol 9; Issue 31, August 2016, Pg: 1-11.

[19] Reshmi. S, and M. Anand Kumar, "Secured Structural Design for Software Defined Data Center Networks", International Journal of Computer Science and Mobile Computing, IJCSMC & ISSN 2320–088X, IMPACT FACTOR: 5.258, Vol.5 Issue.6, June- 2016, pg. 532-537.

[20] M. Anand Kumar, Dr. S. Karthikeyan (2011), "Security Model for TCP/IP Protocol Suite", Journal of Advances in Information Technology, 2[2], 87-91.