International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 6 Issue 3, March-2017

A Study on WPAN Architecture and Communication Challenges and Methods

Amit Kumar Yadav[1], Anisa Irshad Shah[2], Saloni Sehgal[3]

[123]M.Tech. Student, Ansal University, SET (School of Engineering and Technology)

ABSTRACT

WPAN is critical network form defined with restricted area with smart sensing nodes. The energy nodes are defined with energy restrictions. The network suffers from various architecture level, communication level and security challenges. In this paper, a study on various critical aspects to WPAN network are provided. The paper has provided the characterization of WPAN network with topology, bandwidth and other physical properties. The paper also explored the security and communication challenges. Various available communication methods are also discussed in this paper.

Keywords: WPAN, Security, Architecture, Routing Protocol.

1. INTRODUCTION

Personal Area Network is a bunch of sensor devices connected in real environment to capture the sensitive information. In WPAN these sensor devices are known as wireless sensors, which simultaneously adds to the network and forward the data. Figure 1.1 shows about WPAN, transmission in wireless sensors can be done by making air as a medium, as per the figure wireless node can be bodily attached to a motor vehicle, or to a jet to make wireless communication among them[1][2][3][4].

In WPAN for transmission, a wireless node may be the source, the goal, or an intermediate node. When the wireless sensors are acting as an intermediate node then it performs as a router. Such router can accept and transmit the information packets to its adjacent neighbor. In the wireless atmosphere, all sensors keep on moving rather than being stagnant. Therefore, the wireless topology does not remain same all the time. WPAN environment has some limitations for example this network is a self-organizing network. The biggest issue of such network is that the topologies keep on changing because of the movement of the sensors in the wireless network. In such type of network all sensors act as participants and as well as routers. Due to the wireless communication and continuous change in topology there is a large probability of different types of attacks and loss in the information packets [5][6][7].

Security is very important concern because of the weakness like Dynamic topology, wireless links, Cooperativeness or Limited resources, packet loss due to error in transmission and route changes due to mobility and many other challenges. Network security is very important and difficult task because no single security solution is enough for the network. WPANs Characteristics, features, advantages and different types of communication characterization are defining below:

1.1 Network Characteristics:-

Ad hoc Networks are example of networks which offers unlimited mobility without any basic infrastructure. Basically, WPAN is a set of sensors that passes data to each other by making a multi-hop network[8][9]. Characteristics of WPAN are shown below:

i) Dynamic Topologies: Sensors are free to move in the wireless network. Sensors move in a random manner and because of this random movement the topology of the network also changes in an unsystematic manner. As a result directional and unidirectional links are formed between the sensors.

ii) Energy Constrained Operation: Sensors in the wireless system depends on the energy source like batteries. Numbers of tasks are performed by the sensors when they consume more energy. So, energy should be properly utilized in the network.

iii) Bandwidth Constraint: If we compare the efficiency of wireless network to the wired network than wireless has less capacity. Wireless network is less efficient because of several reasons like fading, noise and interference etc. Due to all these reasons clogging (congestion) occurs in the network and it is a big problem in bandwidth utilization.

iv) Limited Physical Security: WPAN are usually more open to physical security threats compared to wired networks because the WPAN is a scattered system and due to this, chances of eavesdropping, spoofing, masquerading [158,159] increases.

1.2 Features of Mobile Ad Hoc Network:-

i) Autonomous Terminal: In Ad hoc Network, every mobile terminal is an independent node. This node can act in many ways, it can act as a host and it can act as a router. Sensors can also behave as switching functions like a router. So, the end point and the switches cannot be identified independently.

ii) Distributed Operation: Circulation of control and management is done between the terminals in order to have vital control over the network operations. In order to execute a function like security or routing, the sensors must pair with themselves and independent node must behave as a relay.

iii) Multi-hop Routing: Ad hoc routing algorithms can be differentiated on the basis of routing protocol and link layer attributes. They can be classified as single hop algorithm and multi hop algorithm. Multi hop algorithm is more complex as compared to single hop because of its structure. During transmission of information, the packets should cross more than one intermediate node.

iv) Light-weight Terminal: In many cases, the Ad hoc Network sensors are movable devices. These devices have very low memory size; they have very less storage for power and quite low processing capacity. Such devices need improved algorithm in order to perform computing and communication function.

2. WPAN SECURITY CHALLENGES

In order to provide a secure networking environment, here are some services that are required [11,16]. For complete security below given services should be fulfilled[10][11][12]:

Figure 1: Shows the Security Goals

i) Authentication: In order to have a secure system, authentication is must. The prime focus of this service is to ensure the sender and the receiver that the other user is authentic and not the fake user. Authentication can be done by giving a user name or a password to individual users or by using cryptographic techniques.

ii) Confidentially: In this service the data is sent in an unreadable form for unauthorized users. By doing this if some unauthorized user wants to read the data then he want be able to do that. So data should be converted in non readable form by using cryptographic techniques data, and another technique is to use directional antennas. This service makes the backbone of security function.

iii) Integrity: This service makes sure that the data is not altered during transmission. For this, service should be provided using cryptographic techniques. Data should be encrypted, in non readable form while transferring to the other user. This survive forms a very important part of network security.

iv) Availability: This service makes sure that the next hop users should always be available to the source user when required. In case, when the desired user is not available then the information will be lost and hence the security will be compromised.

V) Non-repudiation: This is very important service. The main purpose of this service is to make sure that a particular message is sent by a particular individual and that individual should not refuse that this message is not send by him. For remove such problems, this can be done with the help of digital signatures or with the help of private encryption key.

Vi) Access Control: This service depends on authentication. The whole point of access control is that some unwanted user or unauthorized user cannot access to the system and cannot use the services provided by the network. This can be done by assigning user name and password to individual authorized or authentic users.

3. COMMUNICATION CONSTRAINTS

The parameters measured for route optimization are divided in two broader categories called physical parameters and the communication parameters. The physical parameters are generally the static parameters which represent network or node capabilities [13][14][15]. All parameters are described below in figure 2.

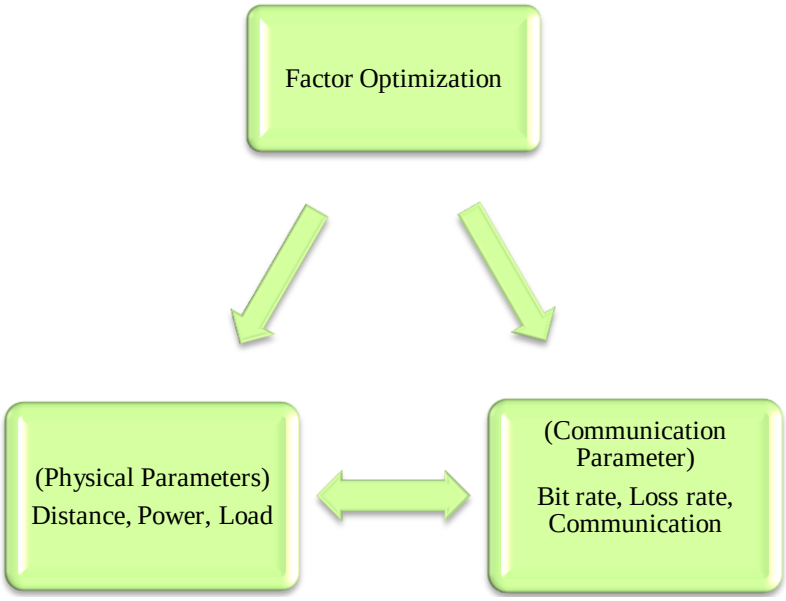

Figure 2: shows the Optimization Factors

To optimize the communication path, it is compulsory to decrease the communication distance. To overcome this, the shortest path algorithms are suggested by various protocols. The path is related to the communication delay and the power used to perform the communication. If we perform the communication from same shortest distance route, the load over the distance will be enlarged. Load is a vector that changes the routing decision. The load is an important factor and that can be increased because of algorithmic approach or it can be increased by some attacker purposely. Larger the network load, less the communication reliability will be. It is very important to select a node with fewer loads as the next hop [15] [16] [17] [18].

Second physical parameter related with individual node is the battery or the energy. Usually, the network sensors are not explained with energy specification, but some of the important and real time Personal Area Network are defined with energy specification such as war or rescue scenario network. In these cases, the network route with less energy consumption is marked as the effective route for network communication. In personal network, such kind of node based characteristic is important for route generation [14] [15].

Next category of optimization parameters is communication parameters. The communication parameters are read dynamically. Such parameters are analyzed for a given instance of time. The session based parameters are periodic and analyzed for a finite interval .Such parameters consist of the delay analysis, communication loss analysis and communication rate study. A network route with less delay, lower loss rate and higher communication rate is considered

as efficient communication path. The loss rate shows the steadiness of packet delivery where as the communication rate and communication delay represents the efficiency parameters [16] [17].

4. COMMUNICATION METHODS

Such kind of network is explained [17][18][19] under the feature guidance at node as well as network level. The network is explained with variable position as well as fixed position scenarios. The location of sensors is explained under mobility guidance and narrow range setting under the implication of stability. The network is explained under the limitation of route identification and volume limit guidance. The network is explained under the node neighbor identification that can identify the efficient next hop to create the effective communication route over the network system. The hop recognition can be finished with the range and other parameters guidance. The routing approaches adapted by different Personal Area Network are shown and discussed. These approaches are given below figure 3.

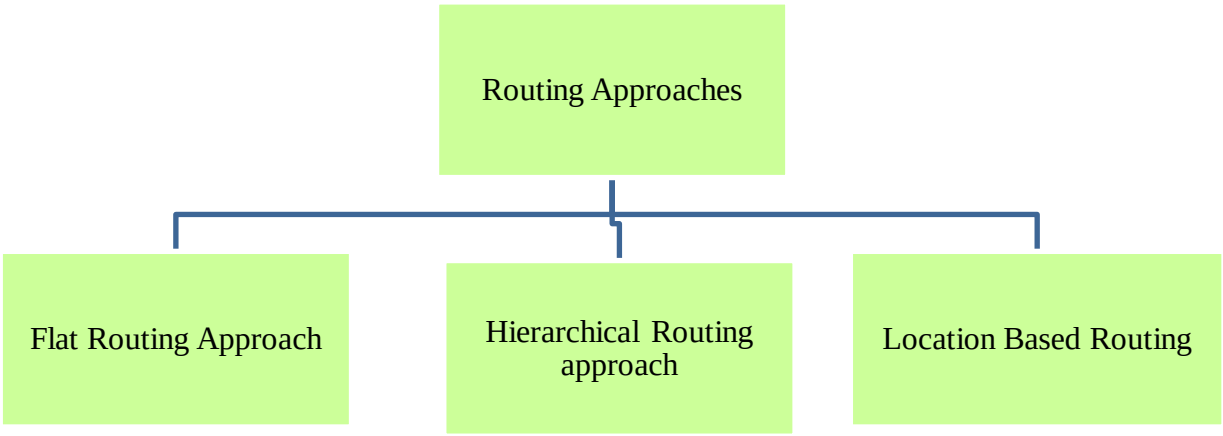

Figure 3 : Routing Approaches

1.8.1 Flat Based Routing: Such kind of routing technique is used in identical network with randomized parameters guidance. All the network sensors are of same type and the multi hop route is used to optimize the network route. In most of the intra- cluster Personal Area Network, these kind of routing approach is been used to carry out the network communication. This routing approach works on the destination adaptive and data adaptive communication carried out over the network. The network also has the multi case communication to minimize the communication effort. To carry out the multi cast communication aggregative communication approach is adaptive in these networks. Such kind of routing technique also requires minimizing the number of intermediate sensors as well as minimizing the communication effort of each involving node over the network. Such kind of communication route read the next neighbor under different physical and communication parameters and choose the node with effective throughput and minimum expected loss and delay. The work is about to minimize the flooding by capturing the routing information as well as minimize the redundancy in communication. The work is also effective to carry out the broadcasting of the network as well as effective hop selection over the network[18][19][20].

1.8.2 Hierarchical Routing: In this routing technique, the inter cluster communication is carried out. The sensors can identical or different but the sensors in a same network are considered as identical. The network area chosen in this network type is generally big and measurable. Each sub network is explained under the guidance of controller node so that the effective network aggregation will be carried out by the node. This controller node takes the adaptive decision regarding the node guidance and the sub network head specification. The segmented communication is made in the form of tree and at each tree node decision regarding the adjacent network election will be done.

1.8.3 Location Based Routing: The routing technique explained here for the guidance of network node and tracking of node under the location guidance and creation. This routing technique relies on the node location and the signal strength of various positions over the network. The satellite guidance is used to select the position of the node and to carry out the activity of the network under guidance of protocol. GPS analysis is carried for node location monitoring and indication to select the node and to perform the zoning of the network with guidance of the criticality for the network with specification of routing and mobility.

5. COMMUNICATION PROTOCOLS

Routing protocols in Ad hoc Networks are divided into three categories depending on their functionality [11,12,16,17,20,21]. Below given figure 4 shows the routing protocol.

1. Reactive protocols
2. Proactive protocols
3. Hybrid protocols

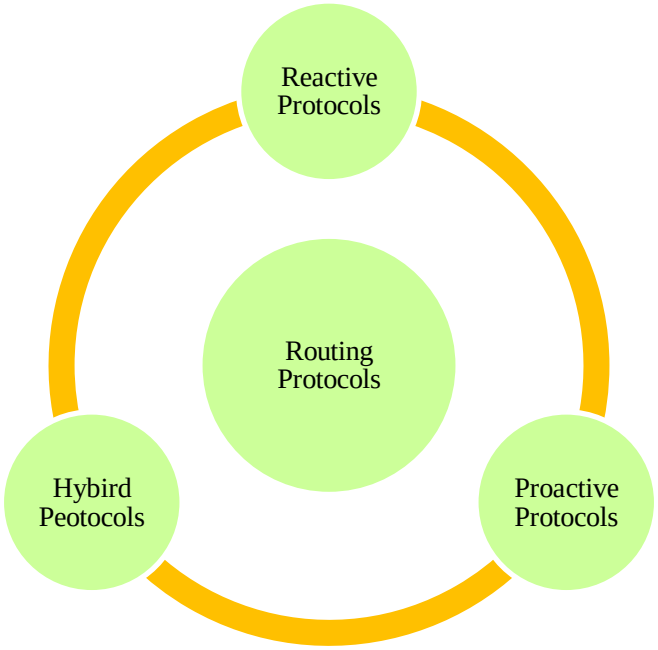

Figure 4 : Shows the Routing Protocol

1.10 Algorithm:-

1.10.1 DSDV (Destination-Sequenced Distance Vector) Algorithm: This algorithm [17] [18] carries out predictably, sending virtually all information packets, when node mobility rate and node movement speed is less, and failing to converge as an outcome node mobility improve. DSDV is a hop-by-hop distance vector routing protocol want every node to time to time broadcast routing updates. The major plus point of DSDV over traditional distance vector protocols is that it guarantees loop-freedom.

1.10.2 TORA (Temporally-Ordered Routing Algorithm) Algorithm: TORA algorithm, although the bad performer in performed trial in terms of routing packet overhead, still delivered over 90% of the packets in scenarios with 10 or 20 sources. At30 sources, the network was not capable to hold all of the traffic generated by the routing protocol and an important fraction of data packets were dropped. TORA is based on a "link reversal" algorithm because TORA is a distributed routing protocol. TORA is planned for, locate out routes on order, offer multiple routes to a target, and create paths fast. Path optimality (shortest-path routing) is considered of next importance, and longer paths are usually used to avoid the overhead of discovering fresh paths.The next step taken by TORA can be described as waterfall and the real network work in the waterfall form. In this, junction symbolizes the sensors in the network, tubes shows the relation between all sensors in the network and water in tubes shows the packets flowing towards the destination. Routing procedure shows, the height difference between the node and the destination node. If a tube is blocked that connect the node A and B than in such form water will not be flow more in the tube, if the node A is set at height location than its neighbor, water will change its direction.

1.10.3 AODV (Ad Hoc On-Demand Distance Vector) Algorithm: AODV algorithm[19] [20][21] acts almost as well as DSR at all mobility rates and movement speeds and accomplishes its aim of reduce source routing overhead, but it still wants the transmission of numerous routing overhead packets and at high rates of node mobility is really more costly than DSR. AODV is essentially a grouping of both DSR and DSDV. It have a loan the basic on demand mechanism of Route Discovery and Route Maintenance from DSR, plus the use of hop by-hop routing, serial numbers, and periodic beacons from DSDV. AODV is a purely reactive routing procedure. In this procedure, every workstation does not want to maintain a view of the whole network or a path to every other terminal. Nor does it want to periodically replace path information with the neighbor terminals. Only when a mobile terminal has packets to transmit to a destination does it want to find out and maintain a path to that destination terminal. In AODV, every terminal contains a path table for a destination. Path table stores the information like: destination address and its series number, active neighbors for the

passageway, hop tally to the destination, and finishing time for the table. The finishing time is updated each time the path is used. If path has not been used for a particular phase of time, it is removed.

REFERENCES

[1]. Rajesh Yerneni, "Enhancing performance of AODV against Blackhole Attack", CUBE September 3-5, 2012, Pune, Maharashtra, India, ACM 978-1-4503-1185-4/12/09.
[2]. Hesiri Weerasinghe, "Preventing Cooperative Blackhole Attacks in Mobile Ad hoc Networks: Simulation Implementation and Evaluation", International Journal of Software Engineering and Its Applications, Vol. 2, No. 3, July, 2008.
[3]. Mehdi Medadian, "Detection and Removal of Cooperative and Multiple Blackhole Attack in Mobile Ad hoc Networks", International Conference on Computer and Software Modeling, IPCSIT, Vol.14, 2011, IACSIT Press, Singapore.
[4]. Sweta Jain, "A Review Paper on Cooperative Black hole and Gray hole Attacks in Mobile Ad hoc Networks", International Journal of Ad hoc, Sensor & Ubiquitous Computing, (IJASUC), Vol.2, No.3, September 2011.
[5]. Sanjay Ramaswamy, "Prevention of Cooperative blackhole Attack in Wireless Ad hoc Networks".
[6]. Varsha Patidar, "Black hole Attack and its Counter Measures in AODV Routing Protocol", International Journal of Computational Engineering Research, (ijceronline.com), Vol. 2 Issue. 5.
[7]. Harsh Pratap Singh, "Guard against cooperative black hole attack in Mobile Ad hoc Network", International Journal of Engineering Science and Technology (IJEST), ISSN: 0975-5462, Vol. 3 No. 7, July 2011.
[8]. Poonam, "Eliminating misbehaving sensors by Opinion based Trust Evaluation Model in WPAN's", ICCCS'2011, Rourkela, Odisha, India, ACM 978-1-4503-0464-1/11/02.
[9]. Poonam Gera,"Trust Based Multi-Path Routing for End to End Secure Data Delivery in WPAN's", SIN'2010, Taganrog, Rostov-on-Don, Russian Federation, ACM 978-1-4503-0234-0/10/09.
[10]. M.Shobana, "Geographic Routing used in WPAN for Black hole Detection", CCSEIT-2012, Coimbatore, Tamilnadu, India, ACM 978-1-4503-1310-0/12/10.
[11]. Poonam, "Misbehaving sensors Detection through Opinion based Trust Evaluation Model in WPANs", International Conference and Workshop on Emerging Trends in Technology (ICWET 2011), TCET, Mumbai, India, ACM 978-1-4503-0449-8/11/02.
[12]. Kamaljit Kaur," Comparative Analysis of Black hole attack over Cloud Network using AODV and DSDV", CCSEIT'2012, Coimbatore, Tamil nadu, India, ACM 978-1-4503-1310-0/12/10.
[13]. B.Revathi, "A Survey of Cooperative Black and Gray hole attack in WPAN", International Journal of Computer Science and Management Research, Vol. 1 Issue 2, September 2012, ISSN: 2278-733X.
[14]. Vishnu K, "Detection and Removal of Cooperative Black/Gray hole attack in Mobile Adhoc Networks", International Journal of Computer Applications, ISSN: 0975 – 8887, Vol. 1, No. 22.
[15]. Moumita Deb, "A Cooperative Black hole Node Detection Mechanism for Ad hoc Networks", Proceedings of the World Congress on Engineering and Computer Science, WCECS 2008, San Francisco, USA, ISBN: 978-988-98671-0-2.
[16]. S. Marti, T. Giuli, K. Lai and M. Baker, "Mitigating routing misbehavior in mobile Ad Hoc Networks", in the 6th ACM International Conference on Mobile Computing and Networking, 2000.
[17]. S. Buchegger and J.Y. L. Boudec, "Performance analysis of the Confidant protocol (cooperation of sensors: Fairness in dynamic ad- hoc networks)", MOBIHOC'02, 2002.
[18]. Balakrishnan, Kashyap, Jing Deng and Pramod K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad hoc Networks", IEEE Transaction on Wireless communication and Networking Conference, Volume 4, 2005.
[19]. Liu, Kejun, et al. "An acknowledgment-based approach for the detection of routing misbehavior in WPANs", IEEE Transactions on Mobile Computing, volume 6, issue 5, pp 536-550, 2007.
[20]. Admir Barolli," Application of Genetic Algorithms for QoS Routing in Mobile Ad-Hoc Networks: A Survey", *2010* International Conference on Broadband, Wireless Computing, Communication and Applications 978-0-7695-4236-2/10© 2010 IEEE.
[21]. Leonard Barolli," A Genetic Algorithm Based Routing Method Using Two QoS Parameters", Proceedings of the 13th International Workshop on Database and Expert Systems Applications (DEXA'02) 1529-4188/02 © 2002 IEEE.