Huffman Coding and Multi-Generation Mixing Assisted Network Coding Based MAC for QoS-Centric Secure Data Communication over MANETs

Prasanthi Konduru
Research Scholar
REVA University, Bangalore
prasanthiraj.rct@gmail.com

Mallikarjuna shastry P.M
Professor, REVA University
Bangalore-560063
mallikarjunashastry@reva.edu.in

Article History: Received: 10 November 2020; Revised 12 January 2021 Accepted: 27 January 2021; Published online: 5 April 2021

Abstract- The exponential rise in wireless transmission has gained widespread attention to meet major mobile communication purposes including, Internet of Things (IoT) and Machine-to-Machine (M2M) communications. Mobile Ad-hoc Network (MANET) has emerged as one of the most viable solution to meet aforesaid mobile communication purposes; however, being decentralized and infrastructure-less network it undergoes adversaries including dynamic topology and security breaches due to malicious node attachment during routing. On the contrary, data security and allied Quality-of-Service (QoS) provision are inevitable in NextGen communication systems. Unlike routing-based security measures, Medium Access Control (MAC) based approaches are found more effective for MANETs. However, most of the classical MAC designs either address QoS or security as standalone objective. Unlike existing MAC solutions, in this paper a state-of-art novel Huffman Coding and Multi-Generation Mixing (MGM) assisted random linear network model-based MAC design (HM2-MAC) is proposed for MANET. Realizing the robustness of the network coding algorithms towards reliable, secure and error-free multicast transmission, we designed HM2-MAC in such manner that Huffman coding helps securing the source data packets, while MGM concept enables reduction in redundant packets to make overall communication resource efficient and secure. Unlike redundant packet-per-generation, MGM concept helps in reducing redundant transmission and hence achieves resource efficiency. Since, in HM2-MAC model the coefficient matrix used to encode the data is known only to the sink, no intermediate node can decode it or can pollute it. It makes multicast transmission more secure over MANET. Additionally, the use of iterative buffer flush technique preserves resources or buffer to accommodate more data for transmission and hence higher throughput. Noticeably, error sensitive packetization and MGM control strengthens our proposed model to retain optimal performance. HM2-MAC has been applied as a sub-layer of native IEEE 802.11 MAC and hence retains backward compatibility towards real-world implementation. MATLAB based simulation revealed that our proposed HM2-MAC protocol achieved almost 99.6% throughput even under varying link-loss patterns, which reveals its robustness to ensure QoS delivery with secure data transmission in MANET.

***Keywords*—** MANET, Network Coding, Huffman Coding, Multi-Generation Mixing, Quality of Service, Data Security.

1. Introduction

In the last few years wireless communication has gained significant demands to meet major communication purposes serving healthcare sector, defense sector, industrial monitoring and control, civic as well as strategic monitoring and surveillance, business communication etc. To meet such demands different wireless networks have been proposed such as wireless sensor network (WSN), MANET, cellular network etc. However, the decentralized and infrastructure less nature of MANET enable it to be one of the most viable solutions to accommodate mobility-based communication. Unlike WSN, the ability to accommodate mobile-communication enables MANET to be used across communication systems, such as IoT, M2M etc. MANET encompass multiple mobile devices with self-configuration ability to enable cooperative communication [1]. Functionally, it forms temporary local network without pre-installed radio devices, receiver or routers, which increases its scalability to serve communication during disaster, natural calamity or inter-vehicular communication [2]. Functionally, each node in MANET acts as a router to enable end-to-end communication while performing random or autonomous movement. MANET nodes can form and retain connection with the pre-established infrastructure or central management units to accommodate communication. Such features make it one of the most sought networking solutions to serve varied wireless communication purposes including IoTs. Noticeably, being mobile in nature it undergoes exceedingly high dynamism and network variations. Additionally, being infrastructure-less and

decentralized solution, it also needs to accommodate other intermediate nodes to serve multihop and/or multicast transmission. This as a result broaden the horizon for a participating node to get access of the node resources for transmitting its data. Such features enable even an intruder [1][3] to get access into the routing table. Thus, a malicious node or intruder getting access to the resource or route forces MANET to undergo different adversaries including eavesdropping, Denial of Service (DoS), packet drop, flooding etc. This as a result impacts overall network efficiency and imposes security related vulnerability [3][4]. Towards QoS provision, MANETs have evolved over numerous enhancements in the form of QoS-sensitive routing solution, QoS adaptation, QoS signaling enhancement and QoS MAC model [4-10]. Amongst the major solutions, QoS routing and QoS MAC protocol has decisive impact on overall network performance [9]. On the other hand, QoS is highly dependent on network conditions such as data security, and optimal transmission decision. The security breach(es) can cause packet drop, packet loss and unwanted bandwidth and resource exhaustion. Unfortunately, so far QoS and security are addressed as the distinct network problems, which makes overall solution computationally over-exhaustive and hence limits network efficiency [9][10]. It indicates the need of a robust and efficient protocol which might ensure both QoS as well as data-security [9]. This mechanism can not only strengthen overall network with confidentiality, authentication, availability, integrity and non-repudiation [9]. This as a result can help achieving QoS provision to the MANETs [9][10].

In MANETs, MAC layer has the irreplaceable significance. MAC helps establishing optimal connection without congestion or contention condition, minimum delay, while ensuring optimal resource allocation and QoS assurance [9][11]. MAC based security systems are found effective for reactive, proactive as well as zone routing protocols [11]. MAC, being the key layer towards resource allocation or channel access undergoes numerous adversaries including intrusion by possible malicious node mimicking like a genuine node [9][15]. Different attacks can damage MANET and its intelligence that can disrupt its QoS ability [72]. In this case, ensuring security of the different layers including PHY, MAC and routing layer is must [72]; however, amongst aforesaid layers, MAC has relatively better efficiency to ensure secure and QoS-communication in MANETs [3][4][72]. With this motive, numerous researches have been made for MAC based data security in MANET; however, retaining QoS and data-security balance has remained the least explored research area [9]. To secure MANET, though different security polices [6] have been proposed, however classical cryptography, and routing-based methods, and/or key-management policies are confined due to increased computational overheads and reduced throughput [16]. On the contrary, the current MANET based IoT and M2M systems demand both QoS provision as well as optimal data security to meet at-hand and/or future networking demands. Unlike cryptography-based methods, recently an information theoretic concept named network coding has been found more viable or potential solution to ensure data security as well as QoS delivery over multicast transmission in MANET [8].

Network coding has emerged as a robust transmission mechanism that enables source node to encode the target data packet and transmit over multiple paths. On the other hand, it enables intermediate node(s) to encode (say, computer) and forward received source node packet(s) to the next hop to meet timely and safe data delivery [9]. Though, present network coding methods are more robust than the classical "Store, Compute and Forward" based methods [9]; however, their resilience to avoid intermediate node's malicious behavior remained a challenge. ON the other hand, its robustness towards MAC design has been affirmed in numerous literatures [1-10][72]. Functionally, it enhances the overall network ability to meet error-free transmission while retaining low-cost communication purposes [35][37][38][72]. However, its classical concept doesn't address any pollution attack conditions during multicast transmission in networks like MANET [40][43]. Such vulnerability might impact overall QoS performance as well as MAC processing. The presence of a malicious node in MANET, can impose fake vectors of the received packet or can introduce invalid combinations of the received packet which can pollute entire data or entire network [11][43]. To address such problems, enhancing network coding is vital [3][20][40][43]. Unlike classical compute and forwards-based network coding models [43], RLNC methods are more robust towards attack-resilience, due to increased randomness during encoding [45][46][48]. However, its suitability as standalone solution can be limited due to pollution attack. Authors [10] suggested to use an additionally security layer in the form of homomorphic encryption to enhance attack-resilience. In this mechanism, to transmit data a source node splits input file into multiple blocks which are encrypted using certain crypto-mechanism named homomorphic encryption. Transmitter node transmits the encoded and combined data instead of the original data to the intermediate node, which participates in network coding to add or append other packet(s) before transmitting towards the sink. Receiving packet(s) from the transmitter, the intermediate node combines the arriving vectors as per local encoding matrix and then forwards it to the neighboring or adjacent nodes. Eventually, the receiver recovers the original message from the received packets using encoding matrix. Though, homomorphic encryption-based network coding and MAC designed [40][43] can prohibit pollution attack up to certain extent, the computational overheads imposed and compromised throughput performance can't be denied. It can affect overall QoS provision by MANET. A viable solution towards aforesaid problem can be certain computationally efficient and error-resilient multicast transmission for MANET.

Considering above stated problems and allied scopes, in this research paper a state-of-art new concept named Huffman coding assisted multi-generation mixing based network coding for MAC design (HM2-MAC) has been proposed. The proposed HM2-MAC model employs the concept of systematic RLNC, with Huffman coding and MGM, which retains higher security with low redundant packet to support QoS. Huffman coding, a compression-based encryption at one hand improves data security from any possible pollution attack or intermediate attack, while MGM with iterative buffer flush enables resource efficient and error-resilient multicast transmission over MANETs. The proposed HM2-MAC has been designed to cope up with multicast transmission and error-sensitive MGM generation, which makes it robust to achieve resource efficiency even with low Galois Field (GF) size and (low) number of redundant packets. MATLAB based simulation has revealed that the proposed HM2-MAC achieves better throughput and conceptually higher attack-resilience for MANET.

The remaining sections of this paper are divided as follows. Section II discusses the related works, followed by problem statement in Section III. Section IV presents the system model and implementation, while MAC implementation of HM2-MAC is given in Section V. The simulation results and allied inferences are given in Section VI. Research conclusion is discussed in Section VII, and the references used in this manuscript are mentioned at the end of the manuscript.

2. Related Work

In MANET, the participating node employ shared channel to exchange information amongst nodes, which makes it vulnerable towards intermediate attack [11]. Moreover, functionally, it undergoes contention or collision in shared channel that reduces the network performance. To alleviate it MAC has been playing decisive role, especially towards better resource allocation, reliable transmission and data security. The existing approaches address security concerns in two distinct manners, first routing-based security and second MAC based security for which different efforts have been made [12-23]. As routing-based solutions, authors [12] designed dual-attack detection model for black-and-Gray hole attack resilience. It employed intrusion detection system (IDS) and connected dominating set (CDS) method to enhance attack-resilience. Applying energy and status packet information, authors [12] identified the malicious node; however, could not address MAC specific network performance improvement. Authors [13] designed a routing concept to avoid blackhole attack in MANET. Similarly, secure Ad-hoc on-demand distance vector (SAODV) protocol was designed in [14] to avoid different attacks such as blackhole, route disruption attack, route invasion attack, and reply attacks. SAODV transmits encrypted message to avoid any possible intrusion or attack, where to encrypt the input packets authors applied public key encryption model with hash chain and digital signature. Despite of the significant changes it could deliver low throughput (less than 90%) with huge computational overheads. Though, data encryption was suggested in [14] as well, however, its computational cost was ignored by authors. Authors [24] used a random number, secrete key, and hash function to develop an authentication scheme for MANET security. They used random number with a time-stamp to secure nodes. In this method the random number applied a hash function to generate a secret key to prevent key-replication. However, it was computational exhaustive, which can impact QoS performance in MANETs. Enhanced secure trusted AODV (ESTA) was proposed in [25] which focused on improving multiple and loop-free disjoint paths in MANET routing. They used trust and authentication (using asymmetric encryption) to secure data. In [26] as well, two secure routing methods named binary decision diagram AODV was proposed for MANET's security. To improve security, authors suggested multipath transmission in MANETs. Authors [15] detected different attacks over IEEE 802.11 MAC and found that back-off attack has more lethal affect than RTS (request to send) flooding. In [16][17] authors measures misbehavior effect of MAC in the network layer performance to enhance security aspects of AODV ad dynamic source routing (DSR). Research in [27] too focused on detecting selfish attack on MAC layer of MANET. While, single adversary attack (SAA) and colluding adversary attack (CAA) were examined in [28] to improve 802.11 protocol in MANET. To alleviate SAA and CAA issues, authors proposed Fair-MAC by controlling traffic flow and adjusting relative distance. However, its robustness towards MANET seems limited, especially when there are high topological changes. In [29], amalgamated destination sequence number and on-hop process for MAC to avoid blackhole attack. An enhanced CSMA/CA MAC was designed in [30] to alleviate DoS attack. Authors applied M-truncated sequential Kolmogorov–Smirnov test to measure network behavior to avoid any DoS attack(s) in MANETs. Authors [31] focused on enhancing MAC 802.11b for both reactive (i.e., AODV) as well as proactive (i.e., OLSR) protocols in MANET. A hybrid model with MAC and routing layer was designed in [12], where cumulative frequency detection (CFD) and data forwarding behavior detection (DFBD) were applied along with MAC authorization to prevent any attack. CFD applied channel busy information with clear to send (CTS) information to detect intruder, while DFBD helped to identify malicious nodes using incentive concept [12][32]. Finally, error-bit concept was applied to identify the intruder node in MAC-based network authentication. However, the computational overhead of this method could limit its efficacy towards real-time mission critical communication in MANET. Authors [23] proposed Diffie-Hellman key exchange-based MAC for MANET. In [33] authors

applied secure hash-algorithm (SH3) based method for MAC design (HMAC-SH3) to avoid DoS attack in MANET. In [34] as well, authors designed MAC protocol for WSN by using localized encryption and authentication protocol (LEAP) and TinySec to thwart away attackers. This approach was found highly exhaustive and computationally overburdened. In the last few years information theoretic concept(s) [35][36] and cryptographic [33][34] [37-42] have been used for data security in wireless networks. Amongst major viable solutions, network coding has emerged as an efficient error-free and secure transmission algorithm [43] which guarantee not only higher throughout but also low delay [43][44]. The RLNC methods are even more robust towards multicast transmission in wireless communication systems [45][44], especially to achieve higher network capacity and reliability [44][45]. Recently, to strengthen overall efficiency, authors [44][45] proposed deterministic polynomial time-network coding, which was found more efficient towards wireless network and MAC designs [46-49]. Despite of better performance, the presence of any malicious node in network coding-based transmission might inject corrupt packets into the information flow which might degrade overall performance. It can also manipulate MAC functionality and hence overall network performance. Authors [50-52] designed theoretical bounds of network error correction to enhance network coding-based communication [53] to avoid any passive adversaries. Similar efforts were made in [50][54-58] to avoid Byzantine attacks [59][60]. However, authors [46] indicated its limitations in wireless network such as MANETs due to increased complexity and possible pollution attacks. To strengthen network coding-based MAC design, a few methods have been proposed using cryptographic methods; however, those approaches are limited due to iterative encryption-decryption at the different intermediate nodes. Moreover, such methods might destroy data originality, and hence can impact QoS delivery. To alleviate such problems, different approaches like homomorphic hashing [61][62], homomorphic digital signature [38][64][65], and homomorphic MAC [43][66] are proposed. However, addressing computational overheads, redundant transmission and resource efficiency is the key challenge in these methods. To alleviate computational overheads at the intermediate node(s), in [67] the intermediate node merely checked the membership of the received vector without making any changes to it. Its efficacy with dynamic topology seems limited. Authors [37] suggested homomorphic signature with lower key size and per-packet overhead for MAC design. Here, signature over a definite and low vector was performed rather complete subspace. However, bilinear pairing imposed significantly large computation to ensure delay-resilient transmission. As enhanced solution, authors [39] proposed probabilistic key-distribution and message authentication code, especially to avoid pollution attack at the MAC layer. However, this method required each source node to add multiple MACs to each data before transmission to the neighboring node. The use of secret key for each data block could impose significantly large overheads. Recently, authors in [43][68] proposed homomorphic MAC to enable data-integrity of the network coded data. Authors in [69] proposed RIPPLE, a symmetric key based network solution for network coding authentication. To achieve it, authors used homomorphic MAC and TESLA [70]. In this method, the use of RIPPLE enabled estimation of the MAC labels, the sources must have the prior information about the longest route from source to the destination. Similarly, homomorphic hashing [39][41][42] and homomorphic signatures [37-40] were proposed to improve network coding-based transmission security; however, their efficacy towards data security could not be examined. Authors [63] proposed a key pre-distribution-based tag encoding concept where each source-node required generating multiple tags for each packet. Additionally, the intermediate node generates a new tag as per the received tag and then verifies the correctness of the data packet. Unfortunately, computational complexity and delay can't be ignored in this case. In [39], authors used RSA-based homomorphic hashing and signature to avoid pollution attack. However, it was computationally expensive and imposed more overhead [71].

3. Problem Formulation

To meet contemporary QoS-centric and secure data transmission demands, different standard protocols recommend IEEE 802.11 MAC to employ packet data conversion protocol to retain smooth and error-free transmission scheduling. In this process, once receiving the content from upper system layers it processes for segmentation followed by encapsulation, before processing at the MAC layer and further transmission. However, such approaches impose computational overheads. On the other hand, such classical methods often undergo intrusion due to common media access condition in MANETs. To alleviate such problem, in this research we hypothesize MAC based secure data transmission system to meet QoS expectation as well as data security. Unlike routing-based security system, MAC based models focus on scheduling packets in optimal manner with seamless transmission ability. In sync with this concept, in this paper and the proposed MAC model at first, we convert input data into packets, without processing for segmentation and encapsulation. Here, it is done to reduce computational overhead on MAC layer. On the other hand, to serve QoS purpose, MAC in MANET requires swift and high-rate transmission, maintaining large size of the packet is significant. To achieve it, the proposed and targeted MAC model recommends concatenating the packet data units (PDUs) to form a single data vector so as to reduce resource exhaustion as well as computational cost. Subsequently, we introduce a state-of-art new Huffman coding and multi-generation mixing (HC-MGM) assisted systematic RLNC algorithm for MAC design.

Here onwards, we call our proposed MAC protocol as HM2-MAC. To retain backward compatibility with the native MANET MAC protocol standard IEEE 802.11, we propose HM2-MAC to be applied as the sub-layer of native 802.11 MAC layer. Functionally, to enhance data security and attack-resilience our proposed HM2-MAC protocol applied Huffman coding also called Prefix-coding concept [73][74], which encodes the input data packet or vector before transmission. This approach resembles compression-based encryption to safeguard input data being transmitted. To execute systematic RLNC, HM2-MAC model at first splits input data into multiple K data vectors (say, symbols) of equal sizes. Thus, encoding each vector, a source node transmits the packet onto the multicast network. Unlike classical approaches where even the intermediate node decodes the input data and appends its other packet before transmission (it imposes the threat of pollution attack on MAC), our proposed HM2-MAC design enables transmitter or sender node to use specific coefficient matrix to encode the data, which is only known to the receiver. It preserves security of the data packets over channels and hence no intermediate node (non-sink node) can decode the data being transmitted. It strengthens the attack-resilience of the transmission system. Additionally, to cope up with QoS demands, our proposed model contributes a number of novelties including only encoded coefficient information (ECI) transmission with embedded coefficient matrix position, which makes decoding easier at the sink node. On the other hand, unlike classical one-to-one redundant packet transmission models, we designed a state-of-art new MGM-based RLNC where we focus on reducing the number of redundant packets per transmission without compromising decoding efficiency or throughput at the sink node. Moreover, the proposed MAC design amalgamates iterative buffer flush concept, which once delivering the packets to the sink node flushes the buffer to accommodate other packets. Here, the prime intend is to avoid the waiting time due to acknowledgement process. Since, the proposed Huffman coding assisted systematic RLNC ensures retaining higher throughput without packet error, our proposed model hypothesizes to flush the buffer occupied by the delivered packet. This concept is also backed up with a novelty introduced, called error-sensitive MGM packetization. This approach intends to ensure error-resilient MAC packet scheduling so that it doesn't have to wait for acknowledgement and hence can make process delay-resilient as well as resource efficient. This as a result can help QoS provision in MANETs.

Functionally, once, receiving the packet data units from the upper layer, HM2-MAC executes Huffman coding compression-based encryption over K data vectors, which are further processed for multicast transmission over the network. Noticeably, the encoded data are generated and converted into EPDU in such manner that it fits to the expected transport blocks (TBs) at the physical layer (PHY). In this manner, it intends to maintain higher data security as well as QoS provision to MANETs. The processed MAC EPDUs is encapsulated into PHY TB, where it transmits EPDU without introducing additional automatic repeat request transmissions. It shows robustness of the proposed model towards reliable data transmission with lower redundant packet transmission and hence resource exhaustion. Once receiving the EPDUs, the sink nodes process it at the HM2-MAC decoding sub-layer where it retrieves the original data transmitted by the source node. Retrieving each packet correctly, the proposed model flushes the buffer carrying minimum possible redundant packet and the data to be transmitted or delivered. This ability reduces buffer and signaling cost in HM2-MAC and hence achieves better resource efficiency. Summarily, to support QoS, HM2-MAC embodies unit level optimization including HC-MGM, iterative buffer flush, coefficient optimization etc., which help retaining higher attack-resilience, higher reliability and QoS support in MANETs. The details of the overall proposed HM2-MAC protocol are given in the subsequent sections.

4. System Model

As discussed in the previous sections, our proposed HM2-MAC design incorporates multiple enhancement measures to retain optimal data security as well as QoS provision in MANET. Unlike classical network coding-based MAC, HM2-MAC intends to enhance coefficient vector as well. To be noted, coefficient vector signifies the coefficient (from the Galois Field (GF)) used to encode packets before transmission. To achieve it, HM2-MAC at first performs linear combination of the received packet data units using a coefficient vector derived from GF). The coefficient vector information is known to the sink node. To carry above stated coefficient vector information, we employ a container called coefficient matrix. A key novelty of the proposed MAC solution is that unlike classical designs such as Homomorphic MAC [37][43][68][69] or other classical network coding algorithms, where complete coefficient vectors are transmitted along with the target data or packet, HM2-MAC employ merely the information signifying which specific row of the coefficient matrix has been applied to encode the data or allied linear combinations. It reduces buffer or memory exhaustion significantly and hence can help achieving QoS provision in MANET. The specific raw of the coefficient vector or matrix used for encoding is referred as encoding coefficient information (ECI). To avoid any possible pollution attack or error probability, we applied Huffman coding also called Prefix coding for data compression followed by encryption [73]. Specifically, we employed an adaptive Huffman coding algorithm as proposed in [73][74] to perform encoding of the coefficient information. The details of the adaptive Huffman coding algorithm can be found in [73][74], which is not discussed in this paper due to space constraints. The use of proposed adaptive Huffman

coding concept not only reduced additional computational overheads caused due to iterative encryption, but also enhanced buffer utilization to meet QoS demands in MANET. Once receiving ECI, the intermediate node in the next-hop appends other packet from the same generation or others to be forwarded without decompressing input packet. This approach alleviates any possibility of the pollution attack in MANET. Appending the other pockets if any, the intermediate node compresses the data again and forwards to the neighboring nodes towards the destination. As already stated, in HM2-MAC the coefficient matrix used by the source node to encode the data is not transmitted to the intermediate node, and hence it avoids any possible unauthorized access or pollution inclusion at the intermediate node. To further improve resource efficiency and network performance enhancement, unlike one-to-one packet encoding, we implemented an MGM and encoding concept, where single redundant packet is transmitted along with the source code data to preserve resource as well as computational cost. On the other hand, HM2-MAC applied error-sensitive or error-probability sensitive packetization or MGM, which makes proposed MAC design more reliable and efficient to meet QoS demands. Now, once receiving encoded PDUs (EPDU) with allied ECI, the target sink node decompresses ECI of the received packet and replaces it with the original coefficient vector (used for encoding) to decode the original packet. Subsequently, it transmits one local ACK message as complete data retrieval, which triggers HM2-MAC to flush its memory occupied by the delivered data packets, which helps it improving resource efficiency. Majority of MANET protocols undergo multi-hop and multicast transmission which often employ trans-receiving processes at the different nodes, i.e., source node, intermediate node and the sink node. Noticeably, above mentioned MAC is hypothesized to be employed with each participating node; however, different nodes as source, intermediate and sink has the different roles and level of access. In this research, we assume the network to be deployed as mobile network where routing takes place in certain network architecture comprising source node, intermediate nodes and multiple sink nodes, where each node performs different tasks. The detail of the processes involved in HM2-MAC is given in the subsequent sections.

4.1 Computation at the Source Node

In HM2-MAC protocol, receiving packet data units from the upper system layers such as Application Layer, the source node executes Huffman coding or prefix coding as per [73], which eventually generated n MAC EPDU, also called the source packets, $(s_1, s_2, \dots \dots s_n)$. Here, each source packet represents a $1 \times s$ vector from a Galois Field 2^F, where we maintained size of the Galois Field F as 8. Unlike classical cryptosystems such as AES or RSA, which employs 256 bits key size to encrypt the data, our proposed model applies coefficient vector from 2^8 space only. Applying $m \times n$ coefficient matrix, with non-zero coefficient, conditioned at $m \geq n$, the n packet data units are combined together to generate m linear combinations (1).

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{bmatrix}_{m\times 1} = \begin{bmatrix} q_{1,1} & q_{1,2} & \dots & q_{1,n} \\ q_{2,1} & q_{2,2} & \dots & q_{2,n} \\ \vdots & \vdots & \dots & \vdots \\ q_{m,1} & q_{m,2} & \dots & q_{m,n} \end{bmatrix}_{m\times n} \begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{bmatrix}_{n\times 1} \quad (1)$$

In (1), the matrix components $(x_1, x_2, \dots . x_m)$signify the generated linear combinations. To improve QoS with lower redundant packet transmission in multicast transmission, we used MGM concept, where $m - n$ packet combinations are transmitted in each generation. It not only reduces the error probability, but also helps reducing the need of additional redundant packet to be transmitted along with the original data. Here, we applied low size $m \times n$ coefficient matrix which is lower in size than the original matrix to further improve resource efficiency of MANET. As already indicated, the coefficient matrix is known to the participating nodes in the multicast group. On the other hand, we generate the Galois field in such manner (with matrix comprising non-zero elements) that the overall rank of $n \times n$ matrix component remains n. It enables linear combination of the generated packet in each generation, which helps in improving probability of a packet combination to be significant for decoding at the receiver node. In majority of the classical network coding approaches, the coefficients employed for combination generation are also transmitted along with the original packet (say, EDPU), and in this case the final output packet x_p becomes $\left[q_{p,1}\ q_{p,2}\ \dots\ q_{p,n} \mid x_p\right]$, where$1 \leq p \leq m$. However, such classical methods impose higher redundancy. To alleviate such issues, we used MGM concept, which is discussed in the subsequent section. In the proposed model, the specific row of the coefficient matrix used to generate a specific packet combination is taken into consideration, which is also called ECI, where each comprising element be I_{p_w}. Additionally, conditions $1 \leq p \leq m$ and $1 \leq w \leq m$ are defined in the form of b bits. Thus, the eventual output packets x_p along with the corresponding ECI $\left[I_{p_1}\, I_{p_2} \cdots\, I_{p_m}\right]$ is defined as (2).

$$\left[I_{p_1}\, I_{p_2} \cdots\, I_{p_m} \mid x_p\right] \quad (2)$$

Let, x_p be generated by means of ECI pertaining to the p^{th} row of the coefficient matrix, then the ECI elements for x_p can be identified as per (3).

$$I_{p_m} = \begin{cases} 1 & ; p = w \\ 0 & ; p \neq w \end{cases} \quad (3)$$

Since it is impossible to amalgamate all the generated packets and therefore it is hypothesized that the majority of the ECI elements exist as zero. In HM2-MAC, the coefficient information ECI is compressed using Huffman coding [73][74], which serves as compression-based encryption to alleviate any attack during multicast. It serves two purposes; first, it reduces the size of ECI, and second it makes data secure over multicast transmission. To perform Huffman coding, we used a simple arithmetic concept where the values and the location of the non-zero ECI elements are identified before compression. We applied a logarithmic function, $[log_2(generation\ time)]$ to estimate the location of the non-zero elements in the matrix. Since we consider merely the non-zero elements for compression, only I_{pm} is sufficient for compression and decoding at the sink node. We used an indicator of N −bits pertaining to the packet headers, which signify what "type of compression" based encryption applied. This parameter (i.e., $N = 1$) primarily depends on the number of compression method used by the node in the network. For further discussion, we represent "type of compression" N as compression and encryption methods identification flag (CEMIF). In case, the compression and encryption method require transmitting more packets, it needs to transmit uncompressed ECI so as to help sink for optimal decoding or the original data retrieval. In this method, the smaller value either of compressed or uncompressed ECI is transmitted over proposed multicast network. In such transmission, we assigned CEMIF as 0.

4.2 Computation at the Intermediate Node

Once receiving single packet combination from the upper layer or from a source node, the intermediate node performs two tasks, first it adds or appends other packets if there is any other packet to be transmitted towards the sink, and second it directly forwards the input packet to the sink. Moreover, if multiple packet combination reaching from the same packet generation, the intermediate node adds the packet elements (of the combinations) over the considered finite field. If an intermediate node receives l combinations, then the final output $x''$is estimated as per (4):

$$x'' = [1\ \ 1\ \ \ldots\ \ 1]_{1\times l} \begin{bmatrix} x_1' \\ x_2' \\ \vdots \\ x_l' \end{bmatrix}_{l\times 1} \quad (4)$$

In (4), the matrix components $(x_1', x_2', \ldots x_l')$ signify the l combinations. Now, employing CEMIF information, it identified the compression and encryption type. Though, the intermediate node can identify the CEMIF type and can decompose the input packets; however, since an unauthorized node doesn't have the coefficient matrix used for compression, it would not be able to decode the data. In case the intermediate node needs to transmit additional packet, it merely appends the input packets with the new packet and updates the ECI information as $(I''_1,\ I''_{2,} \ldots, I''_l)$. To update the ECI information we added m number of k bits from each combination, separately. The packet and allied ECI prepared for further transmission can be (5).

$$[I''_1\ \ I''_2\ \ \ldots\ \ I''_m]_{1\times m} = [1\ \ 1\ \ \ldots\ \ 1]_{1\times l} \begin{bmatrix} I'_{1_1} & I'_{1_2} & \ldots & I'_{1_m} \\ I'_{2_1} & I'_{2_2} & \ldots & I'_{2_m} \\ \vdots & \vdots & & \vdots \\ I'_{l_1} & I'_{l_2} & \ldots & I'_{l_m} \end{bmatrix} \quad (5)$$

Moreover, based on the compression method applied, CEMIF flag is updated before compression and further transmission.

4.3 Computation at the Sink Node

Once receiving packets from the intermediate node, a sink node at first extracts ECI with its coefficient matrix information. On the basis of the ECI obtained, the sink node identifies the coefficient matrix used to generate the packet combinations. Thus, gathering n packet combinations $(\hat{x}_1,\ \hat{x}_2,\ \ldots\ \hat{x}_n)$, with linearly independent coefficient vectors, it obtains the original data transmitted by the source node, using (6). Noticeably, for no packet errors possibility, the outputs of (6) only is considered as the original packet transmitted.

$$\begin{bmatrix} \hat{s}_1 \\ \hat{s}_2 \\ \vdots \\ \hat{s}_n \end{bmatrix}_{n\times 1} = \begin{bmatrix} \hat{q}_{1,1} & \hat{q}_{1,2} & \ldots & \hat{q}_{1,n} \\ \hat{q}_{2,1} & \hat{q}_{2,2} & \ldots & \hat{q}_{2,n} \\ \vdots & \vdots & & \vdots \\ \hat{q}_{n,1} & \hat{q}_{n,2} & \ldots & \hat{q}_{n,n} \end{bmatrix}_{n\times n}^{-1} \cdot \begin{bmatrix} \hat{x}_1 \\ \hat{x}_2 \\ \vdots \\ \hat{x}_n \end{bmatrix}_{n\times 1} \quad (6)$$

4.4 Multi-Generation Mixing

As already discussed in the previous sections, to enhance throughput and reduce computational cost (with reduced redundant packets), we applied MGM concept. In fact, we applied MGM concept to serve dual purposes, first to strengthen error-resilience and low avoidance, and second to reduce the number of redundant packets for resource efficient communication in MANET. The network coding methods at first encodes the data belonging to a specific generation and then it broadcast or multicast the encoded packet as linear mixture across the network. However, to ensure higher data reliability and error-resilience, it is required to transmit redundant packet for each generation, which can make overall system resource exhaustive, and can reduce the performance significantly. To alleviate such problem, in the proposed method we applied MGM concept in which the linear mixtures are obtained for the multiple generations and are transformed into certain combination sets. Subsequently, it performs amalgamation of the data packet belonging to a specific set to improve its error resilience [49]. Considering the overall size of the combination set be Z generations, as depicted in Figure 1. In our proposed model, we applied a position index of each generation, which is always appended in the combination matrix (say, combination set). In fact, it helps to indicate the position of the generation in the combination set. In case of the value of early generation be 1, and the final generation count in the combination set or matrix be Z, then the position index exists in between 1 and Z (i.e., $1 \leq \mathrm{d} \leq \mathrm{z}$, where d is the position of the current packet in the combination set or matrix). As discussed in the previous section, the source node at first combines the initial $d * n$ source packets linearly to generate $d * m$ linear combinations, provided $\mathrm{m} \geq \mathrm{n}$. To ensure reliable delivery to the receiver over considered MANET protocol, under a predefined probability of packet or link loss, it transmits $z * (m - n)$ redundant packet. Let, $[\mathrm{X_d}]_{\mathrm{n}\times\mathrm{s}}$ is the n source packets belonging to the dth generation in above stated combination set or combination matrix. Noticeably, in combination matrix or set each source packet is characterised as a $1 \times \mathrm{s}$ matrix (of symbols) retrieved from the Galois Field with size 2^{F}. In 2^{F}, F presents the order of the Galois field. Here, in multicast transmission, our proposed model obtains $\mathrm{A[C]_{m\times(d.n)}}$ matrix with rank $\mathrm{d} * \mathrm{n}$ at the source node. Thus, from the d-th combination matrix, we obtained m output packet mixtures (7).

$$[Y]_{m\times s} = [C]_{m\times(d.n)} \cdot [X]_{(d.n)\times s} \tag{7}$$

Thus, the generated m packet (say, combinations) pertaining to the $\mathrm{d} \cdot \mathrm{z}^{\mathrm{th}}$ generations are transmitted by the source node. In sync with the discussions made above, the process at the intermediate node is followed same as that of native random linear network coding. In this mechanism, the proposed method encodes the received packet combinations pertaining to the same generation. The details of the processes at the intermediate node remains same as discussed above. Subsequently, once receiving the data packet combinations from a combination set, sink node performs decoding of the $d * n$ MGM packets while maintaining or conditioning that the rank of the received matrix from the initial d generations be $d * n$.

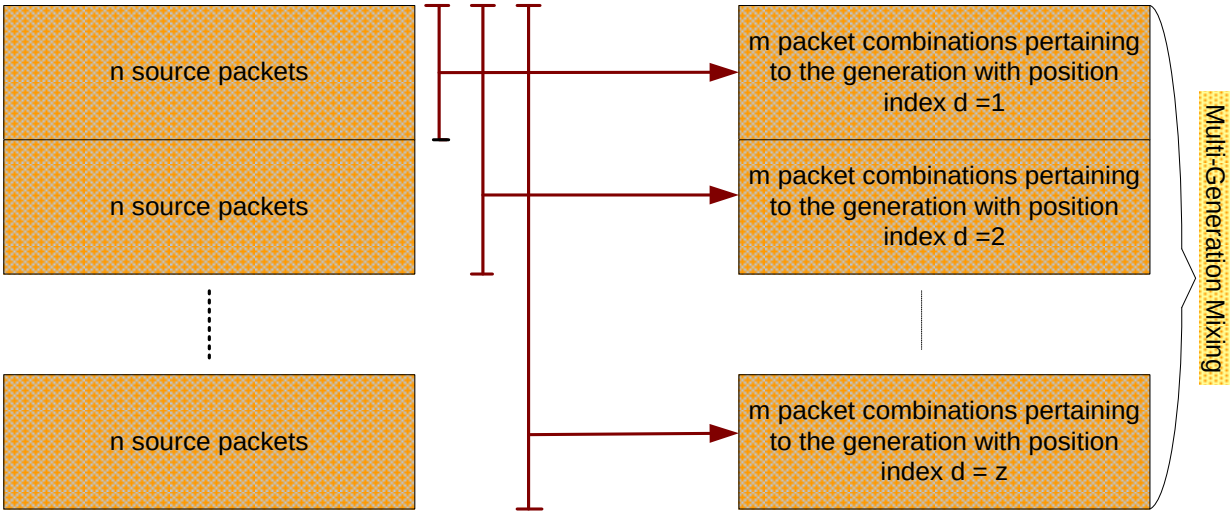

Figure 1 MGM based packetization

Let, $d * n$ packets be $\left[[\hat{C}]_{(d.n)\times(d.n)}[\hat{Y}]_{(d.n)\times s}\right]$, where $[\hat{C}]_{(d.n)\times(d.n)}$ be the coefficient matrix used for generating the (received) packets $[\hat{Y}]_{(d.n)\times s}$, our proposed model decodes and retrieve the data using (8).

$$[\hat{X}]_{d.n\times s} = [\hat{C}]^{-1}{}_{(d.n)\times(d.n)} \cdot [\hat{Y}]_{d.n\times s} \tag{8}$$

Noticeably, in case of lossy network, whose probability can't be ignored in MANETs, $(\mathrm{m}-\mathrm{n})$ redundant packets are generated from d generations. These redundant packets can be employed during decoding at the receiver, if the sink node doesn't receive sufficient number of packets. It is also used as error-resilience measure to help in achieving reliable data transmission. Unlike classical methods where $z*(m-n)$ redundant packets are transmitted to support error-resilience and decoding, in our proposed method the redundant packets are generated for multiple-generations altogether or single for many-generations. It reduces the number of redundant packets significantly and also reduces the radio utilization as well as allied resource (say, energy and computation0 exhaustion. It helps achieving QoS demands. To further enhance resource efficiency or spectrum utilization, once the sink node receives the sufficient number of packet combinations to decode its data successfully, the at-hand buffer carrying data packets and redundant packets are flushed. This process is performed iteratively to maintain maximum possible resource availability for large data transmission in MANETs. It helps preserving radio spectrum and hence increases network scalability and transmission ability.

4.5 Network Condition Awareness Decoding Optimization

Considering the fact that MANET can often undergo dynamic topology and even loss condition due to relative location changes, contention etc., we enhanced HM2-MAC with content aware decoding concept. Unlike classical maximum likelihood-based approaches, we designed HM2-MAC in such manner that it exploits network as well as allied data conditions to decode the data. In fact, the key motive behind our proposed approach was to reduce the trade-off between the lower redundant packers and higher or optimal decoding efficiency. To achieve it, we focused on enhancing decoding probability at each generation, by distributing redundant packet(s) in such manner that it would help decoding all data packets even with lower redundancy. Summarily, our proposed method intends to optimize the decoding probability at each generation to meet QoS demands. Noticeably, to simulate link loss with targeted MANET network, we applied Gilbert-Elliot Link Loss (GELL) model, where decoding efficiency with different loss-probability or loss-conditions were examined. Recalling the fact that MAC layer has the unparalleled significance towards throughout and reliability enhancement. Considering this fact, we designed our proposed MGM assisted HM2-MAC model in such manner that it could enable maximum or optimal data decoding probability. Let, the likelihood of a coded packet (i.e., EPDU) reaching to the sink node be α_{avg}., which can be estimated as per (9).

$$\alpha_{avg} = \frac{\sum_{v=1}^{\varphi} \alpha_v}{\varphi} \tag{9}$$

Let the initial data packets or units be projected as (receiving the data from application layer), a set of packets signifying (10).

$$= \sum_{d=1}^{\mathrm{z}} \mathrm{n_d} \tag{10}$$

In above equation, the variable z signifies the total number of generations, while $\mathrm{n_d}$ be the total source packets generated in a specific generation with the position index d. As already discussed in the previous sections, the source packets are combined with the coefficient information from the Galois Field in linear manner and thus generates $\sum_{d=1}^{z} m_d$ packets pertaining to the different (say, multiple) generations $g_1, g_2, \ldots, g_z$. Let, m_d be the total encoded packets pertaining to the g_d generation, conditioned with $0 < d \leq z$. Noticeably, these packets are generated by combining $\sum_{\mathrm{v=1}}^{\mathrm{d}} \mathrm{n_v}$ packets linearly. Thus, the optimal number of coded packets required to be generated to ensure optimal decoding likelihood at the receiver node is obtained as per the following mechanism. In our proposed model, MAC has been designed in such manner that it can help a sink node to decode the data collected from the $\mathrm{g_d}$th generation and its descendent $g_1, \ldots\ldots, g_{d-1}$, only when it received $\sum_{\mathrm{v=1}}^{\mathrm{d}} \mathrm{n_v}$ linearly dependent packet combinations from the different generations $\mathrm{g_1}, \ldots \mathrm{g_d}$. In HM2-MAC protocol a sink node can decode packets of each generation (i.e., $\mathrm{g_1}, \ldots, \mathrm{g_d}$) in case the data for the generation $\mathrm{g_{d'}}$ (where $0 \leq d' < d$) has been decoded and $\sum_{v=d'+1}^{d} n_v$ number of linearly independent encoded packets have reached to the sink from their respective generations($\mathrm{g_{d'+1}}, \ldots\ldots, \mathrm{g_d}$). Let the likelihood of $\mathrm{g_d}$ packet decoding be ς_d, then in that case with $\mathrm{d} = 1$, ς_1 can be considered equal to the likelihood of receiving minimum $\mathrm{n_1}$ encoded packets out of the total of $\mathrm{m_1}$ coded packets generated from the generation count g_1. In this manner, we achieve the probability of the packet decoding as (11).

$$P_{dec}(n, m, \alpha_{avg}) = \sum_{v=n}^{m} \binom{m}{v} \alpha_{avg}{}^{v} (1-\alpha_{avg})^{m-v} \tag{11}$$

The decoding probability is obtained using (12).

$$\varsigma_1 = P(n_1, m_1, \alpha_{avg}) \tag{12}$$

In the same manner, if the packet combination for the generation g_1 is decoded successfully, the probability of successful decoding of n_2 packet combinations from the generation g_2 be ς_2, which can be estimated as per (13). Thus, the data packets from the different generations g_1 and g_2 can be decoded completely when the sum of packet-mixtures $n_1 + n_2$ is received from the respective generations.

$$\varsigma_2 = \varsigma_1 . P\big(n_1, m_1, \alpha_{avg}\big) + (1 - \varsigma_1) . P\left(\sum_{v=1}^{2} n_v , \sum_{v=1}^{2} m_v , \alpha_{avg}\right) \tag{13}$$

Similarly, the probability of data decoding for $z$generations can be obtained as per (14).

$$\begin{aligned}\varsigma_z \; = \varsigma_{z-1} . P\big(n_z, m_z, \alpha_{avg}\big) + (1 - \varsigma_{z-1}) . \varsigma_{z-2} . P\left(\sum_{v=z-1}^{z} n_v , \sum_{v=z-1}^{z} m_v , \alpha_{avg}\right) + \cdots \\ + (1 - \varsigma_1) . (1 - \varsigma_2) \ldots . (1 - \varsigma_3) . P\left(\sum_{v=1}^{z} n_v , \sum_{v=1}^{z} m_v , \alpha_{avg}\right)\end{aligned} \tag{14}$$

Thus, employing above derived probability factors (14-16), we estimate the total decoding probability ς_d using (15).

$$\varsigma_d = \begin{cases} P\big(n_1, m_1, \alpha_{avg}\big) & ; d = 1 \\ \begin{cases} \varsigma_{d-1} . P\big(n_d, m_d, \alpha_{avg}\big) + \\ \sum_{v=1}^{d-1} \left[\varsigma_{d-v-1} . \prod_{w=d-v}^{d-1} \left((1 - \varsigma_z) . P\left(\sum_{w=d-1}^{d} n_w , \sum_{w=d-1}^{d} m_w , \alpha_{avg} \right) \right) \right] \end{cases} & ; d \geq 1 \end{cases}$$

Let, the decoding probability of g_d (for z generations) be ρ_d, then for $d = z$, we consider

$$\rho_z = \varsigma_z \tag{16}$$

In the same manner, with $\mathrm{d} = (\mathrm{z} - 1)$,

$$\rho_{z-1} = \varsigma_{z-1} + (1 - \varsigma_{z-1}) . \varsigma_z \tag{17}$$

For d =1,

$$\rho_1 = \varsigma_1 + (1 - \varsigma_1) . \varsigma_2 + \cdots + (1 - \varsigma_1) \ldots (1 - \varsigma_{z-1}) \varsigma_z \tag{18}$$

Employing above derived probability functions (16-18), we obtain the generalized probability of optimal decoding as (19).

$$\rho_d = \begin{cases} \varsigma_d & ; d = z \\ \varsigma_d + \sum_{v=d+1}^{z} \left[\varsigma_v . \prod_{w=d}^{v-1} (1 - \varsigma_w) \right] & ; d < z \end{cases} \tag{19}$$

Thus, the average decoding probability $\bar{\rho}$ for MGM based transmission is derived as (20).

$$\bar{\rho} = \frac{\sum_{d=1}^{z} \rho_d}{z} \tag{20}$$

The key significance of $\mathrm{m}_1, \mathrm{m}_2, \ldots, \mathrm{m}_z$ is that it considers the maximum decoding probability $Max(\bar{\rho})$ in such manner that it follows the condition given in (21).

$$\sum_{d=1}^{z} (m_d) = R \tag{21}$$

In (21), the variable R states the addition of the packet combinations which can be transmitted per multi-generation in the assigned bandwidth. In this manner, our proposed HM2-MAC model intends to transmit optimal set of packets per generation in such manner that it retains maximum possible packet decoding success at

the receiver, even under link or network loss possibilities. It can be of great significance to meet QoS expectations in MANETs.

4.6 MAC Implementation

Figure 2 presents the general architecture of IEEE 802.11 MAC protocol serving MANETs communication. The illustrated model signifies the functional architecture of the downlink IP packet flow in MANETs 802.11 protocol stack. As depicted, it embodies a conversion protocol at application layer, where the IP data packets enters the node and is further transmitted to the radio link or network control later layer, before entering into MAC. Performing header compression, the input packet stream is processed for segmentation and (packet) concatenation so as to fit into 802.11 MAC's frame dimension or size. In classical MAC models, these packets are further mapped to fit into PHY transport block. Unlike classical 802.11 MAC solution, in this research our proposed HM2-MAC model is applied as sublayer of the native MAC. This approach helps retaining backward compatibility for MANETs. In 802.11 protocol or its variants such as 802.11b, MAC (frame) delivery primarily relies on the acknowledgement support, and in case (automatic) repeat request fails, the above layer (say, RLC layer) uses acknowledgement mode by using supplementary redundant packets to ensure packet delivery. However, it imposes overheads in the form of redundant packets, signaling cost, energy exhaustion etc. Therefore, to alleviate above stated problem we applied HM2-MAC as the sublayer of 802.11 MAC (Figure 3).

Functionally, the data to be transmitted is mapped into PHY transport block (PHY TB) which is further mapped to time-frequency resource on the wireless link. In general, these mapped data are also called as resource block pair in contemporary advanced wireless networks such as long-term evolution (LTE). Typically, each resource block pair is equal to 1 milli-second time, which is also referred as transmission time interval (TTI). However, the size of transport block (TB) in each TTI relies on multiple factors such as modulation techniques, Acknowledge Model, number of resource block pairs, and channel quality information. However, the number of resource block pairs and acknowledge model are the decisive factors applied to decide PHY TB size. Noticeably, the acknowledgement model primarily depends on the MAC scheduler which exploits channel quality information to decide the size of packet and hence PHY TB. The classical 802.11 MAC solutions, with acknowledgement mode imposes significant computational and signaling overheads, especially during forward error check, which forces the network to undergo delay and resource exhaustion. A solution often used is that the IP packets can directly be transmitted in parallel, autonomous and time-interleaved transmission of MAC frames. It is often supported by means of acknowledge mode architecture, in which the packet is accepted once RLC or MAC segment reaches to the destination node. However, it functions at the cost of increased delay and signaling overhead. Unlike above stated MAC solution, in our proposed model RLC/MAC packets or frames are processed for compression and proposed encoding before mapping it to the transport block for further transmission. It makes our proposed multicast transmission secure and reliable to ensure QoS provision in MANET. Unlike classical approach, HM2-MAC based 802.11 protocol, RLC packet is further split into multiple packets or source symbols to be further processed for proposed networking coding.

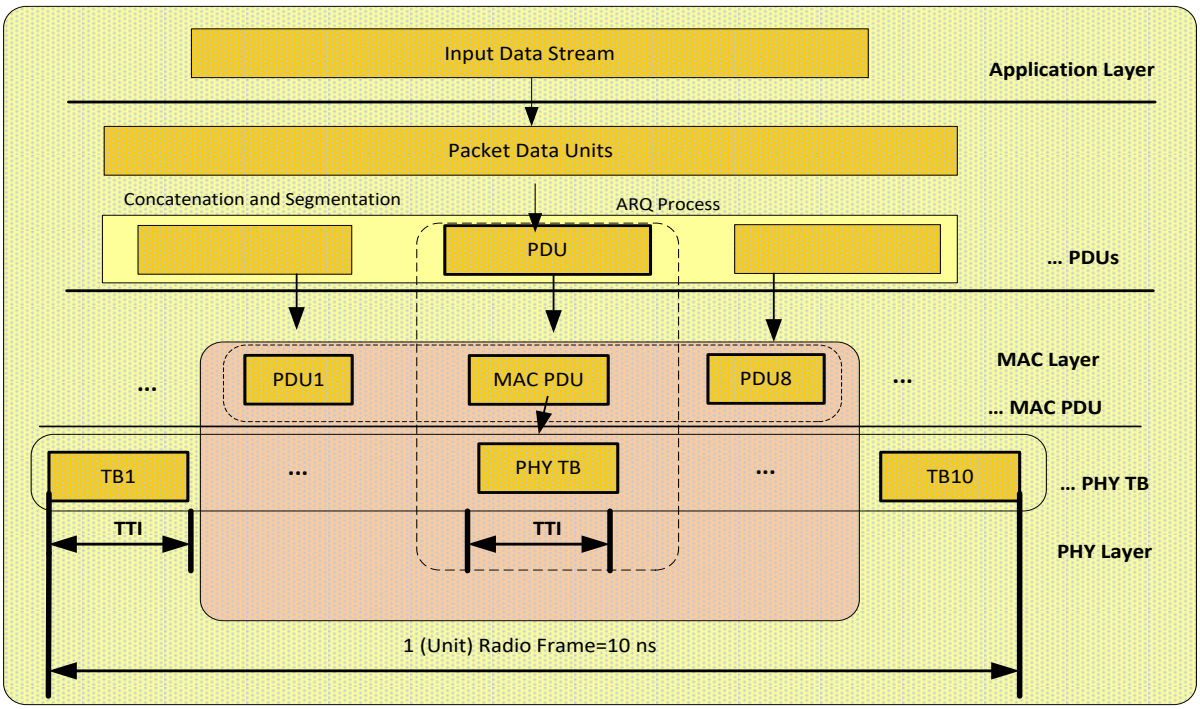

Figure 2 IEEE 802.11 MAC solution

Figure 3 presents the overall proposed method and its implementation. As depicted in Figure 3, the proposed HM2-MAC model generated equal-length packets which were later collected into a MAC frame to fit into the transport block at the PHY layer. Thus, the MAC frames are collected in PHY TB (Figure 3), and the received TB (along with the redundant packets) at the receiver node is decoded as per the decoding method discussed in the previous sections. However, this decoding takes place at the IEEE 802.11 sub-layer, i.e., HM2-MAC layer. In the same time, once getting linearly independent encoded packets or MAC frame from the above layers, the receiver's MAC responds back with an acknowledgement message followed by iterative buffer flush, which flushes the buffers occupied by the already transmitted packets. Additionally, this acknowledgment also serves a purpose to decide RLC packet transmission to ensure dynamic (QoS-centric) packet scheduling.

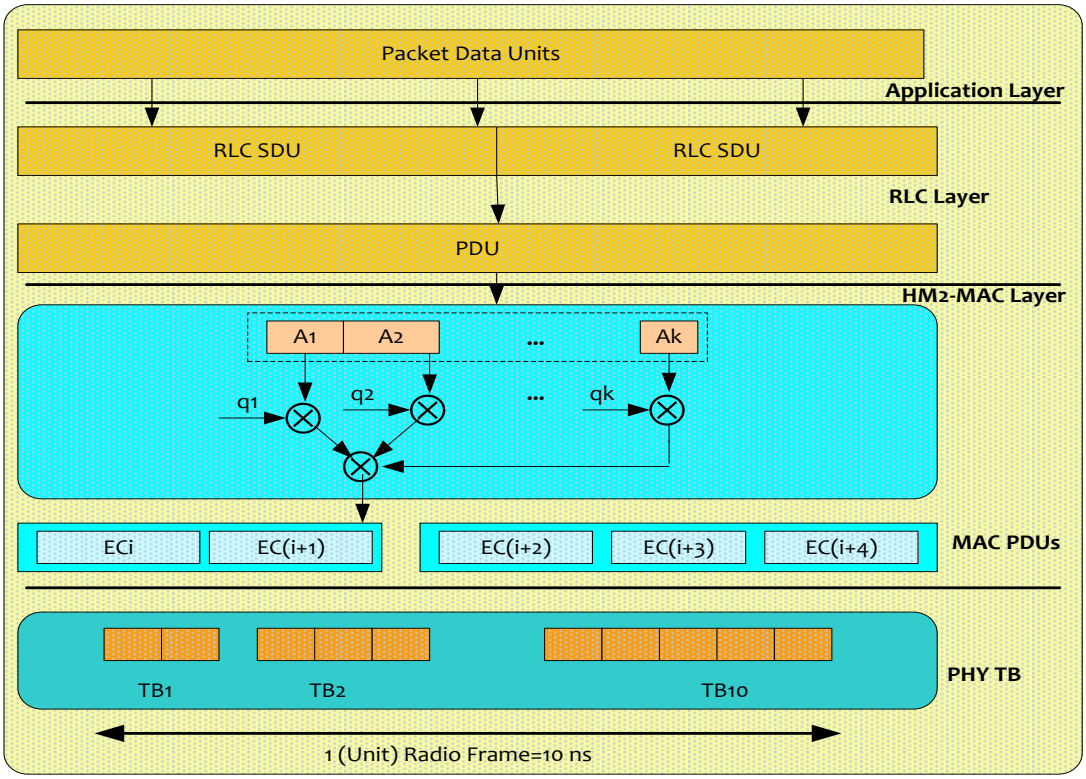

Figure 3 Proposed MGM assisted HM2-MAC architecture

The detailed discussion of the simulation results and allied inferences is given in the subsequent sections.

5. Results and Discussions

MANET, being a decentralized and infrastructure-less network has gained wide-spread attention because of its suitability towards mobile routing based wireless communication ability. However, aforesaid network characteristics broadens the horizon for intruders or malicious node to become a part of routing table or forwarding path. In major cases, malicious nodes mimics or behaves like a genuine node and get attached to the routing table for further routing-decision or packet forwarding. Unfortunately, such malicious nodes or intruders once becoming the route member starts misbehaving and either pollute the original data packets or denies services or even drop the packets. Such events often lead to the performance degradation and hence QoS compromise. On the contrary, the contemporary as well as NextGen communication systems employing MANET as routing technology demands QoS assurance with optimal data security. Majority of the classical approaches either focus on security or QoS support; on the contrary maintaining optimality of the duo is inevitable. Though, a few approaches were developed for routing-based data security or encryption-based security; however, their computational overheads or complexity confined their applicability in real-world applications. Most of the existing approaches can be stated to undergo higher signaling overheads, resource exhaustion etc. Unlike routing-based approaches MAC based systems have higher potential to meet both data security as well as QoS support; however, there are very less efforts made to explore MAC efficiency towards QoS and data security together. Considering these facts, in this paper we focused on designing a state-of-art new MAC routing protocol or architecture which could retain both QoS as well as data security, especially for MANET, a mobility based wireless routing technology. To achieve it, in this paper we inculcated a recently proposed information theoretic concept named network coding algorithm. Unlike classical encryption or cryptosystems network coding possesses efficacy in terms of low-computation and error-resilience, which can be effective towards data security as well as QoS support. However, majority of network coding concepts have been designed for static network such as wireless sensor networks, where the probability of intermediate node malicious behavior is relatively lower. On the other hand, in MANETs, there can be unknown or even random intermediate node willing to be a part of routing path or access the resource. Such nodes can even cause network failure, packet loss or even might pollute the original data. Though, to alleviate such problems authors have proposed homomorphic encryption or other cryptographic algorithms, their computational overheads and reduced throughput probability can't be denied.

Considering above stated problems, in this paper we focused on designing a robust MAC solution which could retain both QoS assurance as well as data security. To achieve it, we designed Huffman coding assisted multi-generation mixing based random linear network coding algorithm for MAC design (HM2-MAC). As the name indicates, we designed HM2-MAC in such manner that the use of Huffman coding, which is a well-known and loss-less compression-based encryption technique for data security as well as resource efficiency. Here, we applied MGM so as to reduce the number of redundant packets that can make overall routing architecture resource efficient. Thus, the use of MGM-RLNC with Huffman coding enabled our proposed model to retain resource efficiency as well as data security (especially resilience towards any possible pollution attack or manipulation by intruder(s)). To further enhance resource efficiency, we designed HM2-MAC in such manner that it encodes a very limited source data (packets), which reduces computational overheads as well as buffer utilization. While, a function called iterative buffer flush which empties the buffer occupied by the delivered packets makes our proposed model more effective to reserve more memory to accommodate higher transmission rate. HM2-MAC was designed in synch with error possibility, where the redundant packets were selected minimally while retaining maximum or optimal decoding possibility at the destination or sink node. In other words, HM2-MAC enabled selection of minimum redundant packets to be transmitted along with source packets, where the number of such packets are decided based on error probability at the sink node. It makes our proposed model more efficient to decode data packets without repetitive acknowledgement or retransmission overhead. Noticeably, the overall proposed HM2-MAC model was applied as a sub-layer of native IEEE 802.11 MAC protocol, which not only achieves QoS expectation, but also supports backward compatibility. Thus, it can easily be applied with real world routing applications.

To simulate the proposed model, we designed MANET network as a butterfly architecture with single source and multiple sink nodes. Being multicast transmission, we considered two sinks with multiple intermediate nodes and allied paths. Considering MANET as a mobile network with varying topology and loss condition, we designed overall network with Gilbert Elliot Model with different loss probability. Here, we simulated the network with the loss probability of 2.5%, 5%, 10%, 15%, 20% and 25%, with respect to which the throughput was obtained. Additionally, packet loss with the different loss probability was examined in this work. Considering QoS expectations of the MANET, where it expects throughput to be higher, resource utilization to be higher, low

packet loss, higher network carrying capacity etc., we obtained the performance outputs in terms of throughput, packet loss over varying payload and loss conditions. Additionally, we examined the number of redundant packets and its demand to enable optimal throughput performance. To be noted, for resource efficient routing maintaining lower number of redundant packets is must. Moreover, realizing the fact that security strength of network coding primarily depends on the size of Galois Field, we examined performance with the different GF sizes. Similar to the redundant packets, we hypothesize that maintaining lower GF size can be computationally effective and resource efficient. The overall proposed model was developed using MATLAB 2019b software tool. The simulated results and their respective inferences are discussed in the subsequent sections. The performance assessment has been accomplished in two manners; first intra-model assessment and second, inter-model assessment. In intra-model performance characterization, we varied different network parameters such as payload (symbols per packet), number of generations in MGM, redundant packets, link loss and GF counts. Varying aforesaid parameters, the performance has been obtained in terms of throughput and packet loss. On the contrary, for inter-model performance assessment, we focused on comparing the performance of our proposed HM2-MAC protocol with other MAC architecture. The details of the results obtained is given as follows.

5.1 Intra-Model Performance Assessment

To perform intra-model performance assessment, we focused on analyzing the throughput and packet-loss performance by varying payload, generation size, Galois Field size, number of redundant packets and link-loss variations. Figure 4 presents the throughput performance by varying symbols per packet, also called payload. Noticeably, we obtained throughput as the ratio of total packets received to the total number of transmitted packets. Observing the results even over varying payload size, the throughput has been found more than 99%. The maximum throughput obtained over varying payload size was found 99.6%. Recalling the fact that the proposed HM2-MAC protocol performs error-resilient multi-generation mixing followed by packetization, its efficiency to delivery higher throughput can be well justified. Additionally, the use of Huffman coding compression with minimum pollution attack enabled proposed model to attain higher throughput, due to minimum packet loss as depicted in Figure 5. The packet loss (%) as observed through Figure 5 depicts that the average packet loss, even over the payload of varying sizes retains lower than 1%. It shows the robustness of the proposed HM2-MAC model to meet Qo demands in contemporary MANETs based IoT or M2M communication.

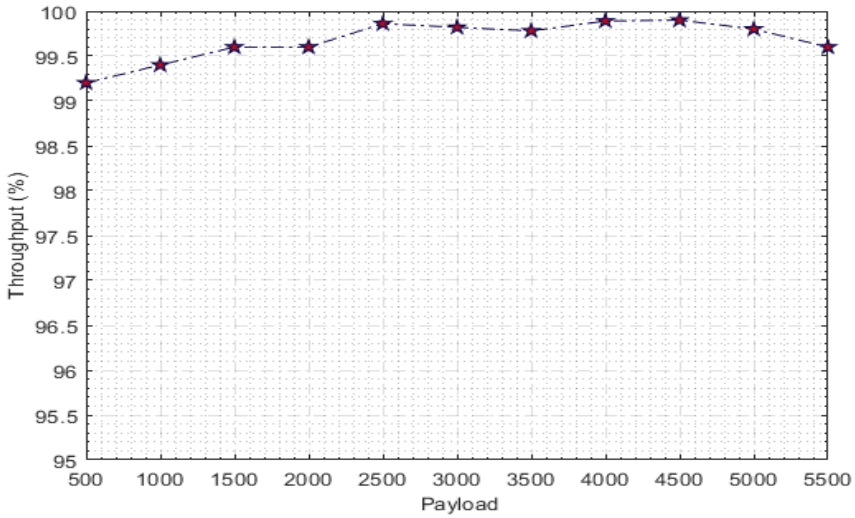

Figure 4 Throughput Vs Payload

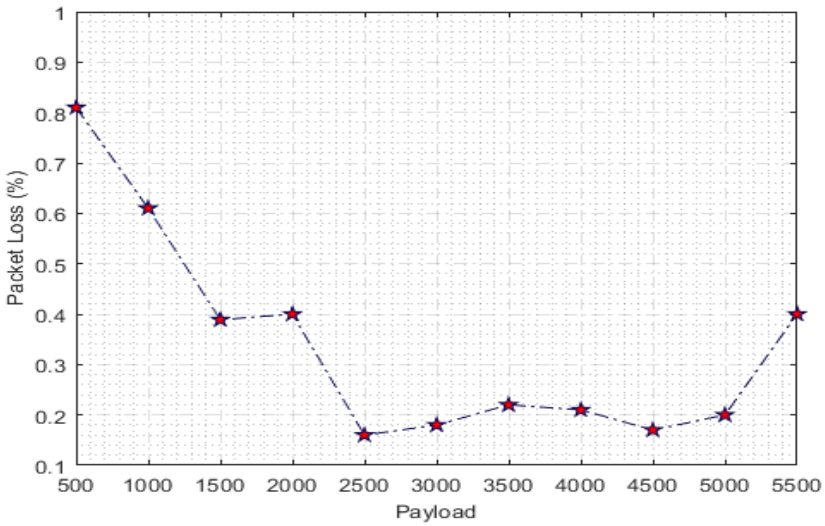

Figure 5 Packet loss Vs Payload

Figure 6 presents the throughput performance over different number of generations. Noticeably, to reduce the number of redundant packets during transmission our proposed HM2-MAC protocol employed the concept of number of generations, also called multi-generation mixing concept. Here, unlike one for each generation, we employed one for multiple generations (mixed) redundant transmission. The prime intend behind this concept was to reduce redundant packets and allied resource exhaustion in the form of transmission energy and buffer utilization. However, maintaining lower redundant packets (here, in Figure 6, we maintained redundant packets as 1) over higher number of generations might force a sink node to suffer packet loss, especially under mobility or topological changes, which is normal in MANETs. To be noted, with increase in the number of generation (eventually the size of packets per generation in MGM) a sink node requires more redundant packets to ensure higher throughput. However, since we focused on retaining lower redundant packets even with higher number of generations in MGM, we observed average throughput more than 97%. It seems satisfactory for at-hand M2M communication or MANET based IoT purposes. In this reference, we assessed whether increasing redundant packets can achieve significantly higher throughput or not. We examined the performance with two different set of redundant packets; 1-RGM, 2-RGM and 3-RGM, signifying one, two and three redundant packet per MGM, respectively. Figure 7 shows throughput performance with different redundant packet sizes. Observing the results, it can be found that the throughput performance with 1,2 and 3 redundant packets (i.e., 1-RGM, 2 RGM and 3-RGM, correspondingly) retains near same performance with merely 0.8% average throughput variation. It signifies that the proposed HM2-MGM concept can be well-realized even with single redundant packet per MGM for multicast transmission in MANET. It can reduce buffer or resource utilization as well as signaling overhead, which can eventually help significantly to preserve QoS in MANETs.

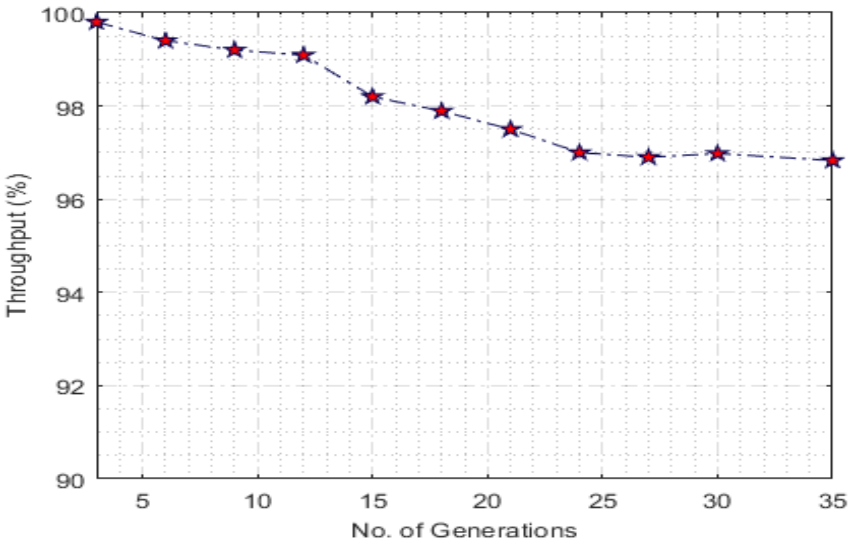

Figure 6 Throughput Vs No. of Generations

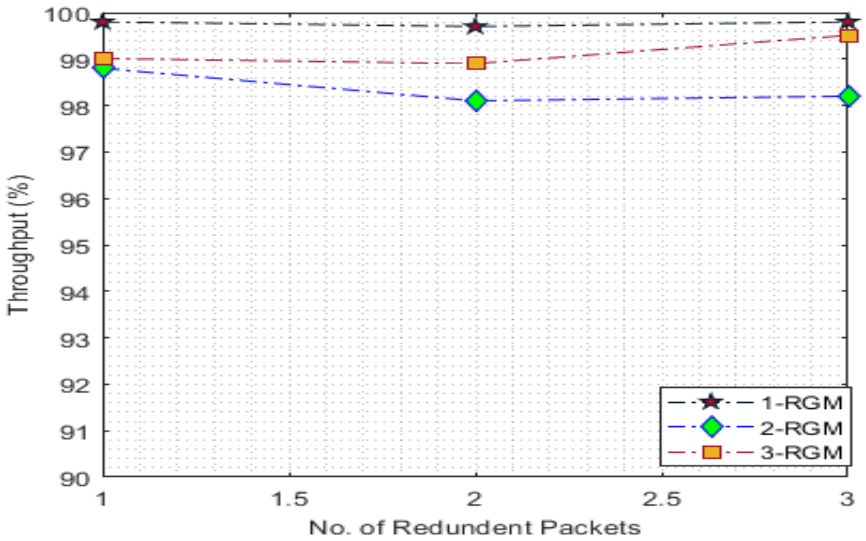

Figure 7 Throughput Vs No. of Redundant packets per generations or MGM

With mobility and exceedingly high topological changes, the probability of link loss can't be ignored in MANETs. Considering this fact, we simulated the proposed model with Gilbert Elliot Model based link-loss probability, where we examined throughput performance by varying link-loss probability as 0.0025, 0.0050, 0.0075, 0.010, 0.0125, 0.0150, 0.0175, 0.020, 0.0225, 0.025, and 0.0275. The throughput performance obtained by our proposed HM2-MAC based MANET is given in Figure 8. As depicted (Figure 8), the maximum throughput by HM2-MAC is almost 100%, while even with higher link-loss probability, it retained average throughput more than 96%. It signifies robustness of the proposed MAC design. The results reveal that the proposed HM2-MAC model is capable to ensure optimal performance even under changing network conditions. It also shows its efficacy towards higher reliability and hence QoS assurance for MANETs.

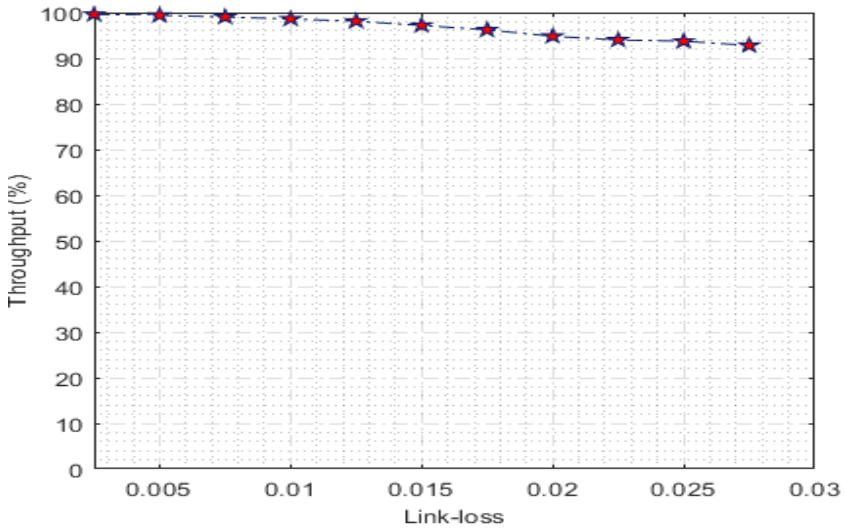

Figure 8 Throughput Vs Link-loss (in dB)

The above discussed results affirm that the proposed model achieves optimal throughput, even under varying link-loss conditions, with low redundant packet transmission or low computational and signaling overheads. It also affirms robustness of the proposed model to achieve QoS support in MANETs. In majority of security models applying cryptography or encryption concepts for data security, authors suggest applying higher coefficient size. Even with network coding-based approaches, different classical methods suggest to use higher Galois Field size. Though, it helps achieving higher level of security; however, at the cost of increased computational overheads and signaling overheads. To assess performance, we examined throughput by simulation proposed HM2-MAC with different Galois Field (GF) sizes. Figure 9 presents average throughput performance with the different GF sizes, which we assigned 4, 8, 16 and 32. The results obtained (Figure 9) revealed that the proposed HM2-MAC protocol shows average throughput of 99% with GF size of 4. Similarly, with GF=8, we find throughput 99.6%, and 99.4% throughput with GF=16. With GF=32, the average throughput performance

obtained is 94%. Observing this result, it can easily be found that the proposed model exhibits the highest throughput of 99.6% with GF=8. Though the overall performance with different GF sizes is close enough to be signifies as near-equal performance (Min-99.3%, Max. 99.6%). This result (Figure 9) affirms that the proposed HM2-MAC protocol with GF=8 can achieve satisfactory performance even with lower computational overheads.

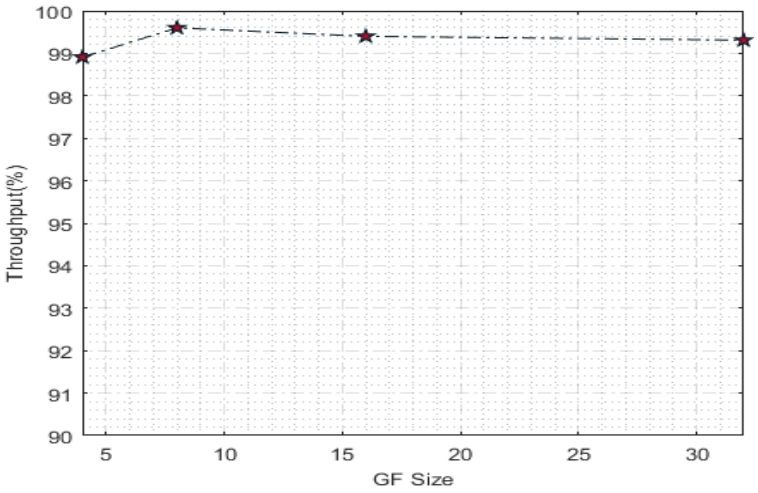

Figure 9 Throughput Vs Size of the Galois Field

Thus, observing overall results, it can be found that the proposed HM2-MAC model achieved reliable and resource efficient multicast transmission over MANETs and hence achieves QoS assurance. The results obtained signifies efficacy of the proposed model with higher data rate (transmission). In addition to the above discussed performance outcomes, the inclusion of iterative buffer flush can enhance overall resource efficiency of the MAC protocol. It can eventually help to achieve QoS provision for MANETs.

5.2 Inter-Model Performance Assessment

To assess relative performance by our proposed HM2-MAC protocols, we considered different secondary source information from the state-of-art existing methods, especially secure MANET protocols. Recalling the fact that in our proposed HM2-MAC model the emphasis is made not only to support security but also QoS provision for MANET. In this reference, we considered a recent work [1] in which authors proposed a game-theoretic model towards reliable data transmission in Futuristic MANETs. To inculcate security amongst the participating node, authors applied incentive-based concept in a cooperative communication environment. In their research authors examined performance in terms of throughput and packet loss. The maximum throughput observed by authors [1] was found to be almost 100%, which is close enough to our proposed HM2-MAC model, which achieves the highest throughput of 99.8%-100%. Interestingly, authors found their approach to undergo packet loss or packet drop of 24 bits per second, which is significantly large to ensure optimal network performance. On the contrary, the results obtained by our proposed HM2-MAC based MANET has exhibited significantly low packet loss (Figure 5) even under high loss condition. It shows robustness of our proposed model over existing method [1]. Similarly, authors in [2] proposed a trust-based predictive model for MANET in IoTs. The highest packet delivery rate (estimated as the average data transmission) was obtained as 92%, which was also found decreasing over increase in the number of malicious nodes. The minimum throughput observed was almost 45%, which is significantly lower in comparison to our proposed HM2-MAC based MANET protocol. A similar work was done in [3], where Chatterjee et al. could achieve the highest packet delivery rate of 92%. Thus, in comparison to the above stated [1-3] methods, our proposed HM2-MAC model achieves better performance. Authors in [4] focused on enhancing data transmission reliability; however, the maximum throughput obtained was 95%. However, their approach [4] was found undergoing reduced packet delivery rate with increase in payloads. In comparison to their proposed method, our proposed HM2-MAC based MANET achieves significantly high throughput, which guarantee reliability of data transmission even under varying topology or network conditions. In [5], authors proposed hierarchical message authentication code for secure data dissemination in mobile ad hoc networks (HiMAC). This approach was designed as an identify-based message authentication code for data security in MANET. The average success rate (say, packet delivery rate) obtained by authors [6] was merely 91%, which is significantly lower than the proposed HM2-MAC based protocol. The highest success rate by HiMAC was 96%, which is still lower than the proposed HM2-MAC protocol. The highest successful packet delivery rate by Secure Ad Hoc On-Demand Distance Vector Routing (S-AODV) was 82%. In

comparison to S-AODV, our proposed HM2-MAC based MANET routing protocol shows almost 18% higher success rate, which signifies its robustness towards QoS-centric secure communication in MANETs. Blackhole protected AODV routing protocol for MANETs based on chaotic map was proposed in [7]. Though, authors examined their performance in different parameters; however, packet delivery ratio signifying overall transmission success rate was found near 97%, which is lower than our proposed HM2-MAC based routing model. Authors in [72] developed preamble time division multiple access (TDMA) fixed slot assignment protocol for IEEE 802.11b MAC, where the maximum success rate was found to be approximately 94%, which was even found decreasing with increase in mobility. Its decrease in performance can be hypothesized with increase in link-loss which is common in MANET. Therefore, in reference to the existing method [72], our proposed HM2-MAC based IEEE 802.11 protocol performs superior to meet QoS as well as secure data transmission demands. Thus, taking into consideration of the different existing methods and their relative performance, it can be found that the proposed HM2-MAC routing model achieves or exhibits better and reliable multicast transmission to meet QoS and data security demands.

5.3 Security Analysis

The above discussed results affirm the suitability of robustness of the proposed HM2-MAC routing model towards QoS assurance in MANET; though the overall proposed model was designed in such manner that it ensures data security as well. Towards this objective, the efficiency of MGM based RLNC and Huffman coding concept can have undeniable significance. Though, Huffman coding is a compression algorithm also called prefix coding; however, it follows the concept of compression-based encryption. The key novelty of this approach is that it encodes the data as well as retains better attack-resilience. In this reference, the strategic amalgamation of MGM-RLNC and Huffman coding concept enabled HM2-MAC to perform multicast transmission without getting any threat from possible pollution attack. In fact, the proposed model alleviates the probability of pollution attack, due to the reason that it doesn't involve decoding of the source packet at the intermediate node(s). It makes proposed HM2-MAC protocol more efficient to alleviate any probable attack during the course of transmission. Since, in the proposed method the coefficient information with which the source node encodes the input packet is known only to the sink node or the destination node; no intermediate node can have the access to the data. Or no intermediate node can decode the information or packet being transmitted over MANET. Unlike major existing MAC protocols which merely focus on malicious node identification and its avoidance during routing decision, our proposed HM2-MAC model will alleviate major possible attacks at the link layer. Summarily, the proposed system maintains a better trade-off between QoS assurance and data security over multicast transmission in MANETs for NextGen communication including M2M and IoT ecosystems.

6. Conclusion

MANET has been recognized as one of the most employed networks these days due to its decentralized and infrastructure-less communication ability. It enables MANET to be used in varied purposes including vehicular ad-hoc networks, M2M, IoT ecosystems, localized network solution during natural disasters, flood etc. However, being mobile in topology and predefined infrastructure less network, it often undergoes adversaries, especially QoS performance and security. Mimicking like a genuine node, an intruder or malicious node can be a part of routing path that can later affect overall performance adversely. It can even drop the packets or can deny responding for routing decision, which can cause QoS degradation. To address such issues, amongst the major solutions MAC-based approaches are found more realistic and promising than routing-based concepts. As viable solution, ensuring optimal balance in between QoS performance and security is of utmost significance for which network coding concept can be of great significance. However, majority of the classical network coding-based methods undergo adversaries like pollution attack caused due to malicious node within the network. Though a few methods like encryption and homomorphic encryption assisted network coding have been proposed for MAC design; however, increased computational overheads and complexity reduces their efficacy to meet contemporary or NextGen MANET communication demands. Considering this fact, in this research paper a novel and robust MAC design was proposed for MANETs. The proposed MAC protocol intended to retain both QoS as well as data security with minimum computational overheads and exhaustion. To achieve it, at first an MGM assisted RLNC model was developed which ensured error-resilient multicast transmission over MANET. Here, the use of MGM enabled minimum redundant packet, while error-resilient (using loss-probability sensitive MAC scheduling) MAC packet scheduling strengthened its reliable transmission even under loss condition or probability. To ensure safety of the data packets, the proposed HM2-MAC model incorporated Huffman coding concept, which is one of the best performing compression methods. Noticeably, here Huffman coding acts as a compression technique to be further used for data encryption. It follows the concept of compression-based encryption to secure packets under transmission and avoid any probable pollution attack. Additionally, the proposed HM2-MAC design incorporated an iterative buffer flush technique which flushes buffer or memory once delivering packets to the sink node, without waiting for acknowledgement. It strengthened our proposed model to

retain better resource as well as delay efficiency. HM2-MAC has been applied as a sub-layer of IEEE 802.11 MAC that retains backward compatibility as well, and hence doesn't demand major changes in protocol stack. Realizing topological changes and hence link-quality variations (say, link loss probability), the proposed MAC routing model was simulated with the different loss conditions. The overall simulation results exhibited better throughput performance even over different link-loss probability. Thus, the proposed system retains both QoS expectations as well as secure data (multicast) transmission, which can be of great significance for real-world MANET communication systems.

References

[1] Khan B. U. I., Anwar F., Olanrewaju R. F. Pampori B. R & Mir R. N. (2020). A Game Theory-Based Strategic Approach to Ensure Reliable Data Transmission with Optimized Network Operations in Futuristic Mobile Adhoc Networks, *in IEEE Access*, 8, 124097-124109.

[2] Alnumay W., Ghosh U. & Chatterjee P. (2019). A Trust-Based Predictive Model for Mobile Ad Hoc Network in Internet of Things, *Sensors 2019*, 19, 1467.

[3] Chatterjee P., Sengupta I. & Ghosh S. (2010), A Distributed Trust Model for Securing Mobile Ad Hoc Networks, *In Proceedings of the IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, Hong Kong, China, 11–13 December 2010, 818–825.

[4]. Elhoseny M. & Shankar K.. (2020). Reliable Data Transmission Model for Mobile Ad Hoc Network Using Signcryption Technique. *IEEE Transactions on Reliability*, 69(3), 1077-1086.

[5] Mershad K., Hamie A & Hamze M..(2017). HiMAC: Hierarchical Message Authentication Code for Secure Data Dissemination in Mobile Ad Hoc Networks, *Int. J. Communications, Network and System Sciences*, 10, 299-326.

[6] Zapata M. G.(2002). Secure Ad Hoc On-Demand Distance Vector Routing. *ACM SIGMOBILE Mobile Computing and Communications Review*, 6, 106-107.

[7] EL-SEMARY A. M. , DIAB H (2019). BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map, *IEEE Access*, 7, 95197- 95211.

[8] Chlamtac I. , Conti I., M.,& Liu J.J. N. (2003). Mobile Ad Hoc Networking: Imperatives and Challenges, *Ad Hoc Networks*, 1, 13-64.

[9] Cizmar A., Papaj J, &Dobo L.(2012). Security And QoS Integration Model For MANETS, *Computing and Informatics*, 31, 1025–1044.

[10] Zafar W. & Khan B. M.(2016). Flying ad-hoc networks: Technological and social implications, *IEEE Technol. Soc. Mag*., 35, 2, 67-74,

[11] Neeraja Y & Sumalatha V.(2015). An advanced wireless medium access backoff algorithm for MANETs. *In: 2015 science and information conference (SAI),* 1033– 1036.

[12] Ali Zardari Z, He J, & Zhu N,(2019). et al. A dual attack detection technique to identify black and gray hole attacks using an intrusion detection system and a connected dominating set in MANETs. *Futur Internet; 11(3): 61, https://www.mdpi.com/1999-5903/11/3/61*

[13] Gupta P, Goel P, & Varshney P,(2019) et al. Reliability factor based AODV protocol: prevention of black hole attack in MANET. *Singapore: Springer,* 271–279.

[14] Soni M & Joshi BK.(2019). Security assessment of SAODV protocols in mobile ad hoc networks. *Singapore: Springer*, 347–355.

[15] Dasari M. (2017). Real time detection of MAC layer DoS attacks in IEEE 802.11 wireless networks. *In: 2017 14th IEEE annual consumer communications & networking conference (CCNC*), 939–944.

[16] Guang L.(2019) Vulnerability assessment of ad hoc networks to MAC layer misbehavior (Mobile CA-WC and, 2007 undefined). *Wiley, https://onlinelibrary.wiley.com/doi/full/10.1002/wcm.391 (accessed 23 February 2019).*

[17] Guang L. (2005). Vulnerabilities of ad hoc network routing protocols to MAC misbehavior. *In: IEEE international conference on wireless and mobile computing, networking and communications (WiMob'2005),.*

[18] Guang L.(2006). A self-adaptive detection system for MAC mis-behavior in ad hoc networks (*On CA-2006 IIC, 2006 undefined*).

[19] Zhou Y & Nettles SM.(2004). Analyzing and preventing MAC-layer denial of service attacks for stock 802.11 systems.

[20] Gupta D, Kaur H & Kumar R.(2016). Detection of sink hole attack in wireless sensor network using advanced secure AODV routing protocol. *Int J Comput Appl* 156.

[21] Alheeti KMA, Al-ani MS and McDonald-Maier K.(2018). A hierarchical detection method in external communication for self-driving vehicles based on TDMA. *PLoS ONE 2018; 13(1): e0188760.*

[22] Murugan R & Shanmugam A.(2010). A combined solution for routing and medium access control layer attacks in mobile ad hoc networks. *J Comput Sci 2010; 6(12):1416–1423, http://www.thescipub.com/abstract/10.3844/ jcssp.2010.1416.1423*

[23] Taya M & Gupta P. A black hole detection algorithm in MANETS using MAC scheme, *www.ijraset.com*.

[24] Alomari A.(2013). Security authentication of AODV protocols in MANETs. *In: International conference on network and system security, Madrid, 3–4 June 2013, 621–627. New York: Springer.*

[25] Singh D & Singh A. (2015).Enhanced secure trusted AODV (ESTA) protocol to mitigate blackhole attack in mobile ad hoc networks. *Futur Internet ; 7(3): 342–362.*

[26] Khamayseh Y, Yassein MB & Abu-Jazoh M. (2019). Intelligent black hole detection in mobile AdHoc networks. *Int J Electr Comput Eng 2; 9(3).*

[27] Aggarwal R.(2018). A survey to improve the network security with less mobility and key management in MANET. *Int J Sci Res Comput Sci Eng Inf Technol; 3(10): 1265–1271.*

[28] Alocious C., Xiao H. & Christianson B.(2015). Analysis of DoS attacks at MAC Layer in mobile adhoc networks, *2015 International Wireless Communications and Mobile Computing Conference (IWCMC), Dubrovnik, 811-816.*
[29] Narayanan S. S. & Radhakrishnan S.(2013). Secure AODV to combat black hole attack in MANET, *2013 International Conference on Recent Trends in Information Technology (ICRTIT), Chennai, 447-452.*
[30] Toledo AL & Wang X.(2008). Robust detection of MAC layer denial-of-service attacks in CSMA/CA wireless networks. *IEEE Trans Inf Forensics Secur; 3(3): 347–358.*
[31] Djahel S, Nait-Abdesselam F & Ahsan F.(2009). Highlighting the effects of joint MAC layer misbehavior and virtual link attack in wireless ad hoc networks. *In: 2009 IEEE/ ACS international conference on computer systems and applications, Rabat, Morocco, 756–763.*
[32] Soni M & Joshi BK.(2019). Security assessment of SAODV protocols in mobile ad hoc networks. *Singapore: Springer,347–355, http://link.springer.com/10.1007/978-981-10-7641-1_30.*
[33] Dilli R & Reddy PCS.(2019). Robust secure routing protocol for mobile ad hoc networks (MANETs). *In: HS Saini, RK Singh, G Kumar, et al. (eds) Innovations in electronics and communication engineering. New York: Springer, 393–399.*
[34] Mishra B, Mohindru V & Singh Y.(2014). Comparative analysis of energy efficient secure MAC protocols for wireless sensor network. *J Basic Appl Eng Res; 1: 13–18.*
[35] Ning Cai R. W. Y.(2002). Network coding and error correction. *In Information Theory Workshop, 119–122. IEEE Computer Society*.
[36 Ning Cai] R. W. Y.. (2006) .Network Error Correction, *II: Lower Bounds. Commun. pages 37–54. Communications Infomation and Systems*.
[37] Boneh D., Freeman D. M., Katz J., & Waters B.(2009). Signing a linear subspace: Signature schemes for network coding. In *Public Key Cryptography, 68–87.*
[38] Charles, D., Jain, K., & Lautner ,K.(2006). Signatures for network coding. *In 40th Annual Conference on Information Sciences and Systems (CISS 06),*
[39] Gennaro, Katz, R. J. , Krawczyk ,H., & Rabin, T. (2010). Secure network coding over the integers. *In Public Key Cryptography, pages 142–160.*
[40] Johnson, R., Molnar ,D., Song ,D. X., & Wagner, D. (2002). Homomorphic signature schemes. *In CT-RSA '02: Proceedings of the The Cryptographer's Track at the RSA Conference on Topics in Cryptology, 244–262, London, UK,Springer-Verlag*.
[41] Krohn, M. N., Freedman, M. J., & Mazieres, D. (2004). On-the-fly verification of rateless erasure codes for efficient content distribution. *In Proceedings of the IEEE Symposium on Security and Privacy, 226–240.*.
[42] Zhao,F., Kalker, T., Medard, M., & Han, K. J. (2007). Signatures for content distribution with network coding. *In Proc. of International Symposium on Information Theory (ISIT).*
[43] Agrawal ,S. & Boneh,D. (2009). Homomorphic macs: Mac-based integrity for network coding. *In ACNS, pages 292–305*.
[44] Park,J.-S., Gerla,M., Lun,D.S.,& Yi,M.M.Y.(2006). Codecast: A network-coding-based ad hoc multicast protocol. *IEEE WIRELESS COMMUNICATIONS, 13(5):76–81*.
[45] Lee, U., Park, J.-S., Yeh ,J., Pau, G., & Gerla ,M.(2006). CodeTorrent: Content Distribution using Network Coding in VANETs. *In MobiShare'06, Los Angeles, CA, Sep.*.
[46] Dong, J., Curtmola, R., & Nita-Rotaru, C.(2009). Practical defenses against pollution attacks in intra-flow network coding for wireless mesh networks. *In: Proc. ACM WiSec , ACM Press.*
[47] Katti, S., Katabi D., . Hu ,W., Rahul ,H., & Medard, M.(2005). The importance of being opportunistic: practical network coding for wireless environments. *In 43rd Allerton Conf. Communication, Control and Computing*.
[48] Katti, S., Rahul, H., Katabi,D., Medard ,M., & Crowcroft, J. (2006) .XORs in the air: practical network coding. *In ACM SIGCOMM*.
[49] Lun ,D., Medard ,M., & Koetter,R.(2005). Efficient operation of wireless packet networks using network coding. *In IWCT.*
[50] Cai, N. & Yeung ,R.(2002). Network coding and error correction. *In: Proc. 2002 IEEE Information Theory Workshop 119–122.*
[51] Yeung, R. & Cai, N.(2006). Network Error Correction, I: Basic Concepts and Upper Bounds. *Commun. Inf. Syst. 6(1):19–35*.
[52] Cai, N. & Yeung, R. (2006) .Network Error Correction, *II: Lower Bounds. Commun. Inf. Syst. 6(1):37–54*.
[53] Cai ,N. & Yeung,R.(2002). Secure network coding. *In: Proc. International Symposium on Information Theory (ISIT '02), June*.
[54] Bhattad ,K. & Narayanan, K.R.(2005). Weakly Secure Network Coding. *In NETCOD 2005, Italy, April*.
[55] Ho,T., Leong,B., Koetter,R.,& Medard ,M. (2004). Byzantine Modification Detection in Multicast Networks using Randomized Network Coding. *In IEEE Proc. ISIT* .
[56] Jaggi,S., Langberg,M., Katti,S., Ho,T., Katabi,D.,& Medard,M. (2007). Resilient network coding in the presence of Byzantine adversaries. *In Proc. INFOCOM, pages 616–624.*
[57] Jaggi,S., Chou ,P. P. A., Effros, M., Egner,S., Jain,K. & Tolhuizen, L. (2003). Polynomial time algorithms for multicast network code construction. *IEEE Transaction on Information Theory.*
[58] Yeung, R. & Cai, N.(2006). Network Error Correction, I: Basic Concepts and Upper Bounds. *Commun. Inf. Syst. 6(1):19–35*.
[59] . Wang, Y. & Desmedt ,Y.(2001). Secure communication in multicast channels: the answer to Franklin and Wrights question. *J. of Cryptology, 14(2):121–135.*.
[60] Wang ,Y. & Desmedt ,Y.(2008). Perfectly Secure Message Transmission Revisited. *IEEE Tran. on Information Theory 54:(6):2582–2595*.
[61] Gkantsidis ,G. & Rodriguez, P.(2006). Cooperative security for network coding file distribution. *In IEEE INFOCOM* .
[62] Krohn ,M., Freedman ,M., & Mazieres, D. (2004) .On-the-Fly Verification of Rateless Erasure Codes for Efficient Content Distribution. *In IEEE Security and Privacy* .

[63] Wu,X., Xu,Y., Yuen,C., & Xiang, L.(2014).A tag encoding scheme against pollution attack to linear network coding, *IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, 33–42.*
[64] Yu,Z., Wei ,T., Ramkumar,B., & Guan ,Y.(2008). An Efficient Signature based Scheme for Securing Network Coding against Pollution Attacks. *In IEEE INFOCOM*.
[65] Zhao, F., Kalker ,T., Medard ,M., Han ,K. (2007). Signatures for Content Distribution with Network Coding. *In Proc. 2007 IEEE ISIT.*
[66] Oggier,F. & Fathi, H. (2009). An Authentication Code against Pollution Attacks in Network Coding. *CoRR abs/0909.3146.*.
[67] Zhao, F., Kalker ,T., Edard ,M.M´, & Han, K. J.(2007). Signatures for content distribution with network coding, *in Proceedings of the IEEE International Symposiumon InformationTheory (ISIT '07), 556–560, Nice, France, June* .
[68] Agrawal,S., Boneh,D., Boyen,X., & Freeman, D. M.(2010). Preventing pollution attacks in multi-source network coding, *in Public Key Cryptography—PKC 2010, vol. 6056 of Lecture Notes in Computer Science, pp. 161–176, Springer, Berlin, Germany.*
[69] Li ,Y., Yao, H., Chen, M., Jaggi ,S., & Rosen, A.(2010). RIPPLE authentication for network coding, *in Proceedings of the IEEE INFOCOM, 1–9, San Diego, Calif, USA, March* .
[70 Krawczyk,H. & Canetti, R. (2002) The TESLAbroadcast authentication protocol, *Rsa Cryptobytes, vol. 20, no. 2.*
[71] Ganesan, P., Venugopalan ,R., Peddabachagari, P., Dean ,A., Mueller, F., & Sichitiu, M. (2003). Analyzing and modelling encryption overhead for sensor network nodes*. In WSNA '03: Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications, pages 151–159, New York, NY, USA, ACM.*
[72] Mohammadani, K. H., Memon ,K. A., Memon, I., Hussaini, N. N.,& Fazal, H.(2020). Preamble time-division multiple access fixed slot assignment protocol for secure mobile ad hoc networks, *International Journal of Distributed Sensor Network, Vol. 16(5), 1-18.*
[73] Usama, M., Malluhi, Q. M., Zakaria ,N., Razzak, I. ,& Iqbal, W.(2020). An efficient secure data compression technique based on chaos and adaptive Huffman coding, Peer-to-Peer Networking and Applications, *Springer.*
[74] Pradeep, G. V. (2012) A Unique Huffman Coding Based Multipath Data Security Standard using Data Compression Technique for Multi hop Network, *IJECT Vol. 3, Issue 2, April - June* .