RESEARCHERID
THOMSON REUTERS
[INIT: January 2017]
ISSN 2348 – 8034
Impact Factor- 4.022

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

RELIABILITY EVALUATION OF WIRELESS SENSOR NETWORKS-A STUDY

Divya.R[*1] & Dr.R.Chinnaiyan[2]
[*1]Research Scholar, Dept. of Master of Computer Applications, New Horizon college of Engineering, Bangalore, India
[2]Professor, Dept. of Master of Computer Applications, New Horizon college of Engineering, Bangalore, India

ABSTRACT

Reliability Evaluation of WSN is an interesting topic in the communication networking environment which has an outrageous development over the traditional method and has to be adopted in the industrial environment for the mile connections in the field of networking .The WSN is also an startling need in the communication network to transport, chunks of data that are forwarded in node to node form in most of the application in the current developing world , which has adaptive link control and enhanced hop-by-hop reliability. The WSN has hundreds to thousands of sensor points which enable the evaluation of permanent faults, optimize the fault occurrences (by improving the WSN QoS), sensor fusion, collaborative target tracking, along with this the Zigbee based networking solution is speedily raising as one of the best choices in order to provide the consistent WSN environment among the multiplicity of sensor network applications. On this aspect, this paper aims to discuss the technology to evaluate the reliability of wireless sensor network .

Keywords- *wsn; Qos; sensor fusion; hop-by-hop; Zigbee;*

I. INTRODUCTION

A Wireless sensor network has been used in variety of areas such as optical, thermal, seismic, aural, and mesmeric, that can monitor heat, sound , radioactivity, force , speediness and article movement. It is to analyse the reliability issues and importance of diverseed fault tolerance, where a single type of sensor backs up heterogeneous types of sensors .

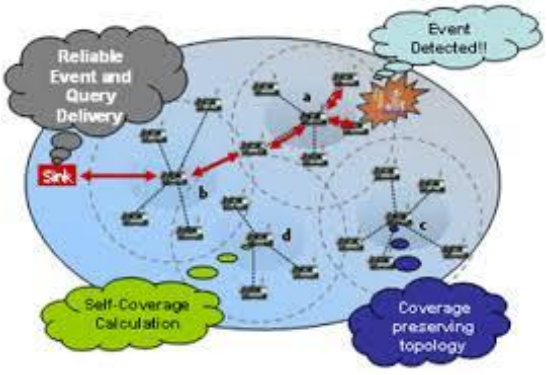


Fig 1.1 Heterogeneous Wireless sensor network

Heterogeneous wireless sensor network (heterogeneous WSN) consists of sensor nodes with different ability, such as different computing power and sensing range. Compared with homogeneous WSN, deployment and topology control are more complex in heterogeneous WSN. It is a relatively simple model of hierarchical WSN, and the model consists of three layers:

ISSN 2348 – 8034
Impact Factor- 4.022

- The middle layer : It consists of sensor nodes(self coverage calculation) , here it may be hundred to thousands of sensor nodes.
- The inner-most layer : It consists of the topology of nodes(covereage preserving topology).
- The bottom layer : It consists of sink(reliable event and query delivery); nodes in sub network collect all perceptual information of sensor nodes ,then each sink node in subnets transmits all the information to the monitoring center in multi-hop way.
- The top level : It consists of the monitoring centre ,and it is the control decision centre to end user(event detection).
-

II. WIRELESS SENSOR NETWORK

WSN relaibility

WSNs are heavily deployed for a wide range of applications. Wireless sensor networks are a scattered, self-organization solution to provide sensing and computing in various environments where conventional networks are impractical.

WSN related issues

Firstly, reliability in wireless sensor networks is an intractable issue due to the limited power and computing capability of little sensors [1][2]. The cost for processing power and wireless communication started to decrease which eventually made WSNs more reasonable and more attractive[3].The work has focused mainly on QoS-based protocols and mechanisms both in MAC and network layers. The results of this work can be consulted to find the consistent issues.[4].It's necessary to study how reliability can be guaranteed in such an issues. There are two well-known ways to achieve reliability on multi-hop paths: multipath and retransmission [5-6].

III. STRUCTURE OF WSN AND CLASSIFICATION

The structure of wireless sensor network has two categories, that is, flat structure and hierarchy structure [9-11],

Reliability of WSN, depends on combination of hard- ware, software and wireless link is modeled in many ways the to reliability modeling of hardware system.Two of the most commonly used are: Deterministic reliability modeling Probabilistic models, but probabilistic not suitable for modeling the reliability of real time applications of WSN [11].

Traditional WSN

This is a traditional single-sink WSN (see Figure 1, left part). Almost all scientific papers in the literature deal with such a definition. This single-sink scenario suffers from the lack of scalability: by increasing the number of nodes, the amount of data gathered by the sink increases and once its capacity is reached, the network size cannot be augmented. Moreover, for reasons related to MAC and routing aspects, network performance cannot be considered independent from the network size. A more general scenario includes multiple sinks in the network (see Figure 2, right part) [13].

ISSN 2348 – 8034
Impact Factor- 4.022

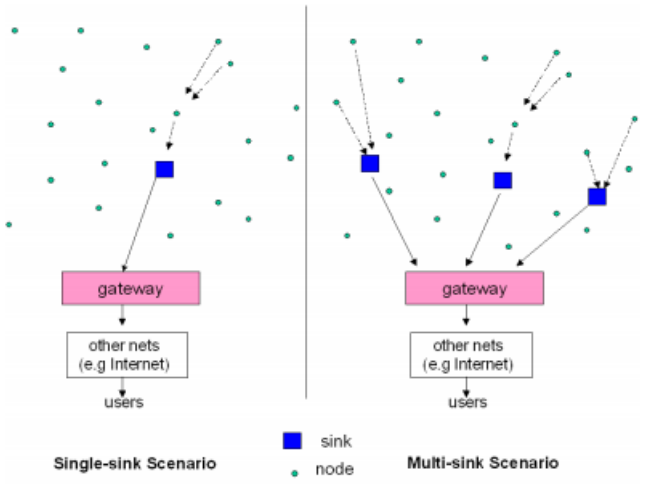


Fig 2. Left side:single sink WSN ;Right side: Multi-sink

Applications of WSN

The variety of possible applications of WSNs to the real world is practically unlimited, from environmental monitoring [7], health care [8], to logistic, localization, and so on. A possible classification for applications is provided in this section. It is important to underline that the application strongly affects the choice of the wireless technology to be used. Once application requirements are set, in fact, the designer has to select the technology which allows to satisfy these requirements. To this aim the knowledge of the features, advantages and disadvantages of the different technologies is fundamental.

Event detection Application

In the first case sensors are deployed to detect an event, for example a fire in a forest, a quake, etc. [17][23-24]. Signal processing within devices is very simple, owing to the fact that each device has to compare the measured quantity with a given threshold and to send the binary information to the sink(s). The density of nodes must ensure that the event is detected and forwarded to the sink(s) with a suitable probability of success while maintaining a low probability of false alarm. The detection of the phenomenon of interest (POI) could be performed in a decentralized (or distributed) way, meaning that sensors, together with the sink, cooperatively undertake the task of identifying the POI. However, unlike in classical decentralized detection problems, greater challenges exist in a WSN setting. There are stringent power constraints for each node, communication channels between nodes and the fusion center are severely bandwidth-constrained and are no longer lossless (e.g, fading, noise and, possibly, external sources of interference are present), and the observation at each sensor node is spatially varying. In the context of decentralized detection, cooperation allows exchange of information among sensor nodes to continuously update their local decisions until consensus is reached across the nodes.

ISSN 2348 – 8034
Impact Factor- 4.022

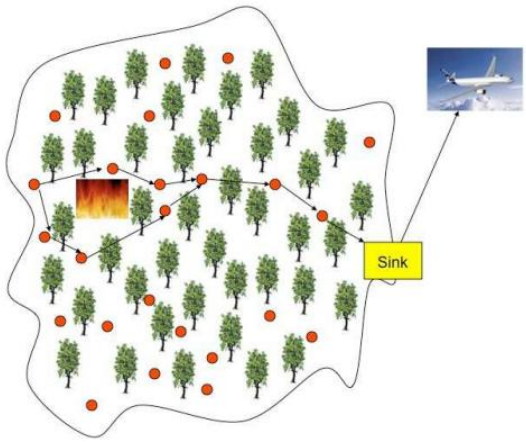


Fig 3: Event detection Application

For example, the location of a fire in a forest, or the detection of a quake, etc. (see Figure 3). Alternatively, the estimation of the temperature of a given area belongs to the second category. In general, these applications aim at monitoring indoor or outdoor environments, where the supervised area may be few hundreds of square meters or thousands of square kilometers, and the duration of the supervision may last for years. Natural disasters such as floods, forest fires, earthquakes may be perceived earlier by installing networked embedded systems closer to places where these phenomena may occur. Such systems cannot rely on a fixed infrastructure and have to be very robust, because of the inevitable impairments encountered in open environments. The system should respond to environment changes as quick as possible. The environment to be observed will mostly be inaccessible by the human all the time. Hence, robustness plays an important role. Also security and surveillance applications have some demanding and challenging requirements such as real-time monitoring and high security.

$$\alpha + \beta = \chi. \qquad (1) \qquad (1)$$

IV. WSN MODELS FOR RELIABLE NETWORK

Access control Models

There are two original access control models in information systems, which are mandatory access control (MAC) [18] and discretionary access control (DAC) [19]. MAC manages access control levels by means of an administrator in the organization. It uses a hierarchical approach to control access to the objects, which represent system resources here. The administrator defines an access control policy that cannot be modified by the subjects. MAC is mostly used in the systems where priority is placed on confidentiality, such as in military applications. The concept of an access control matrix, which defines the relationships between subjects, objects and the actions that the subjects want to perform on the objects, was introduced by Butler Lampson [20]. The subjects' identities are placed in rows and the objects' identities in columns. Each action that a subject wants to perform on an object is placed in the intersection of the corresponding row and column. The size of the access control matrix is directly proportional to the number of subjects and to the number of objects. Samarati and Vimercati [21] suggested that there are three possible approaches to implement the access control matrix in electronic systems, named authorization table, access control list (ACL) and capabilities.

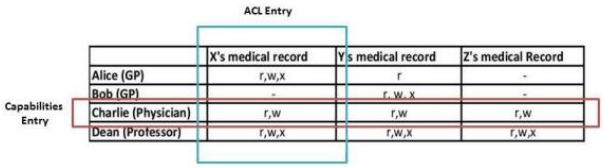
Traditional access control models

Authorization Table :A three-dimensional table, corresponding to subjects, actions and objects, respectively. Each entry in the table corresponds to an authorization.

• Access Control List (ACL): Each ACL contains the list of subjects and their access permissions to a given object. When a subject tries to access an object, the ACL for that object is used to verify the request from the subject. If the subject access pair is in the ACL list, access will be granted. Otherwise, access will be denied. In the ACL approach, the lists of subject and action pair are stored for each object. An ACL is represented by a column in the matrix table as seen in Figure 1. In this figure, r, w and x stands for read, write and executable.

• Capabilities: Capabilities are different from ACLs. Pairs of action and object are stored for each subject in the access control matrix. In a capability approach, the subject can get access to the object, when he presents the correct capability to the system. A subject's capabilities are represented by a row in the access control matrix.

Difference between access control list (ACL) and capabilities.



	X's medical record	Y's medical record	Z's medical Record
Alice (GP)	r,w,x	r	-
Bob (GP)	-	r, w, x	-
Charlie (Physician)	r,w	r,w	r,w
Dean (Professor)	r,w,x	r,w,x	r,w,x

Access control models in wsn's

Access Control Models in WSNs A considerable number of access control models has been proposed for use in WSNs, though some of them are not yet implemented. In this section, we present the proposed access control models before we compare and contrast them in the next section. We group the proposed models into three main categories based on the nature of their architecture, namely: role-based access control (RBAC), cryptography-based access control (CBAC) and users' privacy preserving access control (UPPAC). A taxonomy of access control models for WSNs, including the publication year of each proposal.

Role-Based Access control models

Most of the access control models in WSNs and WMSNs are based on traditional RBAC [22], which has been widely accepted as a policy-based access control model. Applications based on RBAC have been implemented and deployed in commercial companies and education industries. The principle of RBAC model is the role, defined as an intermediary concept relating a group of subjects to a set of access permissions. Any member from the subject group role has all of the permissions that are associated with that role. When a new subject is assigned to a group, he receives all of the associated access permissions, but these permissions are revoked when the subject leaves the group or is removed from the system. It is the same procedure to add and remove permissions from the roles. When a permission is added to a role, all of the members of the associated subject group will receive that permission. The permission will be revoked when it is deleted from the role. This feature helps to simplify system administration when there are many thousands of subjects and objects in an organization. In RBAC, the access decision is a choice between two outcomes: permitted access or denied access. The following access control models are proposed based on the RBAC model with different extensions to provide further security properties in WSNs.

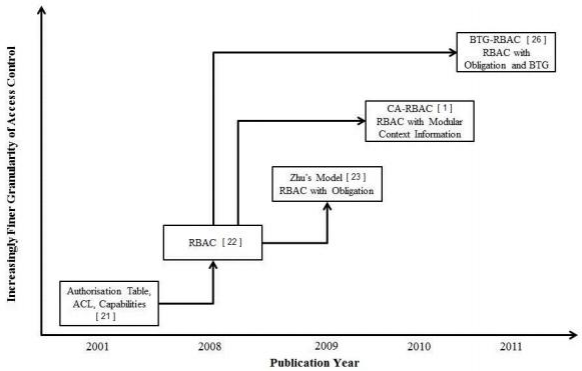


Fig 5:evolution of role based control model

F.Cryptography -Based Access control models

Cryptography-Based Access Control (CBAC) Cryptography-based access control (CBAC) is another form of access control model for the information systems. Ghani et al. [26] mentioned that the CBAC mechanism is designed for untrusted environments, where a lack of global knowledge and control are defining characteristics. The main idea is

to use a unique key for each data resource. Users who are allowed to access that data resource are assigned the key for data access [27]. Cryptography methods in WSNs should meet the constraints of sensor nodes, such as limited power, resources and memory shortage. Therefore, choosing a suitable cryptography method is important in WSNs. There are two types of cryptographic method; asymmetric encryption, known as public key cryptography (PKC), and symmetric encryption, known as symmetric key cryptography (SKC). The PKC-based scheme provides better data access security than SKC in the open multi-user environment [28]. The nature of PKC is using two keys: one for encryption and one for decryption. In PKC, the data encryption is usually targeted to only one recipient or one group. This means that any message encrypted by using a public key can be decrypted only with the corresponding private key.

V. CONCLUSION

The paper is aimed to the performance evaluation and comparison of the proposed models in WSNs. Also obain the wireless sensor netywork reliability based on the event detection in the sensor structure ,which has done the management of the heterogeneous wirless sensor networks.. Access control is a critical security service in sensor networks and is essential to ensure that network services are offered only to legitimate users in WSNs.Here in this paper ,tried to propose different models which are specified[12] through various access control based models , which here proposed the models to find the reliability of the wireless sensor networks. In comparison of present access control models showed that there is still plenty of work to be done on access control models in WSNs, especially for emergency and immediate data access.

REFERENCES

1. *Andreas Willig, Holger Karl. "Data Transport Reliability in Wireless Sensor Networks---A survey of Issues and Solutions", 2005. [2] Dazhi Chen and Pramod K. Varshney. " QoS Support in Wireless Sensor Networks:A survey",Internatioal Conference on Wireless Networks, 2004*
2. *Kuorilehto, M., H¨annik¨ainen, M., H¨am¨al¨ainen, T.D.: A survey of application distribution in wireless sensor networks. EURASIP J. Wirel. Commun. Netw. 2005(5),774–788 (2005).*
3. *J.F. Martinez, A.B. Garcia, I. Corrector, L. L6pez, V. Hernandez and A. Dasilva, "QoS in Wireless Sensor Network: Survey and Approach". To be published in Proc. IEEE/ACM EATIS, May*
4. *Qunfeng Dong, Suman Banerjee, Micah Adler, Archan Misra."Minimum Energy Reliable Path Using Unreliable Wireless Links". MobiHoc 2005.*
5. *B. Deb, S. Bhatnagar and B. Nath , "ReInForm: Reliable Information Forwarding using Multiple Paths in Sensor Networks", Proc. of IEEE LCN, 2003.*
6. *Rajaravivarma, V.; Yang, Y.; Yang, T. An Overview of Wireless Sensor Network and Applications. In Proceedings of 35th Southeastern Symposium on System Theory, Morgantown, WV, USA, 2003; pp. 432–436.*
7. *Verdone, R.; Dardari, D.; Mazzini, G.; Conti, A. Wireless Sensor and Actuator Networks; Elsevier: London, UK, 2008.*
8. *Verdone, R. Wireless Sensor Networks. In Proceedings of the 5th European Conference, Bologna, Italy, 2008.*
9. *Culler, D.; Estrin, D.; Srivastava, M. Overview of sensor networks. IEEE Comput. Mag. 2004, 37, 41–49.*
10. *Basagni, S.; Conti, M.; Giordano, S.; Stojmenovic, I. Mobile Ad Hoc Networking; Wiley: San Francisco, CA, USA, 2004.*
11. *Htoo Aung Maw et.al; 23 January 2014; in revised form: 20 May 2014 / Accepted: 11 June 2014 / Published: 20 June 2014*
12. *Lin, C.; Tseng, Y.; Lai, T. Message-Efficient In Network Location Management in a Multi-sink Wireless Sensor Network. In Proceedings of IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, Taichung, Taiwan, 2006; pp. 1-8.*
13. *Ong, J.; You, Y.Z.; Mills-Beale, J.; Tan, E.L.; Pereles, B.; Ghee, K. A wireless, passive embedded sensor for real-time monitoring of water content in civil engineering materials. IEEE Sensors J. 2008, 8, 2053–2058.*

14. *Lee, D.-S.; Lee, Y.-D.; Chung, W.-Y.; Myllyla, R. Vital sign monitoring system with life emergency event detection using wireless sensor network. In Proceedings of IEEE Conference on Sensors, Daegu, Korea, 2006.*
15. *Hao, J.; Brady, J.; Guenther, B.; Burchett, J.; Shankar, M.; Feller, S. Human tracking with wireless distributed pyroelectric sensors. IEEE Sensors J. 2006, 6, 1683–1696.*
16. *Lucchi, M.; Giorgetti, A.; Chiani, M. Cooperative Diversity in Wireless Sensor Networks. In Proceedings of WPMC'05, Aalborg, Denmark, 2005, pp. 1738–1742.*
17. *Ferraiolo, D.F.; Kuhn, D.R. Role-based access controls. In Proceedings of the 15th National Computer Security Conference, Baltimore, MD, USA, 13–16 October 1992.*
18. *Sandhu, R.; Munawer, Q. How to do discretionary access control using roles. In Proceedings of the 3rd ACM Workshop on Role-Based Access Control, Fairfax, VA, USA, 22–23 October 1998.*
19. *Lampson, B. Protection. In Proceedings of the 5th Princeton Conference on Information Sciences and Systems, Princeton, NJ, USA, January 1971.*
20. *Samarati, P.; Vimercati, S. Access control: Policies, models, and mechanisms. In Foundation of Security Analysis and Design; Springer: Berlin Heidelberg, Germany, 2001; Volume 2171, pp. 137–196.*
21. *Zhao, G.; Chadwick, D.W. On the modeling of bell-lapadula security policies using RBAC. In Proceedings of the 2008 IEEE 17th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE '08), Washington, DC, USA, 23–25 June 2008; pp. 257–262.*
22. *Quek, T.; Dardari, D.; Win, M.Z. Energy efficiency of dense wireless sensor networks: To cooperate or not to cooperate. IEEE J. Select. Areas Commun. 2007, 25, 459–470.*
23. *Toriumi, S.; Sei, Y.; Shinichi, H. Energy-efficient Event Detection in 3D Wireless Sensor Networks. In Proceedings of IEEE IFIP Wireless Days, Dubai, United Arab Emirates, 2008*
24. *Dâmaso, A.V.L.; Rosa, N.S.; Maciel, P.R.M. Using Coloured Petri Net for Evaluating the Power Consumption of Wireless Sensor Network. Int. J. Distrib. Sens. Netw. (IJDSN) 2014, 2014, 13.*
25. *Ghani, N.A.; Selamat, H.; Sidek, Z.M. Analysis of existing privacy-aware access control for e-commerce application. Glob. J. Comput. Sci. Technol. 2012, 12, 1–5.*
26. *Al-Hamdani, W.A. Cryptography based access control in healthcare web systems. In Proceedings of 2010 Information Security Curriculum Development Conference (InfoSecCD '10), Kennesaw, GA, USA, 1–3 October 2010; pp. 66–79.*
27. *Yu, S.; Ren, K.; Lou, K. Fdac: Toward fine-grained distributed data access control in wireless sensor networks. IEEE Trans. Parallel Distrib. Syst. 2011, 22, 673–686.*
28. *Chinnaiyan, R. And Somasundaram , S., Evaluating the Reliability of Component Based Software Systems , International Journal of Quality and Reliability Management (IJQRM), Vol.27, No.1,2010, pp. 78 – 88.*