International Journal of Electrical, Electronics and Computer Engineering **8**(1): 46-49(2019)

ISSN No. (Online): 2277-2626

A Review of Enhancing Energy Efficiency of Wireless Sensor Network

Niharika, Himanshu Yadav and Chetan Agrawal
Department of Computer Science Engineering,
RITS, Bhopal (Madhya Pradesh), INDIA

(Corresponding author: Niharika)
(Received 27 February 2019 Accepted 29 May, 2019)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Wireless Sensor Network (WSN) is known to be a highly resource constrained class of network where energy consumption is one of the prime concerns. In this research, a cross layer design methodology was adopted to design an energy efficient routing protocol entitled "Position Responsive Routing Protocol" (PRRP). PRRP is designed to minimize energy consumed in each node by, reducing the amount of time in which a sensor node is in an idle listening state and (2) reducing the average communication distance over the network. The performance of the proposed was critically evaluated in the context of network lifetime, throughput, and energy consumption of the network per individual basis and per data packet basis. The outcomes show a significant improvement in the WSN in terms of energy efficiency and the overall performance of WSN.

Keywords: Wireless Sensor Network, energy efficient, protocol, consumption.

I. INTRODUCTION

Wireless sensor technology is playing a vital role in many of the commercialized industrial automation processes and various other real life applications. It is particularly suitable for harsh environment applications where deploying of other network infrastructure is difficult and/or almost impossible such as in battlefield, in hazardous chemical plant, and in high thermal environment. It is not uncommon to see that most of the crucial surveillance and security applications also rely on sensor based applications. Sensors which are tiny in size and cheap in cost have the capabilities to be deployed in a range of applications as explained in . Essentially all sensor networks comprise some forms of sensing mechanism to collect data from an intended physical environment.

Recent advances in micro-electro-mechanical systems (MEMS) and wireless communications have highlighted the significance of WSNs as essential reporting devices. Indeed, sensor nodes in WSNs are deemed to be resource constrained in terms of energy, communication range, memory capacity and processing capability. WSNs include specifications and applications such as target tracking, environmental monitoring and battlefield applications. The main purpose of WSNs is to disseminate the information from the source to the sink in multi-hop scheme Network partitioning which is caused by the energy hole problem in WSNs and unbalanced energy consumption are regarded as critical challenges in WSNs and hence will affect the network lifetime of WSNs in routing protocols. Thus, prolonging network lifetime in WSNs has received significant consideration. In recent years, energy-efficient routing algorithms have been proposed to enhance the network lifetime of WSNs. In this section, we will review the literature on improving and prolonging WSNs' lifetime With the development of IoT(Internet of Things, IoT), wireless sensor networks have been widely used in environmental monitoring, smart home, industrial production, military and medical fields1. In present year, for the transmission of information computer network is widely used. The network is classified into two category namely wired and wireless network. Wired network has fixed infrastructure due to this it can send the information to the limited users and can handle only small amount of information. The wireless network overcome all these limitations of wired network because it has capability to form dynamic network due to this no. of users can increase or decrease and also able to transmit a larger amount of information. Mobile ad hoc networks (MANETs) are generally fashioned by an assembly of mobile nodes, which are interconnected using wireless links,[15] The resources of Wireless sensor node are limited especially in terms of computation and energy. Those nodes are often deployed in unmanned and complicated environments. WSNs are vulnerable to the attacks that include node capture, Sybil attack and black-hole etc. More and more researchers study to improve the network performance by effectively resist malicious nodes2 Wireless Sensor Networking is one of the most hopeful technologies that have wide range of applications ranging from home surveillance, military to Internet of Things (IoT). Although Wireless Sensor Networks (WSNs)[16] have attractive features like: less deployment cost and least attended network operation, the security of such networks is a big concern especially when such networks are deployed for critical applications.

A wireless sensor network (WSN) consists of a large scale of cheap microsensor nodes deployed in the monitoring area. These nodes are usually networked in a multihop fashion, to enable cooperation among nodes and real-time delivery of sensed data to the users [1]. Due to the limited resources of the computing power, battery, and communication capacity of sensor nodes in a large scale [2, 3], it is a challenge to prolong the lifetime and balance the energy consumption in a WSN [4]. One of the popular techniques to balance the energy consumption in the nodes and prolong the lifetime of the network is clustering [5]. The energy efficiency and the network lifetime of WSNs are extremely related to a self-organization and clustering mechanism, because of their benefits in these issues [6]. Clustering is a method to divide the nodes into several groups called clusters. Each cluster chooses a special node as a coordinator named the cluster head (CH). In this method, the nodes do not need to communicate with the sink node directly. Alternately, the CHs integrate the data collected in the cluster and transfer it to the sink node. As a consequence, the clustering leads to a significant reduction in the energy consumption in the network. This paper presents a routing protocol for WSN called an energy-balanced routing protocol (EBRP) for wireless sensor networks. The EBRP balances the energy consumption and prolongs the lifetime of the network. The sink node divides the network into K clusters by using a first round, the sink node calculates the chosen value of each node by FLS and chooses the CHs with the maximum value in each cluster. The CH records the energy and distance information of the cluster member nodes for calculating the chosen value. The CH of this round selects the node with the maximum value as a CH of the next round in each cluster. are acquired by the sink node for the current network deployment through a designed GA. We code the as chromosomes of individuals in GA while the Recent advances in development of Wireless Communication in Vehicular Adhoc Network (VANET) has provided emerging platform for industrialists and researchers. Vehicular adhoc networks are multihop networks with no fixed infrastructure. It comprises of moving vehicles communicating with each other. One of the main challenge in VANET is to route the data efficiently from source to destination. Designing an efficient routing protocol for VANET is tedious task. Also because of wireless medium it is vulnerable to several attacks. Since attacks mislead the network operations, security is mandatory for successful deployment of such technology. This survey paper gives brief overview of different routing protocols. Also attempt has been made to identify major security issues and challenges with different routing protocols. Wireless communication is ubiquitous because of its flexibility to adapt to different scenarios. Mobile Ad Hoc Networks (MANETS) is a term coined for the continuously varying network topology handheld mobiles devices.

Vehicular Ad Hoc Networks (VANETS) is one of its types. It deploys the concept of continuously varying vehicular motion. The nodes or vehicles as in VANETS can move around with no boundaries on their direction and speed. Vehicular adhoc network (VANET) involves vehicle to vehicle (V2V), vehicle to roadside (V2R) or vehicle to infrastructure (V2I) communication [1].VANET generally consist of On Board Unit (OBU) and Roadside Units (RSUs). OBUs enables short-range wireless adhoc network to be formed between vehicles. Each vehicle comprises of hardware unit for determining correct location information using GPS. Roadside Units (RSUs) are placed across the road for infrastructure communication. The number of RSU to be used depends upon the communication protocol. VANET provide assistance to vehicle drivers for communication and coordination among themselves in order to avoid any critical situation through Vehicle to Vehicle communication [2] e.g. road side accidents, traffic jams, speed control, free passage of emergency vehicles and unseen obstacles etc. Besides safety applications VANET also provide comfort applications to the road users. Due to the dynamic nature of nodes in VANET the routing of data packets is much complex.

Several factors like the type of the road, daytime, weather, traffic density and even the driver himself affect the movements of vehicles on a road. Hence, the network topology change frequently, and the routing protocol use has to adapt itself to these instantaneous changes continuously. Intelligent Transportation System (ITS) In Intelligent Transportation Systems (ITS) [3], each vehicle broadcast the information to the vehicular network transportation agency, which then uses this information to ensure safe and free-flow of traffic. The possible communication configurations in ITS are inter-vehicle, vehicle to roadside, and routing-based communications [4] all this configurations requires precise and up-to-date surrounding information. Inter-vehicle communication support multi-hop multicast/broadcast over a multiple hops to a group of receivers. ITS is generally concerned with the activity on the road ahead and not on road behind. Naïve broadcasting and intelligent broadcasting [4] are the two message forwarding methods used in inter-vehicle communications. Fig. (1) shows inter-vehicle communication.

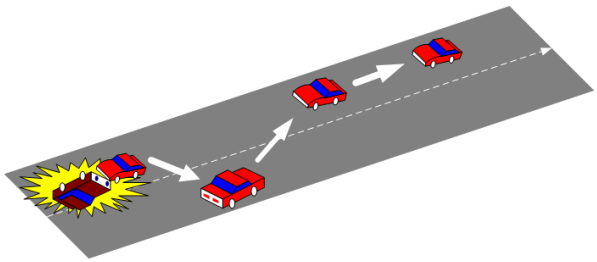

Fig. 1. Inter-vehicle communication.

Naive broadcasting believes on the periodic broadcasting of message, if the message is from a vehicle behind it then vehicle ignores the message, but if the message comes from a vehicle ahead then the receiving vehicle sends its own broadcast message to vehicle behind it. Due to the large number of messages, probability of message collision increases which lowers the message delivery rate and increases its time of delivery. This problem is overcome using intelligent broadcasting. It uses acknowledgment address limiting the number of messages broadcast for emergency events only.

A. Vehicle-to-roadside communication

In this type of communication, vehicle communication is done using single hop broadcasting method. This type of configuration provides ample amount of bandwidth link between communicating parties. In vehicle to roadside communication the maximum load for proper communication is given to the road side unit, it controls the speed of vehicle when it observes that a vehicle violates the desired speed limit, it delivers a broadcast message in the form of an auditory or visual warning, requesting the driver to reduce speed. Vehicle-to-roadside communication is shown in Fig. 2. Here RSU sends broadcast messages to all the equipped vehicles.

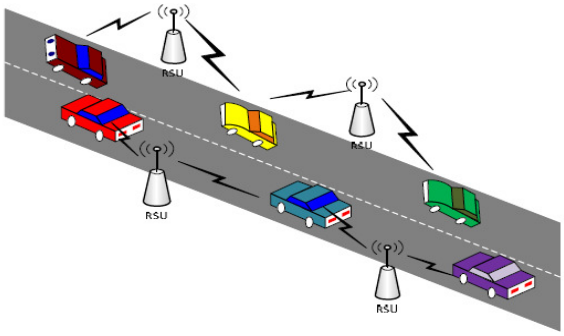

Fig. 2. Vehicle-to-Roadside Unit Communication.

B. Routing-based communication

Multi-hop unicast method is used in routing-based communication configuration. While sending the message, the vehicle sends message using multi-hop fashion until it reaches to the desired vehicle. Receiving vehicle then sends a unicast message to the requested vehicle. Fig. 3. shows the routing-based communication in VANET. Here vehicle A sends message to vehicle C using routing protocols.

Hybrid architecture in Fig. 4 is a combination of infrastructure network and ad hoc network. This is also a possible solution for VANET. The hybrid architecture though can provide better coverage, arises a new problem such as the seamless transition of the communication among different wireless systems.

VANETs can be distinguished from other kind of adhoc networks as follows:

Highly dynamic topology: Due to high speed of movement between vehicles, the topology of VANETs is always changing.

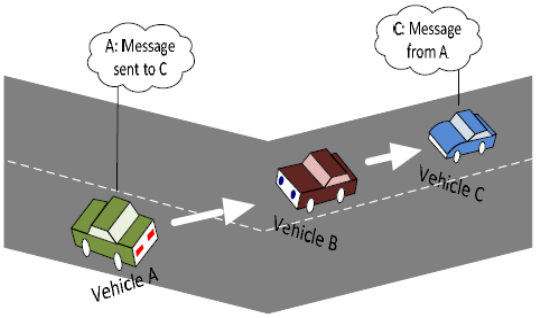

Fig. 3. Routing-based Communication.

Frequently disconnected network: Due to the same reason, the connectivity of the VANETs could also be changed frequently. Especially when the vehicle density is low, it has higher probability that the network is disconnected. However, a possible solution is to predeploy several relay nodes or access points along the road to keep the connectivity.

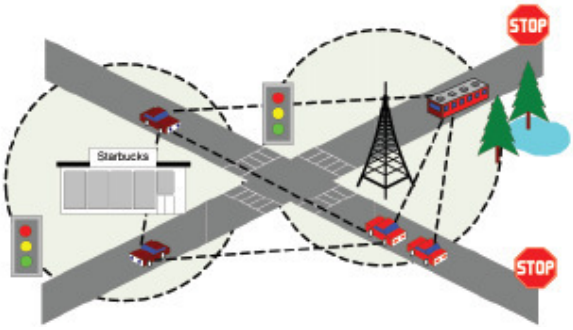

Fig. 4. Hybrid Network Architecture.

Mobility modeling and predication: Due to highly mobile node movement and dynamic topology, mobility model and predication play an important role in network protocol design for VANETs. Moreover, vehicular nodes are usually constrained by pre-built highways, roads, and streets, so on giving the speed and the street map the future position of the vehicle can be predicted.

Geographical type of communication: The VANETs often have a new type of communication that addresses geographical areas where packet needs to be forwarded in safety driving applications).

Various communication environments: VANETs are usually operated in two typical communication environments they are highway traffic scenarios and city traffic scenarios**.** In highway traffic scenarios, the environment is relatively simple and straightforward (e.g., constrained one-dimensional movement), while in city conditions it becomes much more complex.

The streets in a city are often separated by buildings, trees, and other unstated obstacles. Therefore, there isn't always a direct line of communications in the direction of intended data communication.

Sufficient energy and storage: A common characteristic of nodes in VANETs is that nodes have ample energy and computing power (including both storage and processing), here nodes are cars instead of small handheld devices.

Hard delay constraints: In some VANETs applications, the network does not require high data rates but has hard delay constraints. For example, in an automatic highway system, when brake event happens, the message should be transferred and arrived in a certain time to avoid carcrash. In this kind of applications, instead of average delay, the maximum delay will be crucial. Routing protocols [10-12] are the basic building block for efficient communication in any type of network. The goal of routing protocols is to select best path with least time and least expensive route. The routing operation involves finding the best route from source to destination and vice-versa. This is done in two basic ways via source routing or hop by hop routing. It is a challenge to the researchers to develop routing protocols for highly dynamic topology like VANET.

II. CONCLUSION

In this paper various aspect of VANET like its environment, standards and network architecture has been discussed; furthermore various characteristics of VANET have been listed which distinguished it from other networks like MANET, Cellular, and WSN. Routing is an important component which used for more prominent and convenient communication. This paper includes detailed working and designing of various VANET routing protocols, finally various attacks in VANET have been classified depending on the availability, authentication, confidentiality, privacy, non repudiation and data trust. It has been observed that the classification helps to deal with different types of attack on routing protocols in VANET. Since attack creates a more severe condition, it is necessary to analyze the effect of attack on routing which makes more secure vehicular environment.

REFERENCES

[1]. Kawashima, Hironao. (2017). "Japanese perspective of driver information systems."Transportation **17**, no. 3, 263-284. 2017.

[2]. Harsch, Charles, Andreas Festag, and Panos Papadimitratos. (2007). "Secure position-based routing for VANETs." In Vehicular Technology Conference, 2007. VTC-IEEE 66th, pp. 26-30. IEEE, 2007.

[3]. Sun, Jinyuan, Chi Zhang, and Yuguang Fang (2007). "An idbased framework achieving privacy and non-repudiation in vehicular ad hoc networks." In Military Communications Conference, 2007.

[4]. Zeadally, Sherali, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, and Aamir Hassan (2010). "Vehicular ad hoc networks (VANETs): status, results, and challenges." *Telecommunication Systems (2010):* 1-25.

[5]. Yin, Jijun, Tamer El Batt, Gavin Yeung, Bo Ryu, Stephen Habermas, Hariharan Krishnan, and Timothy Talty. (2004). "Performance evaluation of safety applications over DSRC vehicular ad hoc networks." In Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks, pp. 1-9. ACM, 2004.

[6]. Guo, Jinhua and Nathan Balon. (2006). "Vehicular Ad Hoc and Dedicated Short-Range Communication." Book Chapter. Available at: http://www. nathanbalon. com/project/cis95 (2006).

[7]. Stephan Eichler, (2007). "Performance Evaluation of the IEEE 802.11p WAVE Communication Standard", *Proceedings of Vehicular Technology Conference,* 2007, 2199-2203.

[8]. Jiang, Daniel, and Luca Delgrossi. "IEEE 802.11 p: Towards an international standard for wireless access in vehicular environments". In Vehicular Technology , 2008. VTC Spring 2008. IEEE, pp. 2036. IEEE, 2008.

[9]. IEEE (July 2007), "IEEE P802.11p/D3.0, Draft Amendment for Wireless Access in Vehicular Environment (WAVE)".

[10]. Watfa, Mohamed. Advances in Vehicular Ad-Hoc Networks: Developments and Challenges. *Information Science Reference, 2010.*

[11]. Paul, Bijan, Md Ibrahim, Md Bikas, and Abu Naser. (2012). "VANET Routing Protocols: Pros and Cons." arXiv preprint arXiv:1204.1201.

[12]. Kumar, Rakesh, and Mayank Dave. (2011). "A Comparative of Various Routing Protocols in VANET." arXiv preprint arXiv:1108.2094 (2011).

[13]. Raya, M., & Hubaux, J. (2005). The security of vehicular ad hoc networks. In Proceedings of the 3rd ACM workshop on security of ad hoc and sensor networks (SASN 2005) (pp. 1 11), Alexandria, VA.

[14]. Sumra, Irshad Ahmed, Iftikhar Ahmad, Halabi Hasbullah, and J.L. bin Ab Manan. (2011). "Classes of Attacks in VANET." In Electronics, Communications and Photonics Conference (SIECPC), 2011 Saudi International, pp. 1-5. IEEE, 2011.

[15]. Akanksha Khare and Pushpraj Singh Chauhan, (2016). A Rule Based Mechanism to Mitigate the Packet Dropping in Mobile
Ad hoc Network, *International Journal of Electrical, Electronics and Computer Engineering,* **5**(1): 21-26.

[16]. Anand Motwani and Vimal Dhote, Optimized AODV (2016). Routing for Effective Attack Security in Wireless Sensor Networks, *International Journal of Electrical, Electronics and Computer Engineering* **5**(1): 33-40.