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
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 7, July 2016, pg.36 – 43

EFFICIENT TRANSMISSION IN WIRELESS SENSOR NETWORK USING ABS TECHNIQUE

Navpreet Kaur Thind[1], Er. Puneet Kumar[2], Dr. Rachit Garg[3]
[1]Student, M-tech (CSE), SSCET, Amritsar, Punjab, India
[2]Assistant Professor (CSE), SSCET, Amritsar, Punjab, India
[3]Principal, SSCET, Amritsar, Punjab, India
navpreetthind14@gmail.com, *puneetsrisai@gmail.com*

Abstract— In wireless sensor networks (WSNs), it is often necessary to update the software running on sensors, which requires reliable dissemination of large data objects to each sensor with energy efficiency. During data dissemination, due to sleep scheduling designed for energy efficiency, some sensors may not receive some packets at some time slots. In the meantime, due to the unreliability of wireless communication, a sensor may not successfully receive a packet even when it is in the active mode. We proposed ABSM Approach for efficient data transmission.

Keywords— WSN, AODV, RREP, RREQ, DIP

I. INTRODUCTION

WSN has become an emerging field in research and development due to the large number of applications that can become significantly beneficial from such systems and has led to the development of cost effective, not-reusable, tiny, cheap and self-contained battery powered computers These sensor nodes can accept input from an attached sensor and process the input data gathered from the sensor nodes. After that the process data wirelessly transmits the results to transit network. WSNs are highly dispersed networks of lightweight and small wireless nodes, deployed in huge numbers, to monitor the system or environment by the measurement of physical parameters like pressure, temperature, or relative humidity. [11]

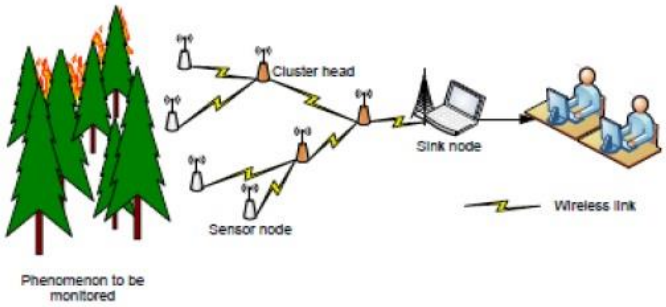

Figure 1.1 Architecture of a Typical WSN

Fig1.WSN ARCHITECTURE

II. DATA DISSEMINATION PROTOCOLS IN WIRELESS SENSOR NETWORKS

Drip: Drip is the dissemination protocol that is used in WSN. Drip is the simplest of all dissemination protocols and is based on Trickle algorithm and establishes an independent trickle or each variable in the data. Every time an application wants to transmit a 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. Drip provides a standard message reception interface in WSN. Each node that wishes to use Drip will register with a specific identifier, which represents a dissemination Routing-Based Communication channel. All messages received on that channel will be delivered directly to the node. Each node is also responsible for caching the data extracted from the recent message received on each channel to which it subscribes, and returning it in response to periodic rebroadcast requests. Drip achieves great efficiency by avoiding redundant transmissions if the same information has already been received by the nodes in the neighborhood. [13]

*Code Drip***:** This protocol is mainly used for dissemination of small values. Network Coding is a mechanism that combines packets in the network thus increasing the throughput and decreasing number of messages transmitted. Code Drip uses Network Coding to improve reliability, and speed of dissemination. Rather than simply retransmitting received data packets, sensor nodes try to combine various packets of small data items into one, and re-transmit the combined packet to its neighbors. Thus, packet loss is avoided since lost packets might be recovered through the decoding of others combined packets. By avoiding of frequent retransmissions, the dissemination process finishes faster. [13]

Dip: It is a protocol based on the Trickle algorithm. It works in two parts: detecting whether a difference in data in nodes has occurred, and identifying which data item is different. It uses the concept of version number and keys for each data item. In the steady state all nodes are up to date and have the same versions. DIP uses Trickle to calculate and send hashes that cover all of the version numbers. Nodes that receive hashes which are the same as their own know they have consistent data write their neighbors. If a node hears a hash that differs from its own, it knows that a difference exists, but does not know which data item has a newer version. Identifying which data item is different and which node has the newer version requires exchanging of the actual version numbers. [13]

*DHV***:** It tries to keep codes on different nodes in a WSN consistent and up to date. Here 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. Deluge: Deluge which is a reliable data dissemination protocol for propagating large data objects (by dividing those to fixed sized pages) from one source node to other nodes over a multi-hop, wireless sensor network. Dissemination of large data objects i.e. program images poses many issues like large size of programs, toleration of varying node densities and ensuring complete reliability in transfer etc. Deluge achieves reliability in unpredictable wireless environments and robustness when node densities can vary by factors of a thousand or more. This protocol is based on Trickle algorithm. Here each node follows a set of strictly local rules to achieve data dissemination in the network. A node at regular intervals advertises the most recent version of the data item it has to whichever nodes that can hear its broadcast. Consider B receives an advertisement from an older node A, and then B will respond with the information that it has. From the information received, A determines which portion of the data items need updating and requests them from any neighbor that advertises the availability of the needed data, including B. Nodes receiving these requests then broadcast any requested data. Thus nodes advertise newly received data in order to propagate it further to other nodes Oppress the Node Resources. [13]

Typhoon: It is mainly used for dissemination of bulky data similar to Deluge. So here also large data objects are divided into fixed sized pages and then again sub-divided into fixed sized packets. Unlike other protocols, Typhoon sends data packets in unicast fashion. This approach allows receivers to acknowledge the receipt of packets and thus quickly recover lost packets if any. While data packets are sent in unicast manner, interested nodes can receive those packets by snooping on the wireless medium. Thus through the combination of unicasting and snooping, this protocol achieves prompt retransmissions and data delivery to all the nodes in a broadcast domain through a single transmission. Typhoon uses Trickle timers for dissemination of meta-data. Here Meta data includes object ID, size and version to indicate the existence of a newly created data object. Depending on comparisons of Meta data nodes decide to accept or not accept new data objects. [13]

MNP: 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 neighborhood, 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 neighborhood. But here there can be issues of collisions. 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. To do pipelining, programs are divided into segments, each of which contains a fixed number of

packets. Once a sensor node receives all the segments of a program, it can reboot with the new program. This continues till all the nodes are hence update. [13]

III. RELATED WORK

A. Senthil Kumar et.al [1], a data discovery and dissemination protocol for wireless sensor networks (WSNs) is responsible for updating configuration parameters of, and distributing management commands to, the sensor nodes. All existing data discovery and dissemination protocols suffer from two drawbacks. First, they are based on the centralized approach; only the base station can distribute data item. Such an approach is not suitable for emergent multi-owner-multi-user WSNs. Second, those protocols were not designed with security in mind and hence adversaries can easily launch attacks to harm the network. This paper proposes the first secure and distributed data discovery and dissemination protocol named (DiDrip).

Saahirabanu et.al [2], secure reprogramming is an important issue in Wireless Sensor Networks (WSN) to suit the sensor nodes for different applications. Reprogramming is the process of uploading a new code or changing the functionality of existing code. It enables users to extend or correct functionality of a sensor network after deployment at a low cost. The mobile sink is most widely used for the sensor programming. The existing protocols are based on the centralized approach in which only the base station has the right to begin reprogramming. It is desirable for multiple authorized network users to simultaneously reprogram sensor nodes without the involvement of base station called as distributed reprogramming. Therefore the base station or the network owner can also assign

Kanchan Verma et.al [3], Wireless sensor network comprises of a set of sensor nodes that communicate among each other using wireless links and work in an open and distributed manner because of less number of resources on the nodes. The sensor nodes sense information about an event from the ambiance and then the information is forwarded to a sink node for further processing and analyzing. The sensed information can be forwarded in many ways, earlier uni cast routing was there to a single sink node, but due to the wide variety of WSN applications the presence of multiple sinks is realized which necessitates multicast routing for efficient data dissemination to multiple destinations. For any disaster surveillance or fire handling emergency scenarios various multicast routing protocols have been proposed by many researchers. This paper focuses on providing a survey of the existing multicast routing protocols by presenting approach, their advantages and disadvantages. Further a comparative study of various multicast protocols is done on the basis of different parameters to identify different issues and challenges that need to be resolved for each one of them.

Gao Weimin et.al[4], the techniques of distributed data storage in wireless senor networks. Firstly, the challenge and the need for such techniques were summarized; Secondly, some representative distributed data storage and retrieval schemes were introduced in detail; finally, the future research directions and open issues were pointed out.

Sneha Ghormare et.al [5], In Wireless Sensor Network, the security of data and confidentiality of data is an important aspect. Hence the data cannot be interrupted by the intruder. For updating configuration parameters and distributing management commands, data discovery and dissemination protocol for wireless sensor network is responsible. But, it has drawback is that, some protocols were not designed with security. For this reason, The DiDrip protocol i.e. first secure and distributed data discovery and dissemination protocol is proposed. The main function of this protocol is for authorized multiple network user. So, with the help of different security parameters the system provides a high security to the wireless sensor network. Energy efficient new algorithm is also used because it is difficult to crack.

IV. PROPOSED SOLUTION

In the Proposed Technique through multi-hop data forwarding techniques, the main task of the route discovery process is to Determine a set of intermediate nodes that should be selected to construct several paths from the source nodes towards the sink node. Different parameters are used in the existing multipath routing protocols to make routing decisions. Among these parameters, the amount of path disjointedness is the main criterion which is utilized by all the existing multipath routing protocols to discover several paths from each sensor node towards the sink node Once a set of paths are selected among the discovered paths, the multipath routing protocol should determine how to distribute network traffic over the selected paths. Based on the primary motivation behind the design of different multipath routing protocols they may utilize various traffic allocation mechanisms. For instance, transmission reliability can be guaranteed by introducing a certain degree of data redundancy in the data delivery process based on the reliability requirement of the underlying application..

Proposed algorithm:-

PROPOSED ALGORITHM

In our proposed Algorithm. The complete distributed system like WSN can Transmit information efficiently, the need for efficient algorithms to select servers according to the

Step 1: Generate WSN scenario using NS2

Step 2: Start with some initial elements like no of nodes neighbor node, Base Station. Doctor

Step 3: Initialize with n no. of nodes.

Step 4: Implement ABSM technique.

Step 5: initially Start ABSM algorithm for efficient resource switching Technique

Step 6: In ABSM if any base station will stop working another available base station will be used for transmission

Step 7: Then finally With ABSM Algorithm secure transmission will be formed.

Step 8: This process continuation until the efficient and secure transmission is formed.

Step 9: This process continuation until the efficient path is formed in network.

V. RESULT AND ANALYSIS

End to end delay: The end to end delay is total alive data packets from the sources to the destinations.

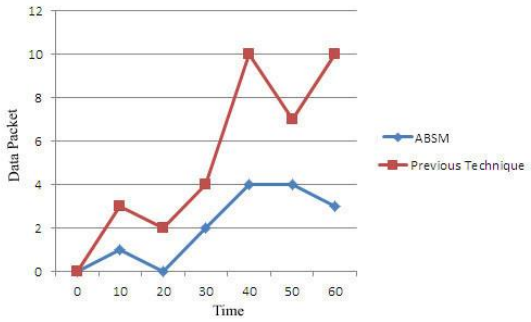

Fig2.end-to-end delay comparison

The fig2. shows the ABSM has less end-to-end delay as compared to previous technique

Packet Delivery Ratio: It is the ratio of the number .of Packets received successfully and the total number of packets transmitted.

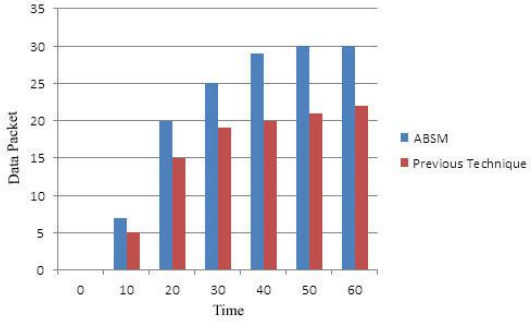

Fig3. Energy consumption comparison

The fig3. shows the ABSM has more Packet delivery ratio as compared to previous technique

Energy Consumption:

It is defined as the Energy consumed at a particular point of time.

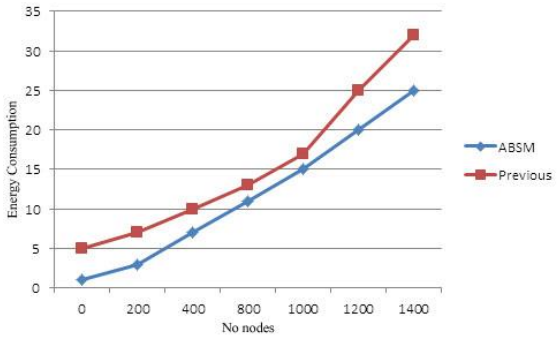

Fig4 Energy consumption comparison

The fig4. shows the ABSM has less Energy Consumption compared to previous technique

VI. CONCLUSION

WSNs are highly dispersed networks of lightweight and small wireless nodes, deployed in huge numbers, to monitor the system or environment by the Measurement of physical parameters like Pressure, temperature, or relative Humidity. In existing model, only base station receives information from sensors. They did not provide any information about the base station and their location. So, we proposed a mechanism which provides two way communications. It sends and receives data from base station.

REFERENCES

[1] A. Senthil Kumar, S.Velmurugan, Dr. E. Logashanmugam (2015), "A Secure Distributed Data Discovery and Dissemination in Wireless Sensor Networks" International Journal of Engineering & Science Research, vol. 5

[2] Saahirabanu Ahamed and Ananthi Sheshasaayee(2015),"Secure Localized Sensor Reprogramming Protocol With Mobile Sink For Wireless Sensor Networks" Middle-East Journal of Scientific Research, pp 1293-1299

[3] Kanchan Verma (2015), "Multicast Routing Protocols for Wireless Sensor Networks: A comparative study" International Journal of Computer Science and Innovation, pp 39-52

[4] Gao Weimin and Zhu Lingzhi (2015), "Distributed Data Storage in Wireless Sensor Networks" International Journal of Database Theory and Application, vol.8

[5] Sneha Ghormare ,Vaishali Saharel, Anil Jaiswal (2015), "A Survey on Data Confidentiality for Providing High Security in Wireless Sensor Network" International Journal of Advanced Research in Computer Science and Software Engineering, vol.5

[6] Jisha Mary Jose, Jomina John 2014, "Secure Data Dissemination Protocol In Wireless Sensor networks Using Xor Network Coding" International Journal of Research in Engineering and Technology, vol.3

[7] Ms. V. Savitha M.E., Mr. E.U. Iniyan M.E., Ms. M. D. Dafny Lydia(2014), "Small Data Dissipation Using Se-Drip –An Enhanced Version of Drip" International Journal of Engineering Trends and Technology,vol.18

[8] Daojing He, Sammy Chan, Yan Zhang, and Haomiao Yang (2014), "Lightweight and Confidential Data Discovery and Dissemination for Wireless Body Area Networks" IEEE Journal of Biomedical and Health Information, vol.18

[9] Ali Bagherinia, Akbar Bemana, Sohrab Hojjatkhah, Ali Jouharpour (2014), "A Key Management Approach for Wireless sensor Network" International Journal of Information Technology, Modeling and Computing, vol. 2

[10] Jin Wang, Bo Tang, Zhongqi Zhang, Jian Shen, Jeong-Uk Kim (2014), Energy Efficient Data Dissemination Algorithm for Wireless Sensor Networks" Advanced Science and Technology Letters, vol. 48

[11] Muhammad Umar Aftab, Omair Ashraf, Muhammad Irfan, Muhammad Maji, Amna Nisar, Muhammad Asif Habib (2015),A Review Study of Wireless Sensor Networks and Its Security", pp 172-179

[12] Pardeep Kaur, Vinay Bhardwaj (2015), "Wireless Sensor Networks: A Survey" International Journal of Advanced Research in Computer Science and Software Engineering, vol.5

[13] Jisha Mary Jose, Jomina John (2014), "Data Dissemination Protocols in Wireless Sensor Networks-a Survey"International Journal of Advanced Research in Computer and Communication Engineering, vol.3

