VOL. 11, NO. 9, MAY 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

LIVE BANDWIDTH ALLOTMENT LBA-MAC PROTOCOL FOR MANETs

S. Vimala[1] and S. K. Srivatsa[2]
[1]Department of Electronics and Communication Engineering, St. Peter's University, Chennai, India
[2]Department of Computer Science Engineering, Prathyusha Institute of Technology and Management, Chennai, India
E-Mail: vimalasaran@gmail.com

ABSTRACT

In this paper, the necessity to achieve a capable Medium Access Control protocol subject to bandwidth constraints is considered. As Medium Access Control has an important role on the bandwidth allotment, bandwidth efficiency is one of the main concept in the design of Medium Access Control (MAC) protocols for MANETs. Nodes are placed in an ad hoc manner, when transmitting the packets nodes will be inactive for more time and when it becomes an active state, some characteristics of MANETs and applications motivate a MAC that is different from IEEE 802.11 in some ways like Live Bandwidth Allotment and self-organization are the targets. The significance of routing protocol that makes security as wanted by providing a broad architecture of Secured PPEM Mechanism based Multi-Hop Strong Path Geographic Routing protocol (SMHSP) with effective key management, secure neighbour detection, secure routing data's, finding malicious nodes, and eliminating these nodes from routing table is considered. In this paper, we would implement the LBA-MAC protocol under SMHSP routing protocol and compare the performance parameters by varying number of nodes in the MANETs.

Keywords: security, routing protocol, MAC protocol, MANETs.

1. INTRODUCTION

Many algorithms are finding the problem of fairness among senders and receivers in MANETs. Some of the algorithms, despite solving the fairness problem, suffer a significant reduction of the channel throughput; increase approach is proposed to solve the fairness problem in MANETs without degrading the parameter metrics. Throughput and fairness in wireless channels are inversely related, for instance, some research maximizes the throughput [1] but keeps the CW(Contention Window) constant, while other research modifies the CW with respect to the size of the region and the state of the channel. Yet, others modify the CW with respect to the conditions of the network load. The Quality of Service (QoS) of the IEEE 802.11 protocol is a critical issue for some applications such as multimedia. Therefore, a key element is that preserving the bandwidth, packet loss rate, and delay for such applications to achieve an acceptable performance in wireless networks.

The classification of the MAC protocol is divided into two categories. One is single and the other one is multi-channel MAC design. In single channel MAC protocols, a channel is shared by a number of nodes located in close proximity [2]. Typical examples include 802.11 DCF [3], MACAW [4], and MARCH [5]. Single channel MAC protocols are commonly used in MANET. It can achieve high bit rate. Collision avoidance is a big issue for single channel protocols since collision increases with the number of nodes. Throughput is affected if too much collision happens due to lack of bandwidth.

2. LITERATURE SURVEY/RELATED WORKS

The term of contact channels and resource sharing is a necessary task for the harmonization of access among network nodes. This practice is simply managed in a central design due to the central trusted entity, which satisfies the coordination function. However, this can potentially be an issue in mobile ad-hoc networks (MANETs), where the topology lacks a central management entity. On the other hand, security is cared as the main standard in maintaining efficient communication. Therefore, designing a secure MAC protocol is essential to networks, to ensure the provision of secure communication among network nodes. There have been a more number of studies into central security mechanisms in the literature. These studies tested protection, detection and authentication methods. For example, Zhu and Mao [6] looked at the issue of authentication, proposing a secure system that authenticates through a base station that grants access and provides a third party for network validation. Another technique was suggested in [7], in which the base stations of both primary and secondary nodes are utilized to provide the nodes that are connected to the base stations using a wired link. Other studies used a trust value technique of the user in previous communication, calculating the value to determine whether or not the user utilizes the channel [8] [9]. Their mechanism is applied when a genuine user has requested a new hidden channel that was not included in the free channel list. The legitimate user then applies the puzzle system to detect the suspicious behaviour among nodes. A timing parameter technique has also been proposed [10] for the detection of malicious nodes during the negotiation stage. In this approach, if the sender is asked to locate time parameters to follow and does not obey by sending frequent packets, the legitimate user will then stop the communication and simultaneously broadcast the information about the malicious node to other nodes. A Synchronized Latency Secured (Sync-LS) MAC protocol as a new protocol which will solve the latency problem by reducing the number of time frames requirement in the cluster while the energy consumption is nearly same as Zigbee [12]. DBC-MAC protocol solves the coexistence problem between CWPAN/IEEE 802.11aj networks and

IEEE 802.11ad networks that are operating in the same or overlapping 60 GHz band and also supports the backward compatibility with the legacy IEEE 802.11ad stations. Performance evaluations show that the DBC-MAC protocol under CWPAN/IEEE 802.11aj networks outperforms the fixed channel bandwidth mechanism under IEEE 802.11ad networks for specific performance metrics [13]. The authors experimentally derive the IEEE 802.15.4 channel capacity using an unslotted Carrier Sense Multiple Access Collision Avoidance (CSMA-CA) MAC protocol. Considering the experimental channel capacity estimation results and the characteristics of real-time multimedia flows by determining the threshold on bandwidth usage, so that the QoS requirements of real-time multimedia flows in terms of delay, bandwidth and packet loss rate can be met. The authors performed several simulations and results show that QoS requirements of applications were met operating within the bandwidth usage threshold determined in this paper [14]. Real Time MAC(RT MAC) for data transmission between mobile terminals and support real time traffic, such as streamed voice or video, which has a more demanding quality-of-service (QoS) requirement and often requires bandwidth reservation. It uses a Bayesian algorithm to calculate contention probabilities and enable faster convergence of the reservation procedure. The Real Time MAC is free of the "hidden terminal" problem and is designed such that reservations can be made quickly and efficiently with negligible probability of conflict. It is fully distributed and parallel and a reservation is made through a localized conversation between nodes in a 2-hop neighbourhood, and scalable [15].A dynamic QoS aware bandwidth allocation scheme for multi-hop WiLD networks which addresses the congestion problem and hence facilitates QoS support for real-time traffic. The proposed dynamic slot scheduling mechanism efficiently distributes the unused bandwidth among the needy nodes. Twenty percent of the total available slots of each node are not allowed for distribution so as to avoid node starvation problem [16].

3. SMHSP MECHANISM

Our main focuses are to introduce SMHSP to protect data transmission and to construct a secured Geographic Routing protocol [11].

Our SMHSP approach uses an ad hoc security approach so that it satisfies the main security requirement and guarantees the discovery of a proper and secure path. The security approaches that the protocol uses are the hash function, Certificates/Signatures, time synchronization and path discovery request.

SMHSP works as a group and has four stages:

A. Route/path request process

a) Route/path Request message with MMD5 (modified message-digest) 256 bits encryption by Destination

b) Send Encrypted Route/path Request data with Symmetric key from Destination with unique ID (MAC Address)

c) Decrypting MMD5 by sender and check the route/path request.

B. Find and remove the attackers from the routing table process

1. Detecting Attackers in the network by looking up duplicate requests.
2. Find the duplicate request which is coming from Attacker.
3. Removing those attacker nodes from the routing table.

C. Distribution of certificate

1. Source node generates the Certificates/Signature with all the node details.
2. Distribute the Certificates/Signatures to all the authenticated nodes.

D. Packet transfer process

1. Sending Packets to the real destination with PPEM data encryption technique.
2. Receiving packets and decrypt the packets by using PPEM decryption technique by destination.

Route/path request process

The MMD5 (Modified Message-Digest algorithm with 256 bits) hash function is used to encrypt and update the Request packet needed for the routing process in order to secure the data request, which in this case is the first path and time to find a right unique destination, whose information uses hash chains. SMHSP uses hash chains in order to protect the mutable packet request of the first path and Td, the maximum time to find a destination for any node in the network including an intermediate node and the destination node, which when it receives the data can verify that the mutable data request has not been decremented by any attacker. SMHSP forms a hash chain by applying it one way. A hash function is the action whereby a node makes an RREQ and a hash function frequently to begin. The MMD5 Hash function functionality is explained briefly in next headings. Using these Request data's is being encrypted and sending to the source. The source node will have the symmetric/private key to decrypt this message to read the proper request data.

Find and remove the attackers from the routing table

Using the above process sender node can easily find the correct destination. And it could easily find the attacker/malicious nodes by receiving duplicate requests. It would be the strongest way to find the attackers and remove from the network by removing these nodes from routing table.

Certificates/Signatures distribution to all the authenticated nodes

SMHSP adopts the sender node create Certificate/Signature approach because of its power in distributing keys and achieving integrity and non-repudiation. The network uses symmetric/private and public keys. The symmetric key is used to sign the

certificate/signature and the public key of all the nodes, while the public key is used to renew certificates/signatures that are issued by sender/source node. All nodes must to have verified certificates/signatures. The public keys and the corresponding symmetric keys of all nodes are created by the sender node, which also issue the public-key certificates of all nodes. Each node has its own public/Symmetric key pair. Public keys can be distributed to another node in the secure route stage, while symmetric keys should be kept confidential to individual nodes.

Each node in SMHSP method receives exactly one certificate/signature after securely authenticating its identity to the Source node. Each node will hold its certificate in the Node Databases. The main structure of node certificates, it contains the identifier of the node, its public key, the name of the sender giving this certificate, the certificate issue and expiry dates, and the public key of the node. Finally, the contents of the certificate will be attached to the signature of the sender node. All nodes in a network should maintain fresh certificates with the sender node. At the secure route stage, nodes use their certificates to authenticate themselves to other nodes in the network.

Packet transfer process

SMHSP approach is to use a PPEM algorithm to launch secure data between nodes. The Secure route stage is found in the first process and is based on the requirement for all nodes to have a protected path with other nodes before sending any route request packet. Any node receiving an RREQ from the sender node or another node without a protected path should discard the request. In our approach, each node is given the system public key in order for any node to be able to send a Secure route Request to another node the first time the certified public keys are exchanged/distributed. The authenticity of the certificate can be confirmed as the nodes have the system public key. The first objective is the exchange of the certified public keys and their confirmation, while its second objective is to ensure the identity of the sender before acceptance of the RREQ.

4. WORKING PRINCIPLE OF PPEM (PACKET PROTECTION ENCRYPTION MECHANISM) ALGORITHM

PPEM (Packet Protection Encryption Mechanism) calculation utilizes Symmetric-keys that are a class of calculations for cryptography that utilize the same cryptographic keys for both encryption of plaintext and decoding of figure content. The keys may be indistinguishable or there may be a straight forward change to go between the two keys. The keys in practice, speak to an imparted mystery between two or more hubs that can be utilized to keep up a private data join. Both the hubs have the right to gain entrance to the mystery key. The key size utilized for a PPEM figure details the quantity of reiterations of change adjusts that change over the data, called the plaintext, into the last yield, called the figure content. The quantities of cycles of redundancy are as per the following:

10 cycles of redundancy for 128-bit keys.
12 cycles of reiteration for 192-bit keys.
14 cycles of reiteration for 256-bit keys.
16 cycles of reiteration for 128-bit keys.

Each round comprises of a few preparing steps, each one containing four comparative however diverse stages, including one that relies on upon the encryption key itself. A set of opposite rounds are connected to change cipher text go into the first plaintext utilizing the same encryption key. Table-1 highlights these categories of data.

Table-1. Categories of data.

128-Bit Key Avalanche
Plaintext Avalanche
Plaintext/Cipher text Correlation
Cipher Block Chaining Mode
Random Plaintext/Random 128-Bit Keys
Low Density Plaintext
Low Density 128-Bit Keys

5. WORKING PRINCIPLE OF MMD5 (MODIFIED MESSAGE-DIGEST ALGORITHM)

"MMD5 message-digest algorithm takes as input a data of random length and gives as output a 256-bit "fingerprint" or "message digest" of the input. It is conjectured that it is computationally infeasible to produce two data having the same message digest, or to produce any data having a given pre specified target message digest. The MMD5 algorithm is proposed for digital signature applications, where a big file must be "compressed" in a secure method before being encrypted with a private key under a public-key cryptosystem such as RSA. MMD5 is considered one of the most efficient algorithms. MMD5 algorithm uses four iterations, each applying one of four non-linear functions to each sixteen 32-bit segments of a 256-bit block source text. The result is a 256-bit digest. Below is a graph that illustrates the structure of the MMD5 algorithm.

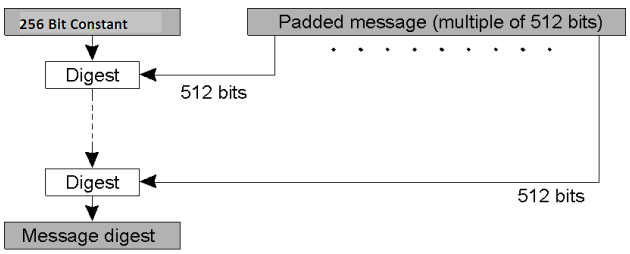

Figure-1. Structure of MMD5 algorithm.

1. Join padding bits
2. Join length
3. Initialize MD buffer
4. Process data in 16-word blocks

6. LBA-MAC PROTOCOL FOR MANETs

The main objective of the proposed LBA-MAC is to allocate bandwidth to the Network users in a more dynamic manner. To this end, we propose two modifications to the MAC: one is Dynamic Bandwidth Allotment (DBA) and other one is Secured Transmission Interval Setting (STIS). Through the proposed designs, LBA-MAC not only can support more complicated network cases, but can also further utilize the spectrum holes in a more effective way. In first phase the LBA-MAC, DBA is proposed such that the network users are not limited to transmit only pre-defined packets. To this end, several new variations of packets are defined, namely MAX PACKET, bandwidth demand of Network Sender (NS) and bandwidth demand of Network Receiver (NR). Similarly, the MAX PACKET is a pre-defined network parameter. However, instead of representing the number of packets that can be transmitted by each user/node, it refers to the maximum number of packets that is allowable to be transmitted by a user/node pair when both network users are on the data channel. On the other hand, the NS and NR refer to the number of packets to be transmitted by the Network Sender and Network Receiver respectively. Considering that a network may carry asymmetric traffic flows between a user/node pair, the values of NS and NR are dynamically decided on the control channel during the BNP (Broadband Network Premises) on the control channel. These values are carried in the control packets, i.e., REQ and GRANT. To this end, REQ and GRANT is extended with a 5-bit field of NS or NR. With the allocation of this 5-bit field, each user/node can request up to a maximum of 31 transmission opportunities. The remaining three bits are left unused for possible future extension. The DBA of LBA-MAC operates in the following way. Firstly, assuming that a Network Sender maintains a separate queue for every Network Receiver. Before sending an REQ, the Network Sender gets the number of packets to be transmitted to a specified Network Receiver by retrieving the current size of the corresponding queue. This information is treated as the value of NS in the REQ and shall be set using the following equation:

$$NS = \begin{cases} CQs, & \text{if } CQs \le MP \\ MP, & \text{if } CQs > MP \end{cases} \quad (1)$$

where CQs denotes the Current Queue size of the Network Sender (for the specified Network Receiver) and MP denotes the pre-defined and fixed network parameter MAX PACKET(MP). Upon receiving the REQCR, the Network Receiver checks the corresponding queue that contains packets to be sent to the Network Sender and then decides the value of NR using Eq. 2. At the same time, the Network Receiver also records the value of NS as the number of packets to be received from the sender (NPRs). After that, it replies a GRANT to the Network Sender.

$$NR = \begin{cases} 0, & \text{if } Qr = 0 \\ MP - NS, & \text{if } CQr \ge \lfloor A \rfloor \text{ and } NS \le \lceil A \rceil \\ \lfloor A \rfloor, & \text{if } CQr \ge \lfloor A \rfloor \\ CQr, & \text{if } CQr \le \lfloor A \rfloor \end{cases} \quad (2)$$

where NR denotes the size of the queue containing packets to be sent to the Network Sender and A denotes M/2.

Finally, the Network Sender reads the value of NR in GRANT and records the number of packets to be received from the receiver (NPRr).It then finalizes its value of NS. Using our proposed DBA, the LBA-MAC can offer very high flexibility in allocating bandwidth to the user/node pair regardless of their traffic condition. Through maintaining the NS, NR, NPRs and NPRr, LBA-MAC can support (1) a uni-directional traffic flow from the Network Sender to the Network Receiver, (2) a bidirectional traffic flow where both the user/node sender and the Network Receiver have the same number of packets to send in their queues, and (3) a bi-directional traffic flow where the user/node sender and the Network Receiver have unequal numbers of packets to send in their queues. In case (3), the user/node pair will swap their sender/receiver identities on the data channel when the Network Sender has transmitted all packets in its queue but the Network Receiver still has packets to send in its queue. At this moment, the bi-directional traffic flow temporarily degenerates to a unidirectional traffic flow.

In phase two of the LBA-MAC, STIS is proposed such that the TI to be carried in the control packets can provide the neighbouring PUs (Position Updates) with the correct timing information when bi-directional bandwidth reservation is needed. In a typical 802.11 network, a two-way handshake of RTS/CTS (Request To Send /Clear To Send) is adopted for bandwidth reservation. In the process of handshaking, the TI is carried in the RTS packet to indicate how long a sender wants to hold the medium. In return, the receiver replies with a CTS packet echoing the expected duration of transmission. Through the exchange of RTS and CTS control packets, all the nodes within the hearing distance of either the sender or receiver or both will set their Network Allocation Vector (NAV) according to the TI in the overheard packets. In the presence of bi-directional traffic flow, further a conditional transmission of RTSe is proposed by the Network Sender after receiving a CTS. As a result, the Network Sender can effectively update all of its neighbouring PUs with its latest TI whenever bi-directional bandwidth reservation is required. The format of RTSe in LBA-MAC is identical to that of the RTS packet. In the STIS, the TI of a CTS packet is set where Dcts, Drtse, Ddata, and Dack refers to the transmission time of a CTS, RTSe, data and ACK packet respectively. Upon receiving a CTS packet, if a bi-directional bandwidth reservation is anticipated, the Network Sender immediately transmits an RTSe control packet with the TIrtse calculated.

To sum up, through the proposed DBA, the LBA-MAC can maximize the achievable throughputs in a Network by minimizing the frequency and overhead of Network users switching from the control channel to the data channel and vice versa in presence of bi-directional flows. Also, through the STIS, the LBA-MAC can broadcast correct information of TI to all neighbouring

nodes of a user/node pair to avoid unnecessary packet collisions.

7. SIMULATION PARAMETERS AND PERFORMANCE ANALYSIS

Table-2. Simulation parameters.

Channel	Channel/Wireless
Network Interface	Wireless
NS Version	NS-2
CBR Packet Size	512 bytes
MAC	LBA-MAC
Routing Protocol	SMHSP
Interface Queue	Priority Queue
Queue Length	100
No. of Nodes	50
Simulation Area Size	800x800
Simulation Duration	20sec
Packet Rate	1000k

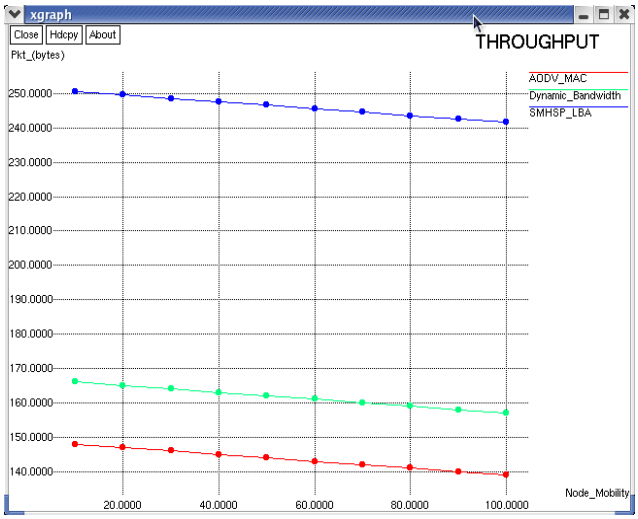

Figure-2. Simulation result data rate vs. throughput.

Figure-2 indicates the throughput values for different number of nodes. The developed protocol LBA-MAC is compared with the existing protocol AODV_MAC, and Dynamic_Bandwidth. LBA-MAC improves the throughput in terms of number of nodes.

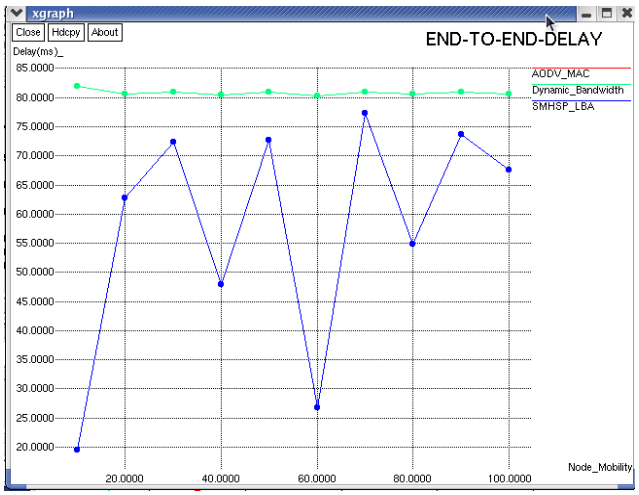

Figure-3. Simulation result data rate vs. delay.

Figure-3 indicates the delay for different number of nodes. The developed protocol LBA-MAC is compared with the existing protocol AODV_MAC, and Dynamic_Bandwidth.

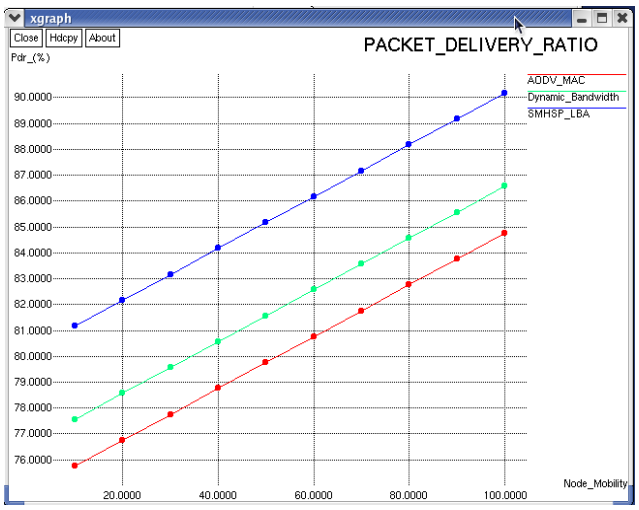

Figure-4. Simulation result of data rate vs. packet delivery ratio.

Figure-2 indicates the packet delivery ratio for different number of nodes. The developed protocol LBA-MAC is compared with the existing protocol AODV_MAC, and Dynamic_Bandwidth. LBA-MAC improves the packet delivery ratio in terms of number of nodes.

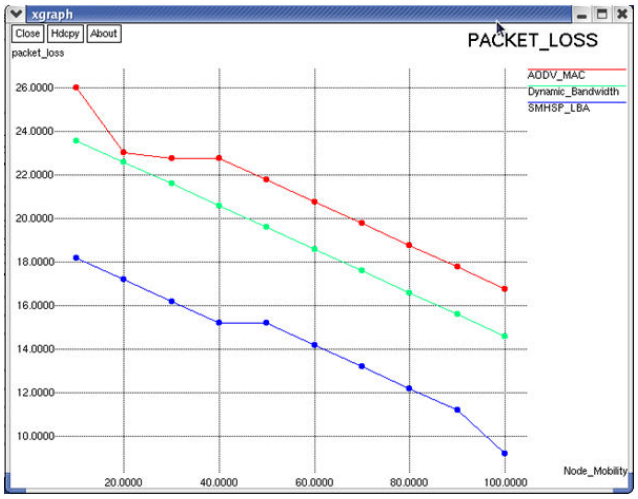

Figure-5. Simulation result of data rate vs. packet loss.

Figure-5 shows that the packet loss is less when compared with other protocols.

CONCLUSION

In this paper, the proposed LBA-MAC protocol for networks over 802.11 networks. The proposed LBA-MAC can reserve bandwidth dynamically to further utilize the spectrum holes of the authorized bandwidth. In addition, the LBA-MAC can support asymmetric two-way traffic flows with variable packet sizes. Simulation results show that the proposed LBA-MAC can significantly enhance the aggregate throughputs of nodes in a network and dramatically improve the spectrum efficiency without degrading the performance in SMHSP routing.

REFERENCES

[1] Sachin Garg, Martin Kappes, and A. S. Krishnakumar. 2002. On the Effect of Contention-Window sizes in IEEE 802.11b Networks. Technical report, Avaya Labs Research, June 2002.

[2] Z. J. Haas and J. Deng. 2002. Dual Busy Tone Multiple Access (DBTMA)-A Multiple Access Control Scheme for Ad Hoc Networks. IEEE Trans. on Communications. 50(6): 975-985.

[3] 1999. LAN/MAN Standards of the IEEE Computer Society, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification. IEEE standard 802.11, 1999 Edition.

[4] V. Bharghavan, A. Demers, S. Shenker and L. Zhang. 1994. MACAW: A Medium Access Protocol for Wireless LANs, Proc. of ACM SIGCOMM 1994. pp. 212-225.

[5] C. K. Toh, V. Vassiliou, G. Guichal and C. H. Shih. 2000. MARCH: A Medium Access Control Protocol for MultiHop Wireless Ad Hoc Networks. Proc. of IEEE MILCOM 2000. 1: 512-516.

[6] L Zhu and H, Mao. 2010. Research on authentication mechanism of cognitive radio networks based on certification authority. In: Computational Intelligence and Software Engineering (CiSE), 2010 International Conference on. pp. 1-5

[7] S, Parvin. and F, Hussain. 2011. Digital signature-based secure communication in cognitive radio networks. In: Broadband and Wireless Computing, Communication and Applications (BWCCA), 2011 International Conference on. pp. 230-235.

[8] S, Parvin, S, Han, B, Tian. and F, Hussain. 2010. Trust-based authentication for secure communication in cognitive radio networks. In: Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on. pp. 589-596.

[9] S, Parvin., S, Han., F, Hussain., and M, Al Faruque. 2010. Trust based security for cognitive radio networks. In: IiWAS '10 Proceedings of the 12th International Conference on Information Integration and Web- Based and Services, 2010. pp. 743-748.

[10] R, Shaukat, S, Khan. and A, Ahmed. 2008. Augmented security in IEEE 802.22 MAC layer protocol. in Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference. pp. 1-4

[11] S.Vimala, Dr.S. K. Srivatsa. 2015. Secured PPEM based Multi strong path Geographic Routing Protocol for MANETs. In International Journal Of Applied Engineering Research. pp. 483-504.

[12] Monir Hossen, Ki-Doo Kim, and YoungiI Park. 2010. Synchronized latency secured MAC protocol for PON based large sensor network. In: IEEE International Conference on Advanced Communication Technology. pp. 1528-1532.

[13] Qian Chen, Xiaoming Peng, Khiam-Boon Png, David Tung Chong Wong and Francois Chin. 2014. Dynamic bandwidth control MAC protocol for CWPAN/IEEE 802.11aj Networks. In: IEEE Globecom. pp. 4726-4731.

[14] Muhammad Omer Farooq, Thomas Kunz. 2013. On determining bandwidth usage threshold to support real-time multimedia applications in wireless

multimedia sensor network. In IEEE Computer Society. pp. 401-406.

[15] M. Murali, Dr. R. Srinivasan. 2009. Bandwidth Reservation in Mobile Ad hoc Network using RealTime MAC Protocol' in IEEE Computer society. pp. 563-566.

[16] Iftekhar Hussain, Zaved Iqubal Ahmed, Dilip Kumar Saikia and Nityananda Sarma. 2015. A QOS-aware dynamic bandwidth allocation scheme for multi-hop WiFi based long distance networks. In EURASIP Journal of Wireless Communications And Networking. pp. 1-18.