A Survey on Fault Detection in Wireless Ad Hoc Network.

[1]Gaurav Sharma,[2]Manoj Kumar Singh
[1, 2] Department of Computer Science & Engineering
[1,2]Shri Shankaracharya Engineering College, Bhilai, (C.G.)

Abstract— **Wireless ad hoc is a collection of multiple nodes with wireless infrastructure and networking potential that help to each other for data transmission in ad hoc network. Nodes are also capable to move in the entire network due to movable property of wireless ad hoc network. Due to the mobility in the network area we called it a wireless Mobile ad hoc network. Now a day Mobile ad hoc network is one of the famous technologies in the area of the data communication. By using ad hoc network, data collection and data transmission is done very easily and frequently, but in this network, security and errors play a major role. Due to movable property there are many challenges occurred in wireless networks which harmful for entire network. In this paper we are study about various faults and problems and how we detect all these and increase the network efficiency and performance.**

Keywords — Wireless ad hoc network, Mobile ad hoc network, Network Lifetime, Security.

I. INTRODUCTION

The mobile ad-hoc networks are the collection of movable node, all the nodes are free to move anywhere in the network due to that ad hoc network is a temporary network as well as there is no centralized administration. In Wireless ad hoc network nodes are working as a host as well as router for transmitting and receiving data packets from other nodes in the network. The nodes are capable to establish dynamic route for data communication. There are multi path for data communication. In Wireless ad hoc network there are multiple nodes together in a network is means more devices are used for communication, due to that security and many fault are occurred. Reliability is one of the major challenges for Wireless ad hoc network. In the absence of a network, wireless ad hoc networks accomplish for end-to-end communications in a successful and efficient way. In wireless ad hoc network if a node want to transmit their data packet in the network then first he will send route request in the network, if the node received route replay the network established and then the node transmit their data packet.

1. Types of wireless ad hoc Network

The self-sustaining, self-configuration characteristic of ad hoc networks makes them very valuable in all situations such as natural disasters, emergency Services, military operations, Flood Management, or rapidly convey information between two nodes. The types of ad hoc networks are as follows:

a. **Wireless sensor networks:** A WSN is a collection of Sensor nodes having limited energy and they are useful for traffic control, weather control, position detecting etc.

b. **Mobile ad hoc networks :** A mobile ad hoc network (MANET) is a self configure network of multiple mobile nodes which or Connected with each other and capable to send or receive data as well as free for moving to entire network.

c. **Wireless mesh networks :** A wireless mesh network (WMN) is a communications network of radio nodes prearranged in a mesh topology.

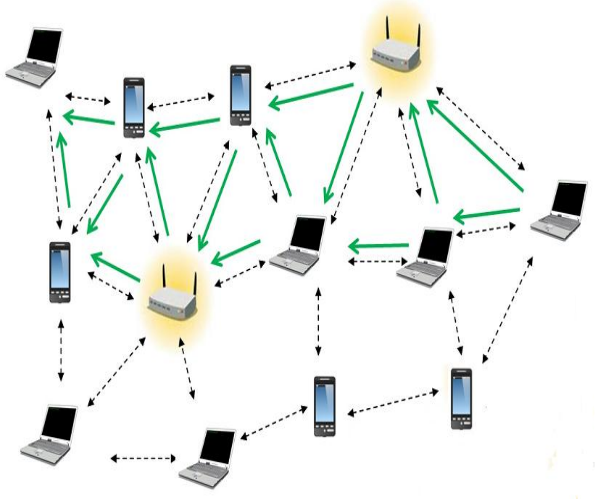

Figure 1: Wireless ad hoc Network.

2. Application of Wireless ad hoc Network

We can use the wireless ad hoc Network to many field, there are few field where we can use wireless ad hoc network.

a. **Battle field:** An ad hoc network helps to provide quick information of movements during war in battleground.

b. **Spot monitor:** Spot monitor one of the most important application in which we will easily and frequently know about all the information about particular Location.

c. **Industry sector:** Ad hoc network is widely used for commercial applications. Ad hoc network can also be used in emergency situation such as disaster relief.

d. **Earthquake detection:** By the help of the wireless network we can easily and quick message to all, about earthquake.

e. **Disaster Management:** Wireless ad hoc network are also helpful during natural disasters.

f. **Location Tracking:** By help of dynamic wireless ad hoc network we can track any node easily.

3. Characteristics of Wireless ad hoc network

a. **Flexibility:** In wireless ad hoc network nodes are flexible to move anywhere and node can adapt any topology easily. Node are capable to self configure and eliminate from the network.

b. **Data Communication:** In the wireless ad hoc network when we talked about the data collection and transmission then at the time of data collection we give attention in data collection mechanism, should be done smoothly and securely and transmit the data to the particular destination.

4. Security issues in DWSN

Security of wireless ad hoc network is one of the major challenges. There are many types of attacks are as follows:

a. **Node Authentication:** It is one of the major issues in wireless ad hoc network. In all connected nodes there is any node not working as a malicious node means any node can't modified data pocket or can't change the data packet.

b. **Data Privacy:** Is one of the most important for any type of the wireless network. It ensures that the data packet is highly secured and can be received by receiver only.

c. **Data Consistency:** Privacy in the data in the wireless ad hoc network ensures that the data has not been stolen by any node it means data are error free and transmit through reliability network path only.

d. **Data Replication:** In the data it should be ensured that we can't send or receive same data packet multiple times because it will effect time, traffic and accuracy also.

II. EVOLUTION

In 2001, I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci studied about wireless sensor networks in which they describe the concept of sensor networks which has been made viable by the convergence of microelectro- mechanical systems technology, wireless communications and digital electronics. First, the sensing tasks and the potential sensor network applications are explored, and a review of factors influencing the design of sensor networks is provided. Then, the communication architecture for sensor networks is outlined, and the algorithms and protocols developed for each layer in the literature are explored. Open research issues for the realization of sensor networks are also discussed [1].

In 2002, Hongmei Deng, Wei Li, and Dharma P. Agrawal, Routing Security in Wireless Ad Hoc Networks in which a mobile ad hoc network consists of a collection of wireless mobile nodes that are capable of communicating with each other without the use of a network infrastructure or any centralized administration. MANET is an emerging research area with practical applications. However, wireless MANET is particularly vulnerable due to its fundamental characteristics, such as open medium, dynamic topology, distributed cooperation, and constrained capability. Routing plays an important role in the security of the entire network. In general, routing security in wireless MANETs appears to be a problem that is not trivial to solve. In this article they study the routing security issues of MANETs, and analyze in detail one type of attack — the "black hole" problem — that can easily be employed against the MANETs. They also propose a solution for the black hole problem for ad hoc on-demand distance vector routing protocol [2].

In 2004, Raquel A.F. Mini, Antonio A.F. Loureiro, Badri Nath develops The distinctive design characteristic of a wireless sensor network: the energy map in which The key challenge in the design of a wireless sensor network is maximizing its lifetime. This is a fundamental problem and new protocol engineering principles needing to be established in order to achieve this goal. The information about the amount of available energy in each part of the network is called the energy map and can be useful to increase the lifetime of the network. They propose using the energy map as a protocol engineering principle for this kind of network. They argue that an energy map can be the basis for the entire design trajectory including all functionalities to be included in a wireless sensor network. Furthermore, They show how to construct an energy map using both probabilistic and statistical predictions-based approaches. Simulation results compare the performance of these approaches with a naive one in which no prediction is used. The experiments performed as an energy dissipation model that They have proposed to simulate the behavior of a sensor node in terms of energy consumption. The results show that prediction-based approaches outperform the nave in a variety of parameters [3].

In 2005, Daniele Puccinelli and Martin Haenggi studied about Wireless Sensor Networks: Applications and Challenges of Ubiquitous Sensing in which Sensor networks offer a powerful combination of distributed sensing, computing and communication. They lend themselves to countless applications and, at the same time, offer numerous challenges due to their peculiarities, primary the stringent energy constraints to which sensing nodes are typically subjected. The distinguishing traits of sensor networks have a direct impact on the hardware design of the nodes at at least four levels: power source, processor, communication hardware, and sensors. Various hardware platforms have already been designed to test the many ideas spawned by the research community and to implement applications to virtually all fields of science and technology. They are convinced that CAS will be able to provide a substantial contribution to the development of this exciting field [4].

In 2006 Yong WangGarhan AtteburyByrav Ramamurthy present a survey on security issues in WSNs First they outline the constraints, security requirements, and attacks with their corresponding countermeasures in WSNs. Then they present a holistic view of security issues. These issues are classified into five categories: cryptography, key management, secure routing, secure data aggregation, and intrusion detection. Along the way they highlight the advantages and disadvantages of various WSN security protocols and further compare and evaluate these protocols based on each of these five categories. They also point out the open research issues in each Subarea and conclude with possible future research directions on security in WSNs [5].

In 2007 Prabhudutta Mohanty, Sangram Panigrahi Nityananda Sarma, Siddhartha Sankar Satapathy they explored explored general security threats in wireless sensor network and made an extensive study to categorize available data gathering protocols and analyze possible security threats on them. [6].

In 2008 Luis E. Palafox , J. Antonio Garcia-Macias they present the growing challenges related to security in wireless sensor networks. They show possible attack scenarios and evidence the easiness of perpetrating several types of attacks due to the extreme resource limitations that wireless sensor networks are subjected to. Nevertheless, they show that security is a feasible goal in this resource-limited environment; to prove that security is possible they Survey several proposed sensor network security protocols targeted to different layers in the protocol stack. The work surveyed in their chapter enables several protection mechanisms vs well documented network attacks. Finally, they summarize the work that has been done in the area and present a series of ongoing challenges for future work [7].

In 2008 Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz deals with some security issues over wireless sensor networks (WSNs). A survey of recent trends in general security requirements, typical security threats, intrusion detection system, key distribution schemes and target localization is presented. In order to facilitate applications that require packet delivery from one or more senders to multiple receivers, provisioning security in group communications is pointed out as a critical and challenging goal. Presented issues are crucial for future implementation of WSN [8].

In 2009, Peng Jiang, A New Method for Node Fault Detection in Wireless Sensor Networks in which Wireless sensor networks (WSNs) are an important tool for monitoring distributed remote environments. As one of the key technologies involved in WSNs, node fault detection is indispensable in most WSN applications. It is well known that the distributed fault detection (DFD) scheme checks out the failed nodes by exchanging data and mutually testing among neighbor nodes in this network., but the fault detection accuracy of a DFD scheme would decrease rapidly when the number of neighbor nodes to be diagnosed is small and the node’s failure ratio is high. In this paper, an improved DFD scheme is proposed by defining new detection criteria. Simulation results demonstrate that The improved DFD scheme performs well in the above situation and can increase the fault detection accuracy greatly [9].

In 2011, Abolfazl Akbari, Arash Dana, Ahmad Khademzadeh and Neda Beikmahdavi Study about Fault Detection and Recovery in Wireless Sensor Network Using Clustering in which Some WSN by a lot of immobile node and with the limited energy and without further charge of energy. Whereas extension of many sensor nodes and their operation. Hence it is normal. Inactive nodes miss their communication in network, hence split the network. For avoidance split of network, they proposed a fault recovery corrupted node and Self Healing is necessary. In this Thesis, they design techniques to maintain the cluster structure in the event of failures caused by energy-drained nodes. Initially, node with the maximum residual energy in a cluster becomes cluster heed and node with the second maximum residual energy becomes secondary cluster heed. Later on, selection of cluster heed and secondary cluster heed will be based on available residual energy. They use Matlab software as simulation platform quantities like, energy consumption at cluster and number of clusters is computed in evaluation of proposed algorithm. Eventually they evaluated and compare this proposed method against previous method and they demonstrate our model is better optimization than other method such as venkata raman, in energy consumption rate [10].

In 2012, Seo Hyun Oh, Chan O. Hong, Yoon-Hwa Choi studies about A Malicious and Malfunctioning Node Detection Scheme for Wireless Sensor Networks in which Wireless sensor networks are often used to monitor physical and environmental conditions in various regions where human access is limited. Due to limited resources and deployment in hostile environment, they are vulnerable to faults and malicious attacks. The sensor nodes affected or compromised can send erroneous data or misleading reports to base station. Hence identifying malicious and faulty nodes in an accurate and timely manner is important to provide reliable functioning of the networks. In this paper, they present a malicious and malfunctioning node detection scheme using dual-weighted trust evaluation in a hierarchical sensor network. Malicious nodes are effectively detected in the presence of natural faults and noise without sacrificing fault-free nodes. Simulation results show that the proposed scheme outperforms some existing schemes in terms of mis-detection rate and event detection accuracy, while maintaining comparable performance in malicious node detection rate and false alarm rate [11].

In 2013, Er. Saurabh and Dr. Rinkle Rani Aggarwal, A Review of Fault Detection Techniques for Wireless Sensor Networks in which Today wireless sensor networks (WSNs) emerge as a revolution in all aspects of our life. WSNs have unique specifications of themselves that describe them different from other networks. Fault tolerance is one of the most significant of many challenges in these networks. Five key features need to be considered when developing WSN solutions: scalability, security, reliability, self-healing and robustness. In this paper the main objective is to provide a comparative study of fault detection techniques using different approaches. Sensor nodes have various energy and computational constraints. To provide quality service by coverage protocols, there arises a need for developing protocols to provide fault tolerance, event reporting, and maintain energy efficiency [12].

In 2014, B Victoria Jancee, S Radha and Nandita Das analysis of non- binary fault tolerant event detection In wireless sensor networks, A distributed non-binary fault tolerant event detection technique is proposed for a wireless sensor network (WSN) consisting of a large number of sensors. The sensor nodes may be faulty due to harsh environment and manufacturing reasons. In the existing works on event detection, the detection of event is decided by only one threshold level. The objective of this paper is to extend the fault recognition and correction algorithm for non-binary event detection. The analysis presented here takes into account both the symmetric and non-symmetric error in a straightforward manner. In addition, simulation is done for Symmetric error and 75 percentages of the errors can be corrected. The theoretical analysis shows that more Than 95 percentage of symmetric errors can be corrected and almost 92 percentage of non-symmetric errors An be corrected (for k=2, i.e. Half of the neighbors give correct decision), even when as many as 10 Percentage of the sensor nodes are faulty [13].

In 2015, Nagalgaonkar Pramod, Dhanraj Biradar and Gaikwad Ranjit Sharnappa, Review on Fault detection and Recovery in WSN in which In recent due to advance research, applications of wireless sensor networks (WSNs) have been increased in different applications. In wireless sensor networks, sensor nodes are operated in unattended mode. In WSNs, it is essential to maintaining the communication between sensor nodes for all the time. Failure of the node affects the consistency of the network. One of the design challenge efficient fault management solutions to recover network from unanticipated failures. In this paper, they discuss different types of faults, detections techniques and fault recovery algorithms [14].

III. CONCLUSION AND FURTHER DEVELOPMENT

In present scenario wireless technology are growing day by day due to highly demanded by entire world, it is very useful for fast and effective communication medium for any field. The importance of the wireless ad hoc network in our day to day life has been discussed in these papers, we are also discussed about the various issues of the wireless network and we have discussed the advantages and problems of these technologies.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci "A survey on sensor networks", IEEE Communications Magazine, 40(8), pp. 102–114, 2002.

[2] Hongmei Deng, Wei Li, and Dharma P. Agrawal, Routing Security in Wireless Ad Hoc Networks, IEEE Communications Magazine, Pp: 70-75, October 2002.

[3] Raquel A.F. Mini, Antonio A.F. Loureiro, Badri Nath, "The distinctive design characteristic of a wireless sensor network: the energy map" , Computer Communications 27 (2004) 935–945.

[4] Daniele Puccinelli and Martin Haenggi, "Wireless Sensor Networks: Applications and Challenges of Ubiquitous Sensing ",IEEE circuits and systems magazine third quarter 2005.

[5] Yong WangGarhan AtteburyByrav Ramamurthy, "A Survey of Security Issues In Wireless Sensor Networks" , CSE Journal Articles. Paper 84. http://digitalcommons.unl.edu/csearticles/84.

[6] Prabhudutta Mohanty, Sangram Panigrahi Nityananda Sarma, Siddhartha Sankar Satapathy, "Security issues in wireless sensor network data gathering protocols: a survey", Journal of Theoretical and Applied Information Technology.

[7] Luis E. Palafox , J. Antonio Garcia-Macias , "Security in Wireless Sensor Networks", 2008, IGI Global.

[8] Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz, "Security Issues in Wireless Sensor Networks", International journal of communications Issue 1, Volume 2, 2008.

[9] Peng Jiang, "A New Method for Node Fault Detection in Wireless Sensor Networks", www.mdpi.com/journal/sensors, Pp: 1282-1294, vol. 9, 2009.

[10] In 2011, Abolfazl Akbari, Arash Dana, Ahmad Khademzadeh and Neda Beikmahdavi Study about Fault Detection and Recovery in Wireless Sensor Network Using Clustering, International Journal of Wireless & Mobile Networks (IJWMN), Pp: 130-138, Vol. 3, No. 1, February 2011.

[11] Seo Hyun Oh, Chan O. Hong, Yoon-Hwa Choi, "A Malicious and Malfunctioning Node Detection Scheme for Wireless Sensor Networks" http://www.SciRP.org/journal/wsn, Pp 84-90, vol. 4, 2012.

[12] Er. Saurabh and Dr. Rinkle Rani Aggarwal, A Review of Fault Detection Techniques for Wireless Sensor Networks, IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 4, No 1, July 2013.

[13] B Victoria Jancee, S Radha and Nandita Das, “analysis of non-binary fault tolerant event detection In wireless sensor networks”, International journal on smart sensing and intelligent systems vol. 7, no. 3, september 2014.

[14] Nagalgaonkar Pramod, Dhanraj Biradar and Gaikwad Ranjit Sharnappa, “Review on Fault detection and Recovery in WSN”, IJARCSSE, Pp: 479-483, Volume 5, Issue 8, August 2015.

[15] F. Stajano and R. Anderson, “The resurrecting duckling: Security issues for ad-hoc wireless networks,” in 7th International Workshop on Security Protocols, Cambridge, UK, Apr. 1999.

Gaurav Sharma , B.E., M.Tech. Scholar in E-Security from Shri Shankaracharya Engineering College, Bhilai, India. Research areas are Wireless ad hoc Network, wireless sensor network & its enhancement.

Manoj Kumar Singh, Asst. Professor in Dept. of Computer Science & Engineering at Shri Shankaracharya Engineering College, Bhilai. India. Having Wide experience in the field of teaching. Research areas are Wireless ad hoc network, Wireless Sensor Network, its Enhancements, and His research work has been published in many national and international journals.