A REVIEW PAPER ON ENERGY EFFICIENT TECHNIQUE OF WIRELESS SENSOR NETWORKS

Heena[1], Simranjit kaur [2]

[1]M.Tech student, Dept. of Electronics & Communication Engineering, Sri Sai College of Engineering and Technology(Badhani), Punjab,India
[2]Assistant professor, Dept. of electronics & Communication Engineering, Sri Sai College of Engineering and Technology(Badhani), Punjab,India

---

Abstract - *The wireless sensor networks is the type of network in which sensor nodes sense the environmental conditions and pass the sensed information to the base station. The network is deployed on the far places and size of the sensor nodes are very small due to battery power of the nodes is limited. Due to far deployment of the network, it is very difficult to recharge or replace battery of the nodes. The Mobile adhoc network is also decentralized type of network in which no central controller is present due to which security attacks are possible in the network In the recent times, various techniques has been proposed which reduce energy consumption of the network. In this paper, various energy efficient techniques of wireless sensor networks is been reviewed and discussed and various security techniques for mobile adhoc network are discussed*

***Key Words*: WSN,Leach,Clustering**

1. INTRODUCTION

There are large numbers of applications of wireless sensor networks due to their various properties. There are a lot of benefits of these types of networks which are the reason of their increasing demands. Wireless sensor networks consist of sensor nodes which are small in size, cheap, and also have self-contained battery powered systems [1]. The input received from adjacent sensor is processed by the sensor nodes. Further, the result is transmitted to transit network within the network. The WSNs are used to monitor the surroundings of area in which they are placed and gather the important information according to the physical parameters such as pressure, temperature, etc. They are dispersed type of networks which have lightweight, small sensor nodes. There is limited power, memory as well as computational capacity in each sensor node [2]. There are various resource constraints such as limited amount of energy, low bandwidth, storage and limited processing present within each node of a WSN. There a certain design constraints as well, which are completely application dependent and are also based on the monitored environment. It completely depends on the surroundings to define the deployment scheme, network topology as well as the size determination of the network [3]. There are few nodes required for the internal environments where as a large number of nodes are required for the purpose of external environments. The sensor nodes of a network can communicate with each other or also with the external base stations of a network. The important part of a sensor node is the battery which is very important as it affects the network's lifetime directly [4]. There are various energy-optimized solutions proposed at various levels of the system for improving the battery consumptions of sensor nodes. The communication amongst the sensor nodes is done with the help of radio signals. There are various applications which use WSN and also include non-conventional paradigms which help in protocol design which involve various constraints. For the purpose of path determination from the source to the destination node, the routing method is utilized. There are various categories according to which the routing protocols are classified. The reactive and proactive are one of the types of classifications of routing protocols. Before the demand of a routing traffic the routing paths as well as the states are provided in the network using the proactive routing protocols [5]. The protocols which trigger the routing actions when the data is to be sent to various nodes is known as the reactive routing protocol. On the basis of their initiation which is source-initiation (Src-initiated) or destination initiation (Dst-initiated) the routing protocols are classified. On the demand of source node, the source-initiated protocol provides the routing path which begins from the source node. The routing path is initiated from the destination node in case of destination-initiated protocol [6]. On the basis of the sensor network architecture also the routing protocols are classified which are the homogeneous nodes as well as the heterogeneous nodes. The protocols can also be here classified further on the basis of the topology they use which is mainly the flat topology or the hierarchical topology. The protocols in which the sensor nodes are addressed using the locations are known as the location-based protocol. For the purpose of calculating the distance between two specific nodes, the location information of nodes is required by the network. This also helps in estimating the energy consumption of the node [7]. The Geographic Adaptive Fidelity (GAF) is an energy-aware routing protocol which is used for the purpose of energy conservation mainly.

1.1 Attacks in Adhoc networks

1.1.1. Black hole Attack: In this attack, an attacker advertises a zero metric for all destinations bringing about all nodes around it to route packets towards it. A malicious hub sends fake routing information, asserting that it has an optimum route and causes other good nodes to route data packets through the malicious one. A malicious hub drops all packets that it receives instead of normally forwarding those packets. An attacker listen the solicitations in a flooding based convention [3].

1.1.2. Wormhole Attack: In a wormhole attack, an attacker receives packets at one point in the network, "tunnels" them to another point in the network, and after that replays them into the network starting there. Routing can be disrupted when routing control message are tunneled. This tunnel between two colluding attacks is known as a wormhole. In DSR, AODV this attack could prevent discovery of any routes and may make a wormhole even for parcel not address to itself as a result of broadcasting. Wormholes are hard to detect on the grounds that the path that is utilized to pass on information is typically not part of the actual network. Wormholes are dangerous on the grounds that they can do damage without even knowing the network.

1.1.3. Byzantine attack: A compromised with set of intermediate, or intermediate nodes that working alone inside network do attacks, for example, making routing loops, forwarding packets through non - ideal paths or specifically dropping packets which brings about disruption or degradation of routing services inside the network [4].

1.1.4.Rushing attack: Two colluded attackers utilize the tunnel procedure to shape a wormhole. On the off chance that a fast transmission path (e.g. a dedicated channel shared by attackers) exists between the two closures of the wormhole, the tunneled packets can propagate faster than those through a normal multi-hop route.

1.1.5. Traffic Monitoring: It can be developed to identify the communication parties and functionality which could give information to launch additionally attacks .It is not particular to MANET, different wireless network, for example, cellular, satellite and WLAN likewise suffer from these potential vulnerabilities [5].

1.1.6. Eavesdropping: The term eavesdrops implies overhearing without expending any expending any additional effort. In this intercepting and reading and conversation of message by unintended beneficiary occur. Portable host in versatile specially appointed network shares a wireless medium. Majorities of wireless communication utilize RF range and communicate by nature. Message transmitted can be eavesdropped and fake message can be infused into network.

1.1.7. Denial of service attack: Denial of service attacks are gone for complete disruption of routing information and accordingly the whole operation of specially appointed network [6].

1.1.8. Gray-hole attack: This attack is otherwise called routing misbehavior attack which leads to dropping of messages. Dark hole attack has two phases. In the main phase the hub advertise itself as having a valid route to destination while in second phase, nodes drops captured packets with a specific probability.

2. LITERATURE REVIEW

Sarab F. Al Rubeaai, et.al (2015) proposed in this paper, [8], a novel 3D real-time geographical routing protocol (3DRTGP) for WSNs. The numbers of forwarding nodes within the network are controlled by this protocol. This is done by limiting the forwarding to a unique packet forwarding region (PFR). Under the different network densities and traffic load conditions, the performance of this protocol is evaluated by performing certain simulations. The needs of real-time applications are fulfilled with the help of the network tuning parameters that are provided by the results. Within the 3D deployments, the Void Node Problem (VNP) is solved by the 3DRTGP heuristically. Even when there is no network partitioning, the 3DRTGP helps is resolving the VNP. With respect to the end-t-end delay and miss ration parameters, this protocol has shown better performance than the other routing protocols.

Adnan Ahmed, et.al (2015) proposed in this paper [9], a Trust and Energy aware Routing Protocol (TERP). For the purpose of detection and isolation of malicious nodes, this distributed trust model is used. A composite routing function is included in TERP which provides trust, residual-energy as well as hop counts of neighboring nodes which will further help in taking the routing decisions. The energy consumption amongst the trusted nodes is balanced when the routing data utilizes the shorter paths with the help of this routing strategy. According to the simulation results achieved there is a reduction in the energy consumption, enhancement in the throughput as well as lifetime of the network when the TERP is used as compared to other protocols.

Gurbinder Singh Brar, et.al (2016) proposed in this paper [10], a directional transmission based energy aware routing protocol named as PDORP is proposed. The properties of Power Efficient Gathering Sensor Information System (PEGASIS) and DSR routing protocols are combined in this newly proposed protocol. A comparison in between the hybridization approach and the newly proposed approach is given. The performance analysis shows that there is a reduction in the bit error rate, delay and energy consumption within the network. There is also an improvement in the throughput which results in providing better QoS and which further results in increasing the lifetime of the network. For the purpose of evaluating and comparing the performance of both the routing protocols, the computation model is used.

Guangjie Han, et.al (2015) proposed in this paper [11], that for various underwater applications, the underwater WSNs (UWSNs) are being used a lot. For the purpose of data transmission and other real-time applications, the energy efficient routing protocol is very important. There are some special characteristics of UWSNs which include dynamic structure, high energy consumption, as well as high latency. These properties have made it difficult to build certain routing protocols for this network. The already existing routing protocols are to be studied in this paper and their performances are to be compared with respect to each other. The routing protocols are classified into two categories on the basis of the route decision maker they use. The results have shown that there are still many enhancements to be made in this technology. In the future work, new technologies are to be evolved to provide better results.

Lein Harn, et.al (2016) proposed in this paper [12], a novel design of secure end-to-end data communication. A newly designed group key pre-distribution method is proposed here which provides a unique group key which is also known as the path key This key is used for protecting the transmitted data which is present in the complete routing path. There are many pairwise shared keys used in repeated form for the purpose of encryption and decryption in the network. To avoid repetitive use, the unique end-to-end path key is proposed here which protects the data which is transmitted across the network. The sensors can be authenticated using this protocol for the purpose of establishing path as well as the path key. Through this protocol, the time which is needed to process data through intermediate nodes is reduced, which is an important advantage here.

JingJing Yan, et.al (2016) proposed in this paper [13], that it is very important to increase the lifetime of a network due to the limited battery available in the sensors. For this purpose the energy-efficient routing techniques are very widely used. The routing protocols that are already proposed are studied and classified into homogeneous and heterogeneous categories as per their orientations. Also the static and mobile protocols are classified accordingly. The characteristic properties, limitation as well as applications are also discussed. The various issues which are related to the energy-efficiency of the routing protocol designs are enlisted here. The mobile WSNs provide more enhanced results as compared to the static WSNs which result in improvement in terms of energy efficiency, energy balance, and higher coverage. The implementations as well as the deployment costs increase however, in these types of networks.

Table -1: Routing Protocols of WSN

Author Name	Year	Description	Outcomes
Sarab F. Al Rubeaai, Mehmmood A. Abd, Brajendra K. Singh, Kemal E. Tepe	2015	In this paper, a novel 3D real-time geographical routing protocol (3DRTGP) for WSNs. The numbers of forwarding nodes within the network are controlled by this protocol.	With respect to the end-t-end delay and miss ration parameters, this protocol has shown better performance than the other routing protocols.
Adnan Ahmed, Kamalrulnizam Abu Bakar, Muhammad Ibrahim Channa, Khalid Haseeb and Abdul Waheed Khan,"	2015	A Trust and Energy aware Routing Protocol (TERP) for the purpose of detection and isolation of malicious nodes. The energy consumption amongst the trusted nodes is balanced when the routing data utilizes the shorter paths with the help of this routing strategy.	According to the simulation results achieved there is a reduction in the energy consumption, enhancement in the throughput as well as lifetime of the network when the TERP is used as compared to other protocols.
Gurbinder Singh Brar, Shalli Rani, Vinay Chopra, Rahul Malhotra, Houbing Song, Syed Hassan Ahmed	2016	A directional transmission based energy aware routing protocol named as PDORP is proposed. The properties of Power Efficient Gathering Sensor Information System (PEGASIS) and DSR routing protocols are combined in this newly proposed protocol.	There is also an improvement in the throughput which results in providing better QoS and which further results in increasing the lifetime of the network.
Guangjie Han, Jinfang Jiang, Na Bao, Liangtian Wan, and Mohsen Guizani	2015	For the purpose of data transmission and other real-time applications, the energy efficient routing protocol is very important. There are some special characteristics of UWSNs which include dynamic structure, high energy consumption, as well as high latency.	The results have shown that there are still many enhancements to be made in this technology. In the future work, new technologies are to be evolved to provide better results.

Lein Harn, Ching-Fang Hsu, Ou Ruan, and Mao-Yuan Zhang	2016	A novel design of secure end-to-end data communication is proposed. A newly designed group key pre-distribution method is proposed here which provides a unique group key which is also known as the path key.	Through this protocol, the time which is needed to process data through intermediate nodes is reduced, which is an important advantage here.
JingJing Yan, MengChu Zhou, and ZhiJun Ding	2016	The routing protocols that are already proposed are studied and classified into homogeneous and heterogeneous categories as per their orientations.	The mobile WSNs provide more enhanced results as compared to the static WSNs which result in improvement in terms of energy efficiency, energy balance, and higher coverage.

Table -2: Security Techniques for MANETs

Name	Year	Description	Outcomes
Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai	2015	A Dynamic Source Routing (DSR)-based routing mechanism is used in this paper to resolve these issues. It is known as the Cooperative Bait Detection Scheme (CBDS).	This technique inherits the advantages of both proactive and reactive defense architectures and the results achieved show that the outcomes vary according to the presence or absence of malicious nodes in the network.
Adnan Nadeem, and Michael P. Howarth	2013	A survey of various attacks is present in the paper and further the intrusion detection as well as protection mechanisms are reviewed.	The results evaluated show the properties of both of these techniques and their applications are defined accordingly. The further research areas are identified at the end.
Ming Yu, Mengchu Zhou	2009	An optimal routing algorithm along with the routing metric is also proposed in this paper which combines the node's trustworthiness and performance properties.	The advantages of the proposed attack detection and routing algorithm can be seen in the simulation results derived. The comparisons are made with some already known protocols to show the enhancements made in this work.
Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat	2012	A new lightweight scheme is proposed here, which helps in detecting the new identities of Sybil attackers. This is to be done without using the centralized trusted third party or any extra hardware like geographical positioning or directional antenna etc.	Many extensive simulations and real-world testbed experiments are presented and it is concluded this method detects the Sybil identities with good accuracy even when mobility is seen in the network.
Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, Nei Kato, Abbas Jamalipour	2007	In this paper, all the possible attacks are discussed in details and their state-of-the-art of security issues are discussed.	The routing attacks such as link spoofing and colluding misrelay attacks are studied well. Also, the ways to prevent or remove such attack from the network are proposed in the existing MANET protocols.
Yingbin Liang, H. Vincent Poor, and Lei Ying	2011	There are *n* number of legitimate mobile nodes and *m* number of malicious nodes in the MANET. Also the	The active attacks need to satisfy more stringent conditions on the number of malicious nodes than the

		delay constraint D is used for the transmission between the legitimate nodes.	passive attacks for achieving same throughput.
Ziming Zhao, Hongxin Hu, Gail-Joon Ahn, and Ruoyu Wu	2012	In this paper, to handle the various routing attacks in a systematic manner, a risk-aware response mechanism is proposed. This approach is based on the extended Dempster-Shafer mathematical theory of evidences.	This method introduces a notion which enlists the important factors required. The experiments achieved show the effectiveness of this proposed approach on the basis of certain performance metrics.

3. CONCLUSIONS

In this work, it is been concluded that wireless sensor network is the network in which security and energy consumption is the major issue . In the recent times, various techniques has been proposed to increase lifetime of the network. In this work, energy efficient techniques has been reviewed and discussed in terms of description and outcome The techniques which are proposed in the recent times to increase security of Adhoc networks are also discussed

REFERENCES

[1] G. Tolle, J. Polastre, R. Szewczyk, D. Culler, N. Turner, K. Tu, S. Burgess, T. Dawson, P. Buonadonna, D. Gay, andW. Hong, “A macroscope in the redwoods,” 2005, 3rd ACM SenSys, New York, NY, USA, pp. 51–63

[2] G. Werner-Allen, K. Lorincz, J. Johnson, J. Lees, and M. Welsh, USENIX Association, “Fidelity and yield in a volcano monitoring sensor network,” 2006, 7th OSDI, Berkeley, CA, USA, pp. 381–396

[3] M. Li and Y. Liu, “Underground coal mine monitoring with wireless sensor networks,” 2009, ACM Trans. Sen. Netw., vol. 5, pp. 10:1–10:29

[4] P. Vicaire, T. He,Q.Cao, T.Yan,G. Zhou, L.Gu, L. Luo, R. Stoleru, J. A. Stankovic, and T. F. Abdelzaher, “Achieving long-term surveillance in VigilNet,” 2009, ACM Trans. Sen. Netw., vol. 5, pp. 9:1–9:39

[5] N. Xu, S. Rangwala, K. K. Chintalapudi, D. Ganesan, A. Broad, R. Govindan, and D. Estrin, “A wireless sensor network for structural monitoring,” 2004, 2nd ACM SenSys, New York, NY, USA, pp. 13–24

[6] L. Liu, X. Zhang, and H. Ma, “Optimal node selection for target localization in wireless camera sensor networks,” 2010, IEEE Trans. Veh Technol., vol. 59, no. 7, pp. 3562–3576

[7] Y. Weng, W. Xiao, and L. Xie, “Sensor selection for parameterized random field estimation in wireless sensor networks,” 2011, J. Control Theory Appl., vol. 9, pp. 44–50

[8] Sarab F. Al Rubeaai, Mehmmood A. Abd, Brajendra K. Singh, Kemal E. Tepe,” 3D Real-Time Routing Protocol with Tunable Parameters for Wireless Sensor Networks”, 2015, IEEE Sensors Journal

[9] Adnan Ahmed, Kamalrulnizam Abu Bakar, Muhammad Ibrahim Channa, Khalid Haseeb and Abdul Waheed Khan,” TERP: A Trust and Energy Aware Routing Protocol for Wireless Sensor Network”, 2015, IEEE

[10] Gurbinder Singh Brar, Shalli Rani, Vinay Chopra, Rahul Malhotra, Houbing Song, Syed Hassan Ahmed,” Energy Efficient Direction Based PDORP Routing Protocol For WSN”, 2016, IEEE

[11] Guangjie Han, Jinfang Jiang, Na Bao, Liangtian Wan, and Mohsen Guizani,” Routing Protocols for Underwater Wireless Sensor Networks”, 2015, IEEE

[12] Lein Harn, Ching-Fang Hsu, Ou Ruan, and Mao-Yuan Zhang,” Novel Design of Secure End-to-End Routing Protocol in Wireless Sensor Networks”, 2016, IEEE SENSORS JOURNAL, Vol. 16, No. 6

[13] JingJing Yan, MengChu Zhou, and ZhiJun Ding,” Recent Advances in Energy-efficient Routing Protocols for Wireless Sensor Networks: A Review”, 2016, IEEE