VOL. 14, NO. 4, FEBRUARY 2019 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

A MULTI-PATH BASED DATA AGGREGATION SCHEME FOR WI-MAX

G. Rama Subba Reddy and S. Balaji
Department of Computer Science and Engineering, Sunrise University, Alwar, Rajasthan, India
Email: balkiparu@gmail.com

ABSTRACT

Wi-MAX is the developing broadband wireless advancements in light of IEEE 802.16 gauges. Data aggregation, an essential paradigm for wireless routing in sensor networks aim to combine the data coming from different sources. Data aggregation can likewise kill excess, limit the quantity of transmissions and subsequently spare the energy. The goal of Data aggregation is to diminish the required correspondence at different levels, thus as to lessen the aggregate energy utilization. When energy consumption for aggregation is less than energy consumption for raw data transmission to the upper level, data aggregation saves energy. In this paper, we propose MS-LEACH Homogenous Multi-path data aggregation scheme is used. It combines multihop and single hop. It reduces the energy consumption by amalgamating between single-hop and multi-hop transmission nodes. But it has limited scalability and extra overhead.

Keywords: wi-max, data aggregation, homogenous multipath, MS-LEACH.

1. INTRODUCTION

Regardless of the difficulties confronted when transmitting information through changing remote channels, broadband metropolitan region remote frameworks are turning into a reality, somewhat on account of the inexorably refined outlines that are being utilized. Such outlines have been made conceivable by hypothetical advances and furthermore by enhancements in innovation that have prompted speedier and less expensive executions contrasted with more established frameworks. As of now, the emphasis is on creating 4G frameworks in the structure of IMT - Advanced [1], an ITU stage on which the up and coming era of remote frameworks will be fabricated. Broadband Wireless innovation has moved toward becoming life line of individuals of the world as of late. The Worldwide Interoperability for Microwave Access (Wi-MAX) is the main broadband remote innovation. Wi-MAX is the alterative and the best alternative in practically identical to Digital Subscriber Line (DSL), which convey broadband over wound match phone wires, and link modem innovation ,which conveys over coaxial satellite TV plant, are the predominant mass market broadband get to advances today [1]. Since the Wi-MAX innovation is to be conveyed as broadband remote metropolitan range systems, IEEE 802.16 standard family is additionally called Wireless MAN [2].

Wi-MAX [1] is a remote system that has a high class set of elements with a considerable measure of adaptability in wording separates it from other metropolitan region remote get to innovations are: 1. OFDM-based physical layer, 2. High pinnacle information rates, 3. Versatile transmission capacity and information rate bolster, 4. Adaptive modulation and coding (AMC), 5. Connection layer retransmissions, 6.Support for TDD and FDD, 7. Orthogonal frequency division multiple access (OFDMA), 8. Adaptable and dynamic per client asset distribution, 9. Support for cutting edge receiving wire procedures, 10. Nature of-benefit bolster, 11. Strong security, 12. Support for versatility, 13. IP-based engineering.

"Data aggregation" is a procedure of amassing the sensor information utilizing collection approaches. These methodologies utilizes the sensor information from the sensor hubs and after that totals the information by utilizing some total calculations, for example, brought together methodologies like LEACH (low energy adaptive clustering hierarchy), TAG, Directed Diffusion [3] [4]. The information amassed is exchange to the versatile sink hub by choosing the effective way. The most famous information conglomeration calculations are bunch based information collection calculations, in which the hubs are assembled into groups and each group comprises of a cluster head (CH) and a few individuals. Every part transmits the detected information to its CH, and afterward each CH totals the gathered information and transmits the information to BS. The group based WSNs have a natural issue of unequal vitality dispersal. A few hubs deplete their vitality quicker than others and result in prior disappointment of system.

The most commanding variable for devouring valuable vitality of WSNs is correspondence, i.e., transmitting and accepting messages. Along these lines, decreasing era of superfluous traffics in WSNs improves their lifetime. Moreover, including whatever number sensor hubs as could reasonably be expected amid information accumulations by the sink hub can use most extreme assets of each sensor hub. Accordingly, an antagonistic situation won't occur in a WSN in which the sensor hubs nearer to the sink come up short on vitality sooner than different hubs and the system loses its administration capacity, paying little respect to a lot of lingering vitality of the other sensor hubs.

Since correspondence is in charge of the greater part of the power utilization, many steering plans in WSN are precisely intended to give exceedingly productive interchanges among the sensor hubs [9]. Among them, information driven plans are extremely mainstream where information transmissions depend on their insight about the neighboring hubs. Directed Diffusion (DD) [10] and Hierarchical Data Aggregation (HDA) [11] plans are two delegate information driven plans.

A standard idea of regular information gathering plans is that they gather information by a sink hub from sensor hubs and exchange information towards the sink hub through multi-bounce. In any case, it offers ascend to two issues. The first is the hotspot issue, in which the sensor hubs nearer to the sink come up short on vitality sooner than different hubs. Thus, organize loses its administration capacity paying little mind to a lot of leftover vitality of alternate hubs. The second one is that system creates pointless traffics amid information transmission for picking a legitimate way to send information.

2. RELATED WORK

Software protection is a standout amongst the most LEACH (Low-Energy Adaptive Clustering Hierarchy) [5] is a cluster based protocol. It is one of the principal progressive directing methodologies for sensor systems. Drain haphazardly chooses hubs as group heads and turns this part among all sensor hubs to adjust the heap in the system. Each bunch head gets information as indicated by a TDMA space and pack the information before conveying it to the base station. Filter permits building single jump bunch and consequently prompts huge number of groups causing awesome vitality utilization of correspondences. It gives break even with likelihood for hubs to end up group heads however it doesn't consider the remaining vitality and area of the hubs.

V-LEACH [6] - it is another variant of LEACH convention. Each group has two cluster heads (CH). Fundamental CH is in charge of sending accumulated information to the BS and the Vice CH is in charge of social event information from group individuals. In the event that the fundamental CH kicks the bucket the Vice-CH will progress toward becoming bunch head. In any case, it is pointless to choose a substitute group head.

Arivazhagan *et al*, [15] consequently specifically concentrate on dynamic connectivity management, which we extensively define as the capacity to alertly oversee how and where traffic flows over a system. Since it is personally included with how traffic flows through the system, Multiprotocol Border Gateway Protocol (MBGP) would be a perfect contender for a significant number of these administration undertakings.

A novel grouping in light of K-implies [7] calculation is utilized to shape the bunches in view of Euclidean separations between hubs. It chooses k-hubs haphazardly as group heads. Hubs choose its CH close to it as indicated by the Euclidean separation. Presently the centroid of the group is ascertained. A hub which is close to the centroid will be taken as new group head and after that it does re bunching in light of the new group head. This approach limits the vitality expended for the sensor hubs to send information to the CH. And furthermore the power utilization of CH is additionally less. Be that as it may, this K-implies approach invests more often than not in bunching and re grouping and along these lines prompts more prominent vitality utilization. And furthermore it frames the groups in light of position of the hubs and consequently prompts many bunches.

"Balanced Clustering Algorithm with Distributed Self- Organization" (DSBCA) [12] - A heap adjusted bunching calculation bargains the stochastic dispersion of sensor hubs. It creates adjusted groups. The group sweep can be dictated by thickness and the separation from the base station. With more remote separation from the base station and lower availability thickness the group span is bigger. Every part in the bunch computes its weight and a hub with higher weight is taken as CH. Weight is a measure of leftover vitality, number of neighbors and the quantity of times the hub was chosen as CH. It makes unequal groups. DSBCA additionally restricts the quantity of hubs in a group. The downside of this calculation is that it devours more vitality for correspondence and furthermore it requires greater investment for figuring weight amid bunch head choice.

"Data-Aware Anycast and Randomized Waiting protocol" (DAARW) [8] is the first sans structure information total plan for occasion driven detailing in sensor systems. Since there is no settled information gathering structure, every hub with occasion information to report sends an anycast RTS first to decide the following jump to the sink. Any hub that gets this RTS is a next bounce applicant. To accomplish more prominent total efficiency, a hub that has similar occasion information to report or is nearer to the sink has higher need to react CTS. To decrease the quantity of transmissions, a randomized holding up conspire is presented. Every hub that has information to report can begin its transmission after an irregular holding up time. Conceivable conglomeration is created when a hub near the sink picks a more drawn out holding up time. The fundamental preferred standpoint of DAARW is that it maintains a strategic distance from structure support overhead. In any case, the randomized sitting tight time system leaves spaces for development, as total efficiency will be poor if hubs that are nearer to the sink have chosen shorter holding up times.

GS-LEACH [14] was proposed as one of LEACH families so as to take care of issues of SecLEACH. In SecLEACH, ordinary hubs need to choose an aggregator, which has a common key with typical hubs. In the event that the closest aggregator does not have a common key, a typical hub must choose a next aggregator. Likewise, if an aggregator having shared key does not exist, an ordinary hub need to transmit straightforwardly to BS despite the fact that much vitality is required for transmission.

S-LEACH [13] is the principal adjusted adaptation of LEACH with cryptographic security against pariah assaults. The calculation is depicted in Figure-1. It proposes that every hub needs to have two symmetric keys, a pairwise key imparted to BS and the last key chain held by BS. For the setup stage, the message sent by CHs should comprise of ID of CH in plaintext, as earlier; and the encoded type of (ID of CH, the counter shared by CH and BS, and the commercial message) utilizing message authentication code (MAC) that is created utilizing the mutual key amongst CH and BS.

Setup phase

1. 1 $H \Rightarrow \mathcal{G}$: $id_H, mac_{k_H}(id_H||c_H||\text{sec\_}adv)$, **sec_adv**
   A_i : store(id_H)
   BS : if $mac_{k_H}(id_H||c_H||\text{sec\_}adv)$ is valid, add (id_H, V)
1. 2 $BS \Rightarrow \mathcal{G}$: $V, mac_{k_{j-1}}(V)$
1. 3 $BS \Rightarrow \mathcal{G}$: k_{j-1}
   A_i : if $\left(f(k_{j-1}) = k_j\right) and\ (id_H \in V)$, id_H is authentic
2. $A_i \rightarrow H$: id_{A_i}, id_H, **join_req**
3. $H \Rightarrow \mathcal{G}$: $id_H, (\ldots, \langle id_{A_i}, t_{A_i}\rangle, \ldots)$, **sched**

Steady-state phase

4. $A_i \rightarrow H$: $id_{A_i}, d_{A_i}, mac_{k_{A_i}}(id_{A_i}||c_{A_i})$
5. 1. $H \rightarrow BS$: $id_H, \mathcal{F}(\ldots, d_{A_i}, \ldots), mac_{k_H}(id_H||\mathcal{F}(\ldots, d_{A_i}, \ldots)||c_H)$
5. 2. $H \rightarrow BS$: $id_H, \left(\ldots, id_{A_i}, mac_{k_{A_i}}(id_{A_i}||c_{A_i})\ldots\right), mac_{k_H}(id_H||c_H)$, **mac_array**
6. $BS \rightarrow H$: intruder ids

Figure-1. S-LEACH protocol.

3. PROPOSED SYSTEM ARCHITECTURE

The proposed framework engineering is appeared in the Figure-2. It contains a solitary base station and various sensors. The sensors are composed into bunches and each group has a bunch head. It is a layered approach and the bunches in layer1 frames group1 and groups in layer2 shapes group2 et cetera.

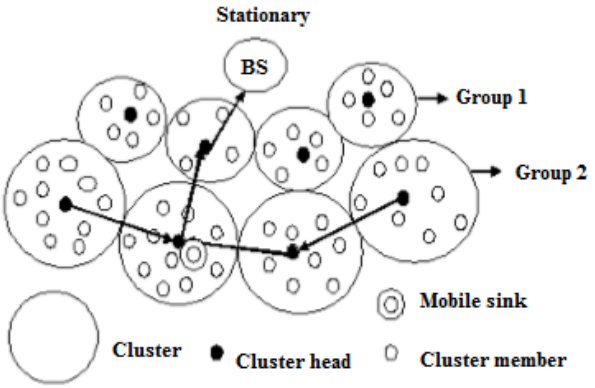

Figure-2. System architecture.

3.1 Data aggregation

Data aggregation is the way toward getting the data from the sensors. Bunch Head readies a TDMA space for its individuals and gathers information as indicated by that. A portable sink hub lands at any of the CH of the nth gathering. It at that point communicates data_request to different CHs of a similar gathering. Portable sink merge the information and finds the best k information. This best k set is engendered to (n-1)th gathering. There again it performs dsts gathering and total with top-k set. Along these lines it conveys the best most dataset to the stationary BS. In the middle of if any CH distinguishes any noteworthy occasion that will be instantly told to the stationary BS independent of the position of versatile sink hub.

Steps:

Step 1. Move the mobile sink node to any of the CH of nth group.
Step 2. Sink node Broadcasts data_request to other CHs of same group.
Step 3. Eliminate duplicate values and perform intra group aggregation.
Find top-k set
Step 4. Move the mobile sink down to (n-1) th group.
Step 5. Repeat step 2 and perform inter group aggregation. Find the new top-k set.
Step 6. Repeat steps 2 to 5 until reach the stationary sink node

3.2 MS-LEACH

MS-LEACH was proposed to improve the security of SLEACH by giving information privacy and hub to-CH confirmation utilizing pair wise keys shared among hubs.

Setup phase

1. 1 $H \Rightarrow \mathcal{G}$: $id_H, mac_{K_H}(id_H||c||\textbf{sec\_}\boldsymbol{adv})$
   A_i : store(id_H)
   BS : if $mac_{K_H}(id_H||c||\textbf{sec\_}\boldsymbol{adv})$ is valid $add(id_H, V)$
1. 2 $BS \Rightarrow \mathcal{G}$: $V, mac_{k_{j-1}}(V)$
1. 3 $BS \Rightarrow \mathcal{G}$: k_{j-1}
   A_i : if $f(k_{j-1} = k_j)$ and $(id_H \in V)$, id_H is authentic
2. $A_i \rightarrow H$: id_{A_i}, id_H, **join_req**
3. H and A_i : $K_{A_i} = f_{KI}(id_{A_i})$
   $K_{HA_i} = f_{K_{A_i}}(id_H)$
4. $H \rightarrow A_i$: $E_{K_{HA_i},C}(id_H, id_{A_i}, T_{A_i}, \textbf{sched}), mac_{K_{HA_i}}\left(c||E_{K_{HA_i},C}(id_H, id_{A_i}, T_{A_i}, \textbf{sched})\right)$

Steady-state phase

5. $A_i \rightarrow H$: $E_{K_{HA_i},C}(id_{A_i}, d_{A_i}), mac_{K_{HA_i}}\left(c||E_{K_{HA_i},C}(id_{A_i}, d_{A_i})\right)$
6. $H \rightarrow BS$: $E_{K_H,C}\left(id_H, \mathcal{F}(\ldots, d_{A_i}, \ldots)\right), mac_{K_H}\left(c||E_{K_H,C}\left(id_H, \mathcal{F}(\ldots, d_{A_i}, \ldots)\right)\right)$

Figure-3. MS-LEACH protocol.

Additional symbols denote:

c - Counter
KI - The symmetric last key chain held by BS preloaded in each node
fK - A family of pseudo-random function.

Figure-3 demonstrates the protocol. Step 1 and 2 are like SLEACH. In step 3, pairwise keys are created between the CH and its part hubs. In step 4, the CH unicasts a TDMA plan sched scrambled with the pairwise key and a counter to every part alongside the MAC of the

counter and the encoded type of the TDMA plan figured with the pairwise key sent. In consistent state stage, each part sends the encoded type of its estimation information and id ascertained utilizing the pairwise key and counter an incentive to the CH alongside the MAC estimation of the counter and the scrambled type of the hub's id and its estimation information computed additionally utilizing the pairwise key. In step 6, the CH scrambles its id and accumulated information utilizing the key KH and counters imparted to BS and furthermore register MAC of counter and the encoded message utilizing KH. At that point it sends the encoded back rub and MAC to BS.

4. CONCLUSIONS

Energy efficiency is a vital issue in remote sensor systems. Vitality effectiveness of grouping based plans for remote sensor systems relies on bunch head determination and appropriate total. In this paper we have displayed an effective group head choice plan that makes organize work for a more extended era. This paper proposes MS-LEACH, an altered variant of S-LEACH that improves the security of unique S-LEACH by giving information privacy and hub CH verification. Proposed MS-LEACH utilized Blowfish calculation as its cryptographic capacity for its effectiveness over RC5 that is utilized as a part of S-LEACH.

REFERENCES

[1] G. Jeffrey, G. Arunabha and M. Rias. 2007. Fundamentals of WiMax. E-book Prentice Hall Kindle 1st edition 27 February.

[2] Mingxi Wang - WiMAX Physical Layer: Specifications Overview and Performance Evaluation, 2nd IEEE CCNC Research Student Workshop.

[3] Nandini. S. Patil, Prof. P. R. Patil. 2010. Data Aggregation in Wireless Sensor Network. IEEE International Conference on Computational Intelligence and Computing Research.

[4] Xuxun Liu. 2012. A Survey on Clustering Routing Protocols in Wireless Sensor Networks. Sensors 2012, doi: 10.3390/s120811113.

[5] Heinzelman. W.R, A. P. Chandrakasan, H. Balakrishnan. 2000. Energy-efficient communication protocol for wireless micro sensor networks. In Proc. 33rd Annu. Hawaii Int. Conf. Syst. Sci., Jan. pp. 1-10.

[6] Mrs. Asha Ahlawat, Ms Vineeta Malik. 2013. An extended vice cluster selection approach to improve V-leach protocol in WSN. 3rd international conference on advanced computing and communication technologies. IEEE.

[7] Geon Yong Park. 2013. A Novel Cluster Head Selection Method based on K-Means Algorithm for Energy Efficient Wireless Sensor Network. Waina, pp. 910-915, 2013 27th International Conference on Advanced Information Networking and Applications Workshops.

[8] Ying Liao, Huan Qi, Weiqun Li. 2013. Load-Balanced Clustering Algorithm with Distributed Self-Organization for Wireless Sensor Networks. IEEE sensors journal. 13(5).

[9] Heinzelman W-R.; Kulik J. & Balakrishman H. 1999. Adaptive protocols for information dissemination in wireless sensor networks, In Proceedings of MOBICOM, pp. 174-185.

[10] Itanagonwiwat C.; Govindan R. & Estrin D. 2002. Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks. In Proceedings of MOBICOM. pp. 56-67.

[11] Zhou B.; Ngoh L. H.; Lee B. S. & Fu, C-P. 2006. HDA: A hierarchical Data Aggregation Scheme for Sensor Networks. Computer Communication. 29: 1292-1299.

[12] K.-W. Fan, S. Liu and P. Sinha. 2007. Structure-Free Data Aggregation in Sensor Networks. IEEE Transactions on Mobile Computing. 6(8): 929-942.

[13] A. C. Ferreira, M. A. Vilac a, L. B. Oliveira, E. Habib, H.C. Wong and A.A. F. Loureiro. 2005. On the Security of Cluster-Based Communication Protocols for Wireless Sensor Networks. In 4th IEEE International Conference on Networking (ICN.05), 3420 of Lecture Notes in Computer Science, Reunion Island. pp. 449.458.

[14] P. Banerjee, D. Jacobson, and S. N. Lahiri. 2007. Security and Performance Analysis of a Secure Clustering Protocol for Sensor Networks. In (NCA 2007), Proceedings of 6th IEEE International Symposium on Network Computing and Applications.

[15] P. Arivazhagan, S. Balakrishnan, K.L. Shunmuganathan. 2016. An Agent Based Centralized Router with Dynamic Connection Management Scheme Using JADE. International Journal of Applied Engineering Research, ISSN 0973-4562, 11(3): 2036-2041.