**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**

***IJCSMC, Vol. 5, Issue. 1, January 2016, pg.219 – 225***

# A Survey on Data Discovery and Data Dissemination in Wireless Body Area Network

**Prameela.S[1], Dr. Ponmuthuramalingam.P[2]**
[1]Ph.D scholar, Department of Computer Science, Government Arts College, Coimbatore, India
[2]Associate Professor and Head, Department of Computer Science, Government Arts College, Coimbatore, India
prameelaswaminathan@gmail.com, ponmuthucbe@gmail.com

***Abstract— Wireless Body Area Networks collect health data of the patients, processes, aggregates and sends to the centralised healthcare database. The health data sent has to be accurate, reliable, confident. Data discovery and dissemination protocols disseminate data. This survey discusses data discovery and dissemination protocols and security in wireless body area networks.***

***Keywords— Wireless Body Area Networks, Data Discovery, Data dissemination, Attacks, strategies, security***

## I. INTRODUCTION

Wireless body area network (WBAN) is a wireless network of wearable computing and implantable body sensor devices. A WBAN consists of a wireless network of tiny and smart intelligent sensors which are embedded to or placed inside a patient to monitor his physiological activities and movements. It is an efficient way to collect and provide constant and real-time health and movement associated information of patients to medical team with security measures in data discovery and dissemination. WBANs automatically monitor physiological readings, forwards to the nearby processing device which is the controller or base station. Smart phone, a wrist watch, a tablet PC, a laptop PC, or a robot can act as base station based on the application needs. Packets broadcast by the base station can be received by each body sensor through one or two hops. The two-tier architecture confirms the features of a WBAN such as communication, resource, deployment, density, and mobility characteristics. Moreover, such a two-tier architecture is indispensable for increasing overall network capacity and scalability, reducing system complexity, prolonging network lifetime, and ensuring the security and privacy. With respect to disseminating data items, sensors of practical WBANs are at most three hops away from the base station.

In an operational WBAN, each node of the network stores some common variables. These variables are added, deleted, and modified by data discovery and dissemination protocols by way of requesting each node to exchange packets so that they eventually become consistent across the network [1].

In Data Collection stage, each data item contains a unique key to identify the parameter or command that it aims to update, and a value to reflect its freshness. In Drip, each data item is formatted as a three-tuple (key, version, data), in which key identifies uniquely the concerned variable, version indicates whether the data item is new and data denotes the disseminated value for the concerned variable.

In Data dissemination phase, a node needs to periodically broadcast a summary of its stored data, unless the same summary has been received recently. If a node receives an older summary from its neighbouring node, it will update the neighbouring node with the latest summary. The broadcast interval is increased exponentially in order to save energy, when the data of all nodes are consistent. A node which has new data, will report more quickly.

Data dissemination were classified by type of the disseminated information or based on nodes status (energy, connectivity) as
1. Clustered Data Dissemination (CDD)
2. Distributed Data Dissemination (DDD)

Clustered Data Dissemination (CDD):
In this data is disseminated from one-WBAN nodes to their coordinator and then from the coordinator to the adjacent coordinators until reaching the team leaders coordinator that is the sink node responsible for collecting data from other body nodes .Each WBAN could operate in a single frequency.

Distributed Data Dissemination (DDD):
Data is disseminated from one BAN nodes to the any reachable adjacent nodes (simple node or coordinator), until reaching the team leaders coordinator. Consequently, all nodes need to share same frequency which could raise an interference issue. The final destination is always the coordinator of the Team Leader.

Data discovery and dissemination protocols are used to adjust configuration parameters of body sensors or distribute management commands and queries to sensors to disseminate the data through the wireless link by ensuring the reliability and confidentiality of the data.

## II. LITERATURE SURVEY ON DATA DISSEMINATION PROTOCOLS

### *A. Drip*

The sensor network management systems dissemination protocol named Drip protocol was proposed by Tolle et al.[2]. This is the simplest of all dissemination protocols which uses trickle algorithm. For transmitting of a new message, a new version number is generated and used. This will cause the protocol to reset the Trickle timer and thus disseminate the new value. It has a standard message reception interface. Each node gets registered with the specific identifier, which represents a dissemination channel. The messages received are delivered to the node directly. Recent messages are broadcasted quickly All messages received on that channel will be delivered directly to the node. Drip avoids redundant transmission and achieves greater efficiency.

### *B. Code Drip*

This data dissemination protocol proposed by Nildo et al.[3] uses network coding and is mainly used for dissemination of small values. In this, received data packets are combined by sensor nodes to one packet and this combined packet is sent to its neighbours.

It uses trickle algorithm. Network Coding is a mechanism that combines packets in the network thus increasing the throughput and decreasing number of messages transmitted and also improves reliability and speed of dissemination.

### *C. SeDrip*

Daojing He et al. proposed a secure, lightweight, and Denial-of Service (DoS)-resistant data discovery and dissemination protocol named SeDrip. SeDrip protocol works under limited resources of sensor nodes. The ECC public key algorithm and Merkle hash tree is combined in SeDrip to avoid frequent public key operations and achieve strong robustness against various malicious attacks.

SeDrip consists of three phases: system initialization, packet pre-processing, and packet verification. Se-drip suffers from some disadvantages, that is delay and centralised approach.

*D. DiDrip*

Distributed data discovery and dissemination protocol [20] was proposed to overcome the disadvantages of SeDrip. It consists of four phases they are System Initialization Phase, User- Joining Phase, Packet Pre-Processing phase and Packet Verification phase. Few Sensor nodes are considered as network owner and few as users and one node as destination. ECC cryptography is used for key generation and keys are distributed to all nodes. Hash function is used to make it more secure. DiDrip is implemented by using two methods they are data hash chain and Merkle hash tree method.

*E. DIP*

Dissemination Protocol (DIP) is a data detection and dissemination protocol proposed by Lin et al. [4]. This protocol is based on Trickle algorithm. It Detects difference of data in a node and identifies the different data item .The concept of version number and keys for each data item is followed . In addition to the version number, DIP ensures that all nodes have same data by decrementing hashes to a minimum of 0.

*F. MNP*

Sandeep et al. proposed a multihop network reprogramming protocol (MNP) [5]. It provides a Reliable service to propagate new program code to all sensor nodes in the network. The main aim of this dissemination protocol is to ensure reliable, low memory usage and fast data dissemination.

It is based on a sender selection protocol in which source nodes compete with each other based on the number of distinct requests they have received. In each neighbourhood, a source node sends out program codes to multiple receivers. When the receivers get the full program image at their side, they become source nodes, and send the code into their neighbourhood. Issues of collisions exists. This is solved by selecting a suitable sensor node based on some parameters maintained by the nodes and some advertisement and download messages exchanged by the nodes. It is like a greedy algorithm. Pipelining can be included in this protocol to enable faster data propagation in the case of larger networks.

*G. DHV*

It is a code consistency maintenance protocol (Difference detection, Horizontal search, and Vertical search).given by Dang et al**. [6].** It tries to keep codes on different nodes in a WSN consistent and up to date. The data items are represented as tuples (key, version).This protocol tries to overcome the disadvantages of previous protocols like DRIP and DIP by reducing the complexity involved in the updating of data in the network. It is based on the observation that if two versions are different, they may only differ in a few least significant bits of their version number rather than in all their bits. Hence, it is not always necessary to transmit and compare the whole version number in the network. Here the version number is given as a bit array. DHV uses bit slicing to quickly determine the out of date code, resulting in fewer bits being transmitted in the network.

## III. DIFFERENT DATA DISSEMINATION STRATEGIES

Fang Hongping and Fang Kangling[7] have classified Data Dissemination strategies into four major categories based on basis of operation Push-based strategy, On-demand (or pull-based) strategy, hybrid strategy and data allocation over multiple broadcast channels.

*A. Push Based Strategy*

Sensory data is pushed by all source nodes to the sink nodes through multi hop routing. The query result from sink nodes is retrieved without communication cost. Its advantage is that it is efficient as it reduces push- query routing cost to zero. The disadvantages are
(1) Communication cost in storage phase is comparatively high (2)Due to multi-hop routing, the neighbour nodes of sink nodes will undertake more data delivery task than other sensor nodes, resulting in hotspots. , the system robustness and stability cannot be ensured.

There are two kinds of push based Data Dissemination strategy namely, flat broadcast and broadcast disks [8].

*1. Flat Broadcast*- The simplest scheme for data scheduling is flat broadcast. With a flat broadcast program, all data items are broadcasted in a round robin manner. The access time for every data item is the same, i.e., half of the broadcast cycle. This scheme is simple, but its performance is poor in terms of average access time when data access probabilities are skewed.

*2. Broadcast Disks*- Data items are assigned to different logical disks so that data items in the same range of access probabilities are grouped on the same disk. Data items are then selected from the disks for broadcast according to the relative broadcast frequencies assigned to the disks.

### *B. Pull Based Strategy*

The pull-based Strategy adopts completely opposite idea to push-based Strategy. The source nodes stores data at home and wait for query passively. On the contrary, the consumer nodes broadcast query demands to source nodes throughout the network on their own initiatives. Communication cost is less but the disadvantage is that some source nodes even if they have no, related data they have to participate in data delivery.

### *C. Push Pull (Hybrid) Strategy*

A better approach, called hybrid broadcast, combines push-based and pull-based techniques. It introduces the combination between consumer node and source node. In the first phase, source nodes get the storage location and then transfer sensory data to rendezvous nodes closest to location. Then consumer nodes can directly transmit query to rendezvous node using same regulations. In this way, queries flooding can be avoided efficiently.

### *D. Data Allocation Over Multiple Broadcast Channels*

Multiple physical channels have capabilities of improved fault tolerance and also have scalability benefits.

### **Security in WBANS**

Security in WBAN faces different challenges due to Wireless nature of communication model, Lack of fixed infrastructure, Resource limitation of nodes, Unknown topology of network prior to deployment. The goals to be achieved are Confidentiality of data, Integrity of data, Authentication for data, Access control, Data availability, Non-repudiation, Authorization .Some of the specific security goals are Efficiency, Scalability, Freshness of data, and Survivability of network.

## IV. ATTACKS DURING DISSEMINATION

External and internal attacks occur during dissemination. External attack is performed by attackers external to networks but the internal attacks are more dangerous one as attackers is already in the network.

### *A. Eavesdropping Attack*

The eavesdropping attack is an external attack .It can be passive or active. In passive eaves dropping message is being listened from broadcast medium. In active eavesdropping, node enacts as valid node and grabs information. Encryption techniques are used to prevent this type of attack[9]

### *B. Replay Attack*

A replay attack or playback attack is a kind of attack in which a valid data transfer is repeated or delayed by attackers. Packet signature ,verification operations and Bloom filters are some techniques to prevent occurrence of replay Attacks.

### *C. Pollution Attack*

This kind of attack is seen primarily during data dissemination in WSN. It can be used to pollute or flood the network with false data. Especially when network coding technique is used invalid network coded data is stored as intermediate nodes in a node path. To overcome this attack cryptographic technique like homomorphic hashing, identity certificates and signatures can be used.[10]

### *D. Sybil Attack*

In this type of attack a malicious node imitates other nodes or simply by claiming false identity.
In data dissemination Sybil attack collects vital messages from the base station. So Sybil attacks must be dealt with as well. Many techniques have been proposed like identity certificates, methods based on Merkle hash tree [11].

### *E. Denial of Service Attack*

Lack of proper authentication leads to valid packets being denied of their required status .Due to the characteristics of energy-sensitivity, dynamic nature of nodes and limited resources, sensor networks are very vulnerable to DoS attacks. Proper authentication schemes can be used in data dissemination to avoid this kind of attack. Se-Drip is one such protocol [12].

*F. Wormhole Attack*

An adversary connects two distant points in the network using a direct communication link called a wormhole link. Single symmetric key for reprogramming is to be avoided. An internal intrusion detection system (IDS) system is one method that can help networks to limit the risk from insider attacks [13].

## V. OVERVIEW OF DATA DISSEMINATION PROTOCOLS BASED ON ARCHITECHTURE

Based on nature of architecture the overview of networks are as

*A. Directed Diffusion(DD)*

(DD), was proposed by Intanagonwiwat et al. [14] shows the operation of data centric communication protocol for a WSN scenarios. Directed diffusion protocol based on query, where sink queries the sensors in an on-demand fashion by disseminating an interest. Directed diffusion consists of three stages:

1. *interest propagation*: In this stage on demand from sink node for a packet its matching target is searched.

2. *initial gradient setup* : a reply link or gradient from the target node is setup.

3 .*Data Delivery Reinforced Path*: Source node sends data packets to sink node in the initial setup gradient direction. Sink sends a reinforced packet to the neighbour node which is the first one receiving the target data. This continues and hence a path with maximum gradient is formed, so that in future received data reinforced path. packets can transmitted along best way.

The possible advantages are saving of network energy thus prolonging network lifetime. Shortcoming of this protocol is that it can't be used where continuous data delivery is required as it is on demand based data model.

*B. Two- Tier Data Dissemination-*

TTDD [15] is based on decentralized architecture. It uses a grid structure to divide the topology into cells. Sensors located at a cell boundary need to forward the data. Forwarding points near grid boundary called dissemination nodes (DN). These DN hears query from consumer node and is same as that of query propagation path as shown in Fig.1.

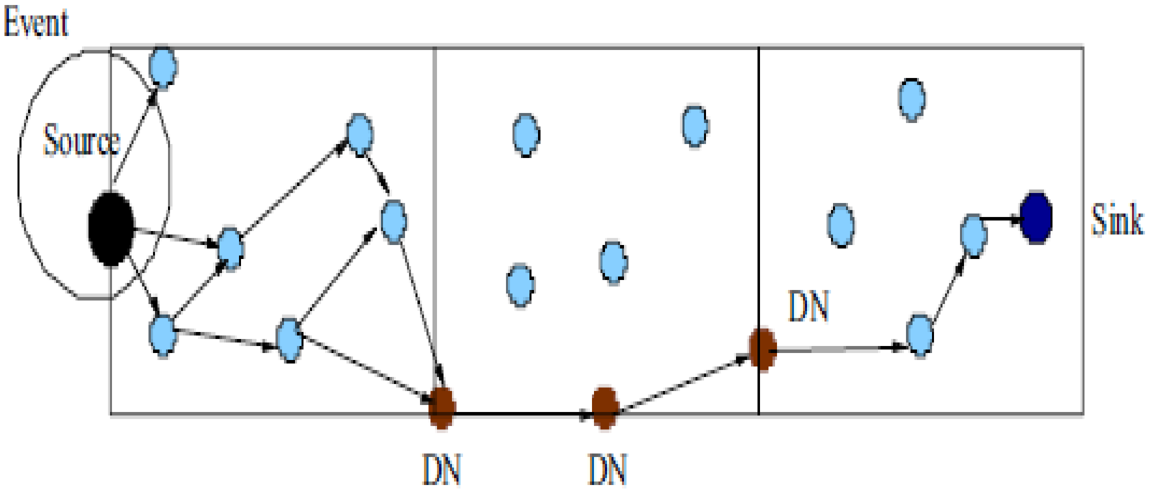

Fig.1 Two- Tier Data Dissemination [15]

*C. Location Oblivious Hybrid Data Dissemination-LOHD*

LOHD[16] it adaptively selects rendezvous node called ultranode through a well-controlled flooding and the ultra-node maintains the gradients from sources to sinks. Steps involved are selecting an ultra node, sending the gradients from source to sink, sending gradients through control messages and finally sending the data. Various networks are used for source sink distributions. The disadvantage of this protocol is that routing overhead increases.

*D. Balancing Push- Pull*

The model [17] combines push and pull for information dissemination and gathering. The push component features data duplication. The pull component features a dynamic formation of a non-demand routing structure. A major application of such a query generation mode is to support mobile information gathering agents (mobile sinks) or hierarchical networks where higher hierarchies are more intelligent and may demand information

*E. Core Based Reliable Data Dissemination*

The object dissemination is divided into two distinct phases. Reliable links are selected as core nodes before data dissemination actually starts. The object is propagated from the sink to the core nodes. Then the core nodes disseminate the object to their neighbouring non-core nodes in parallel. The core based two-phase approach used by CORD [19] is motivated by the goal of reducing the energy consumption for disseminating the object within the network.

A distinctive feature of CORD is that in addition to adopting a two phase approach, it aggressively uses sleep scheduling in order to further reduce energy consumption for large object dissemination.

*F. Real Time Data Dissemination*

In this protocol [18], the Data Dissemination procedure consists of three steps: normal routing projection routing and overhearing of the mobile sink. All the procedures are based on the spatiotemporal approach.

In normal routing a data packet is forwarded from a source node to the exit point of movable area. Some relay nodes within a movable area are selected as branch nodes for projection routing. The reason of two routing nodes is to define the transmission distance between a source and a mobile sink. This protocol calculates the desired delivery speed. The value of time deadline success ratio which is defined as the ratio of successfully received data packets on the time. All generated data packets from the source node are high in case of RTDD. Fig. 2 depicts the Data Dissemination in RTDD.

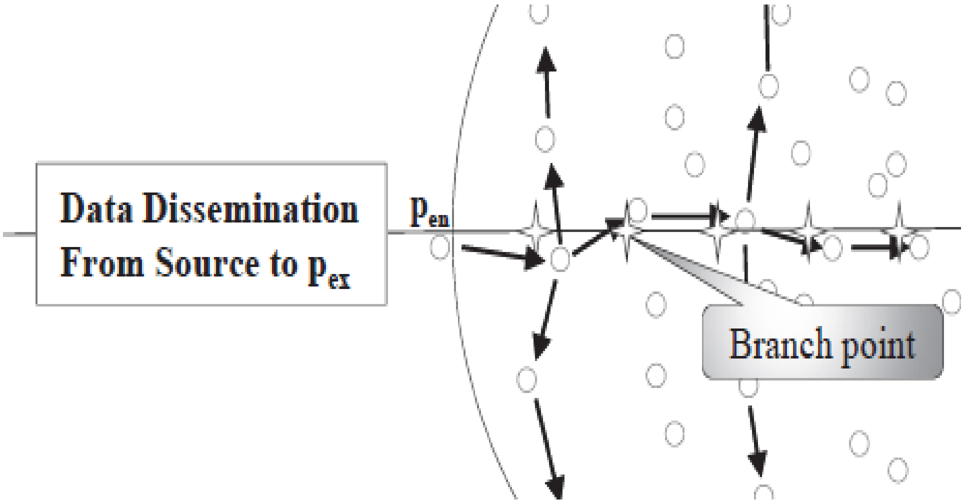

Fig.2 Routing Branching in RTDD [18]

## VI. CONCLUSION

This survey is on various dissemination protocols, the strategies employed in these dissemination protocols ,their architecture and also various security attacks. Security being one of the key objective in dissemination of medical data in WBAN as it deals with sensitive medical data of patients. It is also essential to be disseminate data reliably and with energy efficiency. Execution time, propagation delay, energy overhead, memory overhead are certain important aspects which are to be evaluated.

## REFERENCES

[1] Daojing He, Sammy Chan, Yan Zhang,and HaomiaoYang,,"*Lightweight and Confidential Data Discovery and Dissemination for Wireless Body Area Networks*", IEEE Journal of Biomedical And Health Informatics, Vol. 18, NO. 2, pp.440-448,March 2014.

[2] G. Tolle and D. Culler , "*Design of an application-cooperative management system for wireless sensor networks*", in Proc. EWSN, pp. 121–132, 2005.

[3] NildoRibeiro Junior, Marcos A. M. Vieira, Luiz F. M. Vieira, and Omprakash Gnawali,"*CodeDrip: Data Dissemination Protocol with Network Coding for Wireless Sensor Networks*", in Proceedings of the 11th European conference on Wireless sensor networks (EWSN 2014), Feb. 2014.

[4] Lin, K., Levis, P.," *Data discovery and dissemination with DIP",* In :Proceedings of the 2008 International Conference on Information Processing in Sensor Networks (IPSN 2008), Washington, DC,USA, IEEE Computer Society (2008) 433–444.

[5] S. Kulkarni and L. Wang,."*Mnp: Multihop network reprogramming service for sensor network".* In 25th International Conference on Distributed Computing Systems, June 2005.

[6] T. Dang, N. Bulusu, W. Feng, and S. Park, "*DHV: a code consistency maintenance protocol for multi-hop wireless sensor networks*," in Proc. 2009 EWSN, pp. 327–342.

[7] Fang Hongping, Fang Kangling, *"overview of Data Dissemination strategies in wireless sensor networks*", in International conference on E- Health Networking, Digital Ecosystem & Technologies,2010.

[8] YasirFaheem, SaadiBoudjit, Ken Chen, "*Data Dissemination strategies in mobile sink wireless sensor network: A Survey*," IEEE communication letters, Vol. 17, No. 1, March, 2009.

[9] Hong-Ning Dai, Qiu Wang, Dong Li, and Raymond Chi-Wing Wong, "*On Eavesdropping Attacks in Wireless Sensor Networks with Directional Antennas"* ,International Journal of Distributed Sensor Networks Volume 2013.

[10] Ming He, Hong Wang, Lin Chen, Zhenghu Gong, Fan Dai and Zhihong Liu*," Securing network coding against pollution attacks based on space and time properties*", In Proceedings: 2012 2nd International Conference on Computer Science and Network Technology.

[11] Q. Zhang, P. Wang, D. S. Reeves, and P. Ning.," Defending against Sybil attacks in sensor networks", In 25th IEEE International Conference on Distributed Computing Systems Workshops (ICDCS 2005 Workshops), pages 185-191, 2005.

[12] Daojing He, Sammy Chan, Shaohua Tang, and MohsenGuizani, "*Secure Data Discovery and Dissemination based on Hash Tree for Wireless Sensor Networks*", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS,VOL. 12, NO. 9, SEPTEMBER 2013.

[13] RiteshMaheshwari, JieGao and Samir R Das, *"Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information*",INFOCOM 2007. 26th IEEE International Conference on Computer Communications May 2007.

[14] Chalermek Intanagonwiwat, Ramesh Govindan, and Deborah Estrin." Directed diffusion: A scalable and robust communication paradigm for sensor networks", .In Proceedings of the Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 2000), pages 56–67, Boston, MA, USA, August 2000. ACM Press.

[15] F. Ye et al., "*A Two-Tier Data Dissemination Model for Large-Scale Wireless Sensor Networks,"* Proc. ACM/IEEE MOBICOM, 2002.

[16] Xu Cheng Feng Wang Jiangchuan Liu, "*Hybrid PUSH-PULL for Data Diffusion in Sensor Networks without Location Information*", IEEE communication society , ICC proceedings , 2008

[17] Xin Liu, Qingfeng Huang and Ying Zhang, *"Balancing Push and Pull for Efficient Information Discovery in Large-Scale Sensor Networks*", IEEE Transactions on Mobile Computing, vol. 6, No. 3, March 2007

[18] Seungmin Oh, YongbinYim, Jeongcheol Lee, Hosung Park, and Sang-Ha Kim, *" Real-Time Data Dissemination for Slowly-varying Mobile Sinks in Wireless Sensor Networks*", IEEE 24th International Symposium on personal, indoor and mobile radio communication: Mobile and Wireless networks, 2013.

[19] Leijun Huang and SanjeevSetia, *"CORD: Energy-efficient Reliable Bulk Data Dissemination in Sensor Networks*", 26th IEEE international conference on advanced information networking and applications, 2012.

[20] A.SenthilKumar,S.Velmurugan,E.Logashanmugam*." A secure distributed data discovery and dissemination in wireless sensor networks*", International Journal of Engineering & Science Research, ISSN 2277-2685 Vol-5,Issue-7,708-713, July 2015