ARPE : An Attack-Resilient and Power Efficient Multihop WiMAX Network

M. Deva Priya
Department of CSE,
Manakula Vinayagar Institute of Technology,
Puducherry, India.
mail2devapriya@gmail.com

J.Sengathir
Department of CSE,
Manakula Vinayagar Institute of Technology,
Puducherry, India.
j.sengathir@gmail.com

Dr.M.L Valarmathi
Department of CSE,
Government College of Technology,
Coimbatore , Tamil Nadu - 641 013, India.
ml_valarmathi@rediffmail.com

Abstract- **IEEE 802.16 standard known as WiMAX (Worldwide Interoperability for Microwave Access), is one of the most promising wireless access technology for next generation all-IP networks. The fundamental requirements for WiMAX to define itself as a possible winning technology are data reliability and the ability to deliver multimedia contents. WiMAX networks face all the problems related to hostile wireless environment, where power constraints make it difficult to provide hard QoS guarantees. This paper addresses the main issues of security and power efficiency, proposing an efficient cross-layered approach for data transmission. Direct transmission consumes more energy. Multihop communication involves formation of groups, where group heads aggregate the data before transmitting it to the Base Station. It uses Chessboard clustering algorithm to perform clustering. If a group head is compromised, then the Base Station cannot ensure the correctness of the data sent to it. A group head is selected at random for forwarding the aggregate. Hence, this paper proposes a novel mechanism for the Base Station to ensure the correctness of the data sent to it.**

Keywords - Data aggregation, Direct Voting, Witness-Based Approach, Clustering, Indirect Anti-voting.

I. INTRODUCTION

IEEE 802.16, also called WiMAX was developed to accommodate large coverage and high bandwidth last-mile Internet access. Indeed, the provision of QoS guarantees will be a pressing need in the next generation of Internet, in order to enable the introduction of novel broadband multimedia applications. Even if the deployment and the use of this standard has started, the use of WiMAX networks is still limited to particular situations. It represents an emerging research area, providing useful applications in various fields such as habitat monitoring, battlefield surveillance and forest fire monitoring. In fact, WiMAX technology allows reaching high bit rate and covering large areas with a single Base Station (BS). It gives the operators the possibility to offer connectivity to end users in a cost effective way. It delivers 70 Mb/s over 30 miles theoretically. It supports multi-class services and guarantees the QoS requirements of delay-bounded services [2]. Users are getting more and more interested in broadband applications (e.g., video streaming, video conferencing, online gaming etc.) that require assurances in terms of throughput, packet delay and jitter to perform well [3].

WiMAX solutions are highly deployable. So the initial response team can set up a temporary wireless network at the site of the accident, event or natural disaster in a matter of minutes. They can also relay traffic from this network back to a control or dispatch center over an existing WiMAX network. The 802.16 standard specifies two modes for sharing the wireless medium: Point-to-Multipoint (PMP) and Mesh (optional). In the PMP mode, the nodes are organized into a cellular-like structure, where a Base Station (BS) serves a set of Subscriber Stations (SSs) within the same antenna sector in a broadcast manner, with all SSs receiving the same transmission from the BS. Transmissions from SSs are directed to and coordinated by the BS. On the other hand, in Mesh mode, the nodes are organized adhoc and scheduling is distributed among them [1]. In this paper PMP mode of communication is used. To conserve power, the Base Station and the nodes very far away, do not communicate directly.

While the Base Station can have continuous, unlimited power supply, other nodes usually have limited power supply and are battery-powered. It is inconvenient to replace them once they are deployed. Sometimes, replacement is even impossible. Thus, energy efficiency is a critical design consideration of WiMAX networks. Communication is a dominant source of energy consumption. Security is one of the main barriers and is crucial to wide-scale deployment of WiMAX networks, but has gained little attention so far. Once a node has been compromised, the security of the network degrades quickly if no measures are taken to deal with this event.

II.ISSUES

There are various issues to be considered. They are discussed below.

A. Security

The necessity for security in large-scale WiMAX networks can be best illustrated by the following example. Suppose a person wishes to retrieve some important documents from his corporate network back in one place via a local WiMAX network in another place, where he is on a business stay. The serving WiMAX network has to corroborate the identity of a person to avert fraudulent use of network resources; on the other hand, a person might as well want to authenticate the serving WiMAX networks to prevent an attacker from impersonating a legitimate WiMAX Network to obtain confidential information from him. Other security concerns may include the location privacy of a person, passive eavesdropping, denial-of-service (DoS) attacks, and so forth. [4]. In some critical applications like Battlefields, the information transferred is of high importance. If the information is modified, misused or not transferred, then the Base Station has to ensure the correctness of the information sent to it.

B. Power

Efficient management of the wireless network is crucial to extend the life of the system. Nodes' energy cannot support long haul communication to reach a remote command site and hence they require multi-tier architecture to forward data. It is a known fact that 70% of the energy is spent in data transmission. This paper proposes a secured, fault tolerant and a power-efficient mechanism for data aggregation in a WiMAX network.

1) Data Funneling

Due to energy and other resource constraints, communication between a set of nodes to a single destination should be reduced to a minimum. Aggregation techniques are often used for secure routing and have many advantages. The Data Funneling method [14] allows the network to reduce the amount of energy spent on communication setup and control- an important concern in low data-rate communication. Instead of having an individual data stream from each node to a destination, there exists only one data stream from a group of nodes to that particular destination. Lossless compression of data is done using encoding information in the ordering of the nodes' packets, which helps in obtaining additional gains.

2) SEDAN

An efficient way to enhance the lifetime of the system is to partition the network into distinct groups with a high-energy node called gateway as group-head. SEDAN (Secure and Efficient protocol for Data Aggregation in Sensor Network), an existing approach presents a data verification procedure at all levels in a Sensor Network. This technique is applicable to a WiMAX network. But it is not energy efficient as it involves transmission overhead. It is described in the sections that follow.

III. SELECTION OF GROUP HEADS

The Data Aggregation paradigm is an essential key for the lifetime of the network due to the reduced number of broadcasts and collisions. By avoiding unnecessary transmissions, power consumption in a wireless network can be very much reduced. Data aggregation is the collection and processing of information from various nodes before transmitting it to the Base Station, thereby reducing the amount of traffic. The data from a group of nodes (referred to as groups) are collected at their corresponding group heads. The Chessboard Clustering scheme is used for Clustering sensors. The same is applied for clustering nodes in a WiMAX network. However, data aggregation is potentially vulnerable to attacks such as injecting bogus information or forging the values without being detected. This paper focuses on the integrity of the data (due to its importance) in sensing applications. The data from the group heads are transmitted to the command center (Base Station). The nodes do not communicate with one another, but the group heads can communicate with the other group heads. Thus, nodes and group heads are functionally different.

A. The Chessboard Clustering scheme

This section discusses about the uneven energy consumption (UEC) problem in sensor networks and briefly describes the chessboard clustering scheme that solves the UEC problem. The same clustering technique can be used in a WiMAX network also.

1)The UEC problem

In LEACH [6] and LRS [15] solve the uneven energy consumption problem (i.e., a cluster head consumes much more energy than a cluster member). Periodically different nodes are elected to serve as the group head.

However, these schemes suffer from the large overhead of frequent re-clustering. Further, cyclic selection of group-heads does not solve the UEC problem caused by the many-to-one traffic pattern in the network, where the nodes near the BS have much heavier communication burden than others. For example, in Fig.1, the BS is located in the left-bottom corner of the BS via multi-hops communication. Nodes within the transmission range of the BS are the critical nodes. When all the critical nodes fail, other nodes will be disconnected from the BS and the whole network becomes unavailable. The UEC problem exists no matter where the BS is located (eg., at the center)

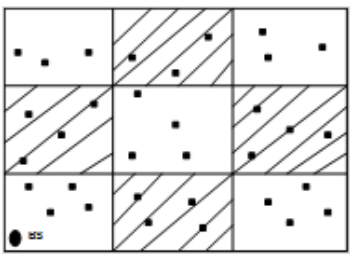

Figure 1: UEC near the BS

Clusters are formed after node deployment. It is natural to let powerful H-nodes serve as group heads. When sufficient number of H-nodes is randomly deployed in the network, there is a high probability that all H-nodes are connected and the probability goes to 1 as the number of H-nodes increases [16]. All H-nodes form a communication backbone in the network. Each L-sensor sends data to its cluster head and the cluster head forwards data to the BS via the H-node backbone. Since H-nodes have sufficient energy supply, the architecture solves the UEC problem near the BS. Unfortunately, there is another UEC problem in clustering schemes with fixed cluster heads. Consider a cluster in Fig. 2, where a node has transmission range r. The nodes that are within the circle (with radius r) from the cluster head are referred to as critical nodes. Every transmission from a node in the group to the group head has to go through one of these critical nodes. Among all the nodes in a cluster, the critical nodes have the highest burden of relaying data.

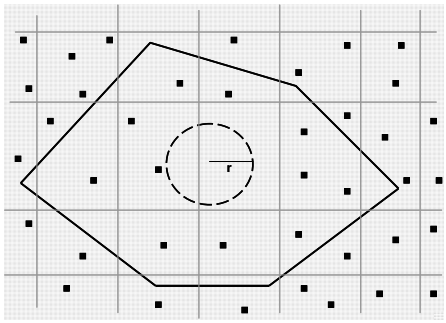

Figure 2 : Critical nodes in a cluster

Since the critical nodes have much heavier traffic load than nodes in the cluster, they run out of energy much faster than other nodes. When all critical nodes drain out their energy and become unavailable, other nodes will not be able to send packets to the cluster head and the entire cluster becomes unavailable even though the remaining energy of many sensor nodes are still high. The remaining energy in the noncritical nodes is wasted.

2)The Chessboard clustering scheme

To solve the UEC problem within a cluster, the CC scheme is proposed [17]; consider a heterogeneous network consisting of two types of nodes; a small number of powerful high-end nodes and a large number of low end nodes. Nodes can use location services as in [18, 19] to estimate their locations and a Global Positioning System (GPS) receiver is not required for each node. For simplicity, assume that the network is a two-dimensional rectangle. As illustrated in Fig. 1, the left-bottom corner of the network is the original point O and the horizontal side as the X-axis. The network is divided into several small cells and adjacent cells are filled with different colors – white or black as illustrated in Fig. 1 (where the cross-lines represent black cells). Given the point O, the direction X, the size of the cell and the node location, a sensor can determine whether it is in a white cell or a black cell.

The CC scheme includes two phases. The first phase starts after node deployment. Only H-nodes in white cells are active and H-nodes in black cells turn themselves off. All L-nodes are active. Clusters are formed around the H-nodes in white cells and L-nodes close to these H-nodes (in white cells) as the Group head and this leads to the formation of Voronoi cells wherein the group heads are the nuclei of the cells. The second phase starts when H-nodes in white cells run out of energy, H-nodes in black cells wake up and form a different set of clusters in the network. Because of the formation of two different sets of clusters during different time periods, previous non-critical L-nodes become critical nodes. Since critical nodes consume much more energy than other nodes, this switch balances the energy consumption among L-nodes and this prolongs the network lifetime.

IV. INFORMATION ASSURANCE

Clustering reduces redundancy in a network [5].Even though this data collection and processing architecture drastically relieve the communication burden on the network, the nodes conducting clustering are vulnerable to attacks. [6] Clustering or grouping is usually implemented over the network. Since the node is typically placed in locations accessible to malicious attackers, information assurance of the clustering process is very important. If a group head is compromised, it can send bogus data to the Base Station. In particular, it is to be guaranteed that if the Base Station accepts a reported fusion result from the group heads, then the reported result is “close” to the true value with high probability. Communication bandwidth is extremely dear: each bit transmitted consumes about as much power as executing 800–1000 instructions [7], and as a consequence, any message expansion caused by security mechanisms comes at a significant cost. Thus, the resource-starved nature of networks poses great challenges for security. In a network, an adversary can easily inject messages, so the receiver needs to make sure that the data used in any decision-making process, originates from the correct source. Data authentication prevents unauthorized parties from participating in the network and legitimate nodes should be able to detect messages from unauthorized nodes and reject them.

In the two-party communication case, data authentication can be achieved through a purely symmetric mechanism: The sender and the receiver share a secret key to compute a Message Authentication Code (MAC) of all communicated data. When a message with a correct MAC arrives, the receiver knows that it must have been sent by the sender. Once an incorrect MAC is detected, the report is dropped. [8]

The Group heads can combine all the local decisions, to yield the final result and directly communicate with the Base Station. Finally, one of the Group heads is chosen to send the final result to the Base Station. Unless all the Group heads or all the nodes fail, this detection and fusion scheme guarantees that the Base Station obtains the detected result. However, the accuracy of the result is not certain.

Two problems must be solved to ensure that the Base Station obtains the correct result. First, every group head must correctly fuse all the local decisions, which also implies that all the fusion results must be the same. This work assumes that this problem has been solved. The second problem is concerned with the assurance of the fusion result. The transmission between the fusion node and the Base Station is assumed herein to be error-free.

Since some Group heads may be compromised, the node chosen by the Base Station to transmit the fusion result may be one of the compromised nodes. Malicious data may be sent by the compromised node, and the Base Station cannot discover the compromised nodes from the normal Group heads, since the data detected by the nodes are not sent directly to the Base Station. Consequently, the result obtained at the Base Station may be incorrect [9].

V. EXISTING SYSTEM

In the following sections, only one group/cluster is taken into consideration. SEDAN provides hop-by-hop security. Witness based Approach and Direct Voting provide secured transfer of data between the Cluster head and the Base Station. These approaches ensure security in a WSN. The same is applicable to a WiMAX network.

A. SEDAN

SEDAN, an existing approach for providing secured transmissions is not energy efficient. The low-level nodes are the Subscribers who forward the data to the group heads. The group heads are more critical and vulnerable to malicious attacks than normal nodes. Therefore providing security at the group head is the problem to be dealt with.

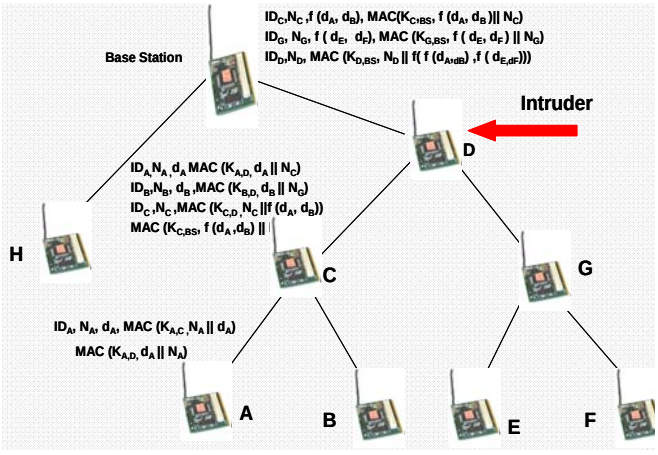

Figure 3 : SEDAN architecture

Direct transmission is a simple approach in which each node transmits its own data directly to the Base Station. However, if the Base Station is far away, the cost of sending data to it becomes too large and the nodes die quickly. Since large numbers of nodes are densely deployed, neighbor nodes may be very close to each other. Multihop communication can effectively overcome some of the signal propagation effects experienced in long-distance wireless communication. Nodes carry limited, generally irreplaceable, power sources. Therefore, while traditional networks aim to achieve high quality of service (QoS) provisions, network protocols must focus primarily on power conservation.

It involves long MACs. Even from the lower level, the nodes send their ID, data and the MAC (K_A, d_A).[10] At the next level the nodes append their data and their MAC. It is a known fact that the low-level nodes are less prone to attacks. They forward data. So the intruders are less interested in these nodes. Providing security at these nodes involve unnecessary transmission overhead.

Various methods have been proposed that deal with providing an assured data transfer from the Group heads to the Base Station. They are Witness Based Approach and Direct Voting. But these methods have various demerits. They involve unnecessary transmissions. Within a particular cell, more than one fusion nodes are present. When a particular cell is active, these nodes are alive and aggregate the data. Only one node forwards the aggregate to the next active cell.

B. Witness Based Approach

Du et al [11] used the "witness" concept to solve the assurance problem between data fusion nodes and the Base Station. Du *et al.* presented a Witness Based Approach to ensure the correctness of the fusion result. One of the fusion nodes is chosen to transmit the fusion result to the Base Station. All the other fusion nodes act as witnesses of the transmitted fusion result. Several fusion nodes are used to fuse the collected data and have the ability to communicate with the Base Station. Witnesses, encrypt the fusion results to Message Authentication Codes (MACs). The MACs are then sent to the Base Station through the chosen fusion node or the group head. Finally, the Base Station utilizes the received MACs to verify the received fusion data. A long MAC increases the reliability of the verification. However, the transmission of the long MAC imposes a high communication burden. If the received fusion result at the Base Station cannot pass the verification, then a polling scheme is started to determine whether any valid fusion result is available at the other fusion nodes.

Demerits:

- Long MAC's are an overhead
- Many copies of the fused data are sent to the Base Station.
- Not Power efficient

C. Direct Voting Mechanism

In many applications of WiMAX Network, a Sink is interested in aggregated data instead of exact values from all nodes. Sending aggregated data reduces the amount of data to be transmitted and thereby conserve energy. Indeed current in-network aggregation schemes are helpful to conserve

energy but they are designed without considering possible security issues related to data privacy. A wireless network designed with neighboring nodes shares keys. In either situation the potential for aggregator nodes to be physically compromised is high. That is data privacy is at high risk. Therefore secure data aggregation is desirable where data can be aggregated without the need for decryption at aggregator nodes. Aggregation becomes especially challenging if end-to-end privacy between a source and a destination is required. [12]

Saving energy is a very critical issue in WiMAX Network, since nodes are typically powered by batteries with a limited capacity. Since the radio is the main cause of power consumption in a node, transmission/reception of data should be limited as much as possible. Hung-Ta Pai and Yunghsiang S. Han [13] proposed a new scheme to ensure data fusion assurance. This method is better than the witness-based method. The Base Station obtains votes contributing to the transmitted fusion result directly from the witness nodes. Only one copy of the correct fusion data provided by one uncompromised fusion node is transmitted to the Base Station. No valid fusion data is available, if the transmitted fusion data are not approved by a pre-set number of witness nodes. The witness node overhears the transmitted fusion result from the chosen node. It then compares the overheard result with its own fusion result.

Finally, the witness node can transmit its vote on the overheard result directly to the Base Station, rather than through the chosen node. When a fusion node wishes to send its fusion result to the Base Station, it adopts the group key to encrypt the result, and other fusion nodes serving as witness nodes can decode the encrypted result. The witness node then starts to vote on the transmitted result. A Polling Scheme based on the voting mechanism using a public key is proposed to ensure data fusion assurance.

Demerits:

- The Polling Scheme is an overhead.
- Use of a public key is a threat to security.

VI. PROPOSED SYSTEM

Initially, this paper concentrates on the energy constraints of the nodes. Direct communications between low level nodes and the Base Station consumes more energy. Multi-hop communications involving Clusters are best suited for this scenario. Secondly, this work proposes a novel energy-conserved, fault-tolerant, intrusion-less clustering mechanism. Therefore, security at the group heads in a region is ensured. Two layers in WiMAX are involved – MAC (PS) Layer (for ensuring security) and the PHYsical Layer (for energy). Security is provided at the low-levels by using Public-key Cryptography. The procedure is explained below. (The procedure for public-key cryptography is the same as the one used for higher levels). If several copies of the fusion data are sent to the Base Station, energy required for data transmission is very high. Hence in this method, instead of sending the entire set of the fusion data, only the aggregate is transmitted to the Base Station. The proposed mechanism adopts the public-key cryptography. The method makes use of a set of keys as shown below. This can be termed as Indirect Anti-voting mechanism, as there is no direct communication between the witness nodes.

In the proposed method, a Group head is selected at random for forwarding the aggregate.

The Group head sends the data by encrypting it with the K_1, where

K_1 = private key of the Group head + public key of the Base Station (1)

Data after encryption at the sender = data from the sender ^ K_1 (2)

The Base Station receives the encrypted value, decrypts it with key K_2, where

K_2 = private key of the Base Station + public key of the Group head (3)

Data after decryption at the receiver = data at the receiver ^ K_2 (4)

- The Base Station broadcasts the aggregate value after encrypting it with a key K_2.
- The Base Station waits for Anti-Votes from the Group heads which do not accept the data.
- All the Group heads receive the encrypted aggregate value sent by the Base Station. They calculate another aggregate using the locally available fusion data and compare it with the decrypted copy of the received aggregate. Here decryption makes use of the key K_1.
- If the aggregate values differ, then the Group heads generate Anti-Votes, encrypt them with key K_1 and forward it to the Base Station.
- If there is less number of Anti-votes from the Group heads, then the Base Station requests the selected Fusion Node for real fusion result and then receives it. The system may be pre-programed to tolerate only 2 Anti-votes, if there are say only 5 Group heads. When the number of Group heads increase or the application changes (for eg: in case of military applications only less number of Anti-Votes are acceptable), the number of Anti-Votes allowed may change accordingly.

A . Credibility of the Proposed Mechanism

In the proposed mechanism, practically there will not be any need for retransmission of fusion data, until the randomly selected Cluster head is a malicious node. As the Cluster head to transmit the data is selected at random, the intruder will not be able to find out the node chosen at that particular instant. Hence the vulnerability of attacks is very much reduced. If a malicious Cluster head generates Anti-votes to invalidate the data of some other Cluster head chosen to forward the data, then it will not be considered at the Base Station, as there will not be sufficient Anti-votes from other genuine Group heads to support this node. Since a public-key system is used, a malicious Cluster head cannot forward any proxy Anti-votes also.

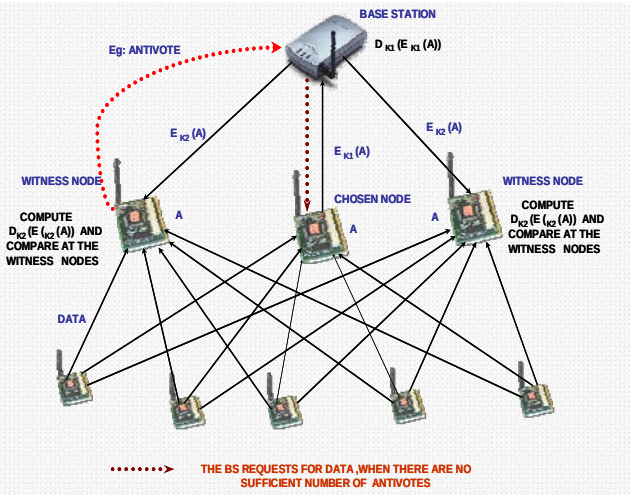

Figure 4 : Proposed system

The main merit is that the private keys are not communicated, transmitted or revealed to any other nodes. If the malicious node tries to send invalid aggregate to the Base Station, the Base Station receives a lot of Anti-Votes from other genuine Group heads and rejects the malicious node. The malicious Group head may try to send a valid aggregate to get approval from the Base Station and then send an invalid fusion data. If this is the case, this can be detected at the Base Station by re-calculating the aggregate and comparing it with the one sent already by the same malicious node. The system is fault-tolerant because there are more than one group heads for a particular region.

B. Reduced power consumption in the Proposed Mechanism

An aggregate very small in size is used to validate the data. It is transmitted only once from the selected fusion node to the Base Station. Power is preserved at the other Group heads. In the Witness Based Approach [11], many copies of the fusion data (MAC) are sent to the Base Station and in the Direct Voting Mechanism [13], one encrypted copy of the fusion data is made available at the Base Station. In the existing methods, this copy of the data has to be approved by all the witness nodes. Only then will the Base Station accept the fusion data. In case the Base Station rejects the data, copy/copies of the fusion data at the Base Station is of no use and hence is a transmission overhead. In this proposed method, this is avoided by initially sending the aggregate value to the Base Station and then sending the fusion data only when the Base Station makes a request. Since the transmission of fusion data consumes a lot of energy, obviously the proposed method reduces the transmission overhead and thereby power consumption. This system avoids re-transmission also. Since Anti-Voting mechanism is used, power is spent only for Anti-voting, (i.e) if and only if there is an invalid aggregate at the Base Station. So the power at the Group heads is not wasted for Voting/Anti-Voting during normal operations.

VII. PERFORMANCE ANALYSIS

The scenario was simulated using ns-2. It included one Base Station, 5 Cluster heads and a number of normal nodes. The following graphs show how the transmission overhead is reduced when compared to the existing methods. The reduction in transmission overhead conserves energy.

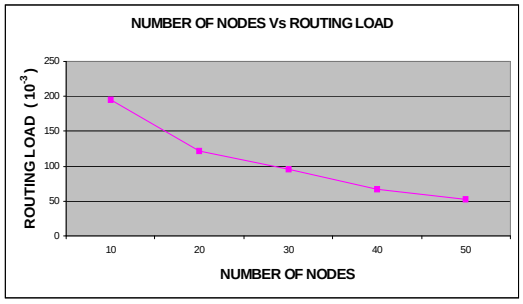

Figure 5 : Data, Votes and Anti-Votes are sent

Fig. 5 shows the transmission overhead when the entire set of data (not the aggregate), votes and anti-votes are transmitted to the Base Station. Fig. 6 shows the transmission load when the aggregate (instead of the entire set of data) and both, anti-votes and votes are sent to the Base Station for verification.

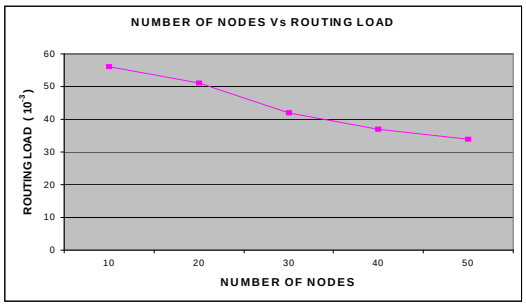

Figure 6 : Aggregate, Votes and Anti-Votes are sent

The transmission overhead is very much reduced in the proposed mechanism. Only the Anti-votes are sent. Further the aggregate is forwarded, thus reducing the load to a greater extent (Fig.7).

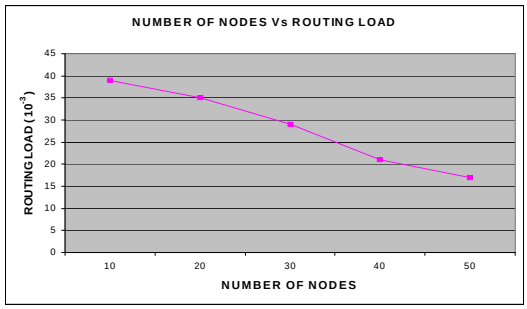

Figure 7 : Aggregate and Anti-Votes are sent

Thus the graph in Fig. 7 shows the transmission load in Indirect Anti-Voting mechanism - the load when only the aggregate and anti-votes (if any) are sent to the Base Station from the Group head, selected for transmission.

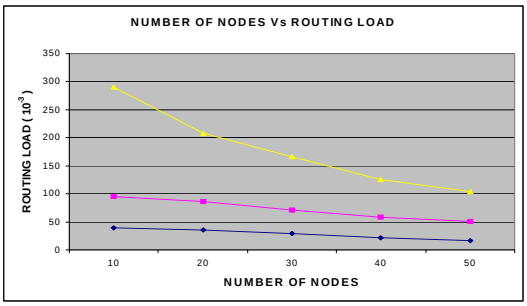

Figure 8 : Combined graph

Fig. 8 shows the comparison of all the transmission loads. It is the combination of all the preceding graphs, showing the reduced transmission load of the proposed system. As the transmission overhead is reduced, the energy expended will also be less.

VIII. CONCLUSION

Power consumption plays a vital role in WiMAX networks. The proposed mechanism conserves power to a greater extent by reducing unnecessary transmissions. The Clustering technique used here avoids depletion of energy. The amount of traffic in the network is very much reduced as the aggregate value is transmitted, instead of the entire set of fusion data. Only on request by the Base Station which is based on the number of Anti-votes, the group head sends the data. Compared to SEDAN, this system is energy efficient, as the data or the keys do not get appended. In contrast to Witness-Based approach and Direct-Voting, to avoid the compromise of the group heads, each node has its own private and public keys. The keys are not transmitted in the network. So the attacks and the corruption of the keys are avoided. To be precise, this cross-layered mechanism provides a secured transfer of data as well as avoids re-transmission. Mathematical models on energy expended can be proposed. This work can be extended to a mobile environment (with multiple levels) with many group heads between the Base Station and the nodes at the lowest level.

REFERENCES

[1] Claudio Cicconetti, Alessandro Erta, Luciano Lenzini, and Enzo Mingozzi, “Performance Evaluation of the IEEE 802.16 MAC for QoS Support”, IEEE Transactions On Mobile Computing, Vol. 6, No. 1, January 2007.

[2] Sheng-Tzong Cheng, Bo-Fu Chen, and Chih-Lun Chou, “Fairness-based Scheduling Algorithm for TDD Mode IEEE 802.16 Broadband Wireless Access Systems”, 2008 IEEE Asia-Pacific Services Computing Conference .

[3] Francesco De Pellegrini, Daniele Miorandi, Elio Salvadori and Nicola Scalabrino ,“QoS Support in WiMAX Networks: Issues and Experimental Measurements”.

[4] Yanchao Zhang, and Yuguang Fang, “ARSA: An Attack-Resilient Security Architecture for Multihop Wireless Mesh Networks”, IEEE Journal on selected areas in Communications, Vol. 24, No. 10, October 2006.

[5] Huseyin Ozgur Tan and Ibrahim Korpeoglu, “Power Efficient Data Gathering and Aggregation in Wreless Sensor Network”, SIGMOD Record, Vol. 32, No. 4, Dec. 2003.

[6] Heinzelman W.et al, “Energy-efficient communication protocols for wireless microsensor networks”, in proceedings of Hawaiians Int’l Conference on Systems Science, January 2000.

[7] Yi Yang, Xinran Wang, Sencun Zhu, and Guohong Cao, SDAP: A Secure Hop by Hop Data Aggregation Protocol for Sensor Networks, MobiHoc’06, Florence, Italy, May 22–25, 2006.

[8] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler and K. Pister, System architecture directions for networked sensors. In Proceedings of ACM ASPLOS IX ,November 2000.

[9] Feng Li and Jie Wu A Probabilistic Voting-based Filtering Scheme in Wireless Sensor Networks, IWCMC’06, Vancouver, British Columbia, Canada, , July 3–6, 2006.

[10] M. Bagaa , N. Lasla , A.Ouadjaout ,Y.Challai, “SEDAN : Secure and Efficient protocol for Data Aggregation in Wireless Sensor Networks”, 32nd IEEE conference on Local Computer Networks 2007,1053-1060.

[11] W . Du, J. Deng , Y. S. Han , and P. K. Varshney, A Witness-Based Approach For Data Fusion Assurance In Wireless Sensor Networks, In Proc. GLOBECOM 2003, volume 3, pages 1435–1439, Dec. 2003 .

[12] Kifayat, Kashif Merabti, Madjid Shi, Qi Llewellyn-Jones, David , Applying Secure Data Aggregation techniques for a Structure and Density Independent Group Based Key Management Protocol , 44-49 , IEEE, AUG 2007.

[13] Silvio Croce, Francesco Marcelloni and Massimo Vecchio , Reducing Power Consumption in Wireless Sensor Networks Using a Novel Approach to Data Aggregation , The Computer Journal Advance Access published online on July 11, 2007.

[13] Hung-Ta Pai and Yunghsiang S. Han, Power-Efficient Data fusion Assurance Using Direct Voting Mechanism in Wireless Sensor Networks, Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC’06), July 2006 .

[14] Petrovic D, Shah RC, Ramachandran K, Rabaey J,” Data funneling: routing with aggregation and compression for Wireless Sensor Networks”, Proceeding of the IEEE International Workshop on sensor Network Protocols and Applications(SNPA-03), May 2003.

[15] Lindsey S, Raghavendra C, Sivalingam K, “Data gathering in Sensor Networks using the energy Delay Metric”, In proceeding of the IPDPS Workshop on Issues in Wireless Networks and Mobile Computing, 2001.

[16] Shakkottai S, Srikant R, Shroff N, “Unreliable Sensor grids: coverage, connectivity and diameter”, In proceeding of the IEEE INFOCOM 2003.

[17] Du X.Xiao Y, “Energy efficient chessboard clustering and routing in heterogonous sensor network”, International Journal of Wireless and Mobile Computing (IJWMC), in print.

[18] Doherty L, Ghaoni LE, Pister KSJ ,”Convex Position estimation in wireless sensor networks”, In proceedings of IEEE Infocom 2001, Anchorage, AK, April 2001.

[19] Savvides A, Han C, Strivastava M, ”Dynamic fine-grained localization in ad-hoc networks of sensors”, In proceedings of ACM MOBICOM’01,ACM press, 2001,pp.166-179.

AUTHOR PROFILE

M. Deva Priya received her B.E (CSE) and M.E (CSE) degrees with distinction from Anna University, Chennai, Tamil Nadu, India in 2005 and 2007 respectively. She is currently pursuing her research in Wireless Networks-WiMAX. She has published 7 papers in National and International Conferences. She has 3 years of teaching experience and is currently working as Senior Lecturer in the Department of Computer Science and Engineering in Manakula Vinayagar Institute of Technology, Puducherry, India. Her area of

interest is Wireless Networks. She is a life member of ISTE.

J. Sengathir received his B.Tech (CSE) and M.Tech (IS) degrees with distinction from Pondicherry University, Pondicherry, India in 2005 and 2009 respectively. He is currently pursuing his research in Wireless and Adhoc Networks. He has published 5 papers in National and International Conferences. He has 3 years of teaching experience and is currently working as a Lecturer in the Department of Computer Science and Engineering, Manakula Vinayagar Institute of Technology, Puducherry, India. He is a life member of ISTE.

M. L. Valarmathi received her Ph.D. in Computer Science and Engineering from Bharathiar University in 2007. She received her B.E (EEE) degree in 1983 from Alagappa Chettiar College of Engineering and Technology, Karaikudi, Tamilnadu, India and her M.E (CSE) from GCT, Coimbatore, Tamil Nadu, India in 1990. She has 25 years of teaching experience. Her areas of interest include Parameter Optimization, Image Processing, Wireless Networks and Computational Intelligence. She has published more than 60 papers in national and international conferences. She has also published 13 papers in National and International Journals. She is currently working as Assistant Professor in the Department of Computer Science and Engineering in Government College of Technology, Coimbatore. She is a life member of ISTE.