Multipath Collision Avoidance Using Hybrid Co-Ordination Function for Efficient Routing and Data Security in MANET

Renuka Mohanraj
Department of Computer Science, Maharishi University of Management, Fairfield, Iowa, USA-52556.
mr.renuka@gmail.com
Dr. Sangeetha Krishnan
Associate Dean, Faculty of Technology, Academic City College, Accra, Ghana
kavigeethrethin@gmail.com

ABSTRACT

Mobile Ad-hoc NETwork (MANET) is an infrastructure-less multi-hop network with self-organizing and self-operating nodes for data packets routing within the transmission range through multi-hop route. During the data packets routing in MANET, when two or more nodes send the data packets to the same node collisions occurs which lacks the data security. In order to avoid the data packets collision and increase the data security level, Hybrid Coordination Function based Poly Data Flag Encryption (HCF-PDFE) Technique is proposed in MANET. Initially in HCF-PDFE technique, Hybrid Coordination Function scheme is introduced with combination of Distributed Coordination Function (DCF) scheme and Point Coordination Function (PCF) scheme for collision avoidance. In HCF scheme, DCF and PCF schemes are used to avoid the collision for cyclic and acylic node links respectively. During collision avoidance in DCF scheme, it checks whether the transmission channel is idle or not using Binary Exponential Backoff (BEB) algorithm. For acyclic node links, polling based access method is used in PCF scheme where the access point (AP) polls all the nodes to send out the data packets after receiving beacon message. This in turn helps to improve collision avoidance rate and throughput. Once the collision gets avoided, the data security level gets improved during the routing process in MANET using Poly Data Flag Encryption and Decryption Model. In this model, the data packets from multiple paths are encrypted with the flag value. Then, the poly data flag encryption process collects all the encrypted data packets and sent to the destination node. In the destination node, the poly data flag decryption process decrypts the data packets and flag value separately for each path which resulting in higher security level. An experimental result shows that the proposed HCF-PDFE technique improves the routing performance in terms of routing overhead, throughput, security level based on dropping ratio and collision avoidance rate when compared to the state-of-the-art works.

Keywords: Mobile Ad-hoc NETwork (MANET), Binary Exponential Backoff, Distributed Coordination Function, Point Coordination Function, Poly Data Flag Encryption, Poly Data Flag Decryption

1. INTRODUCTION

In MANET, multipath routing uses essential physical network resources through multiple source-destination paths. TOpology HIding Multipath routing Protocol (TOHIP) [1] is loop-free protocol and not represents the network topology. TOHIP failed to transmit the routing information. It helps in reducing the malicious nodes activities in network topology with increasing the packet delivery rate. But, the problem occurs while identifying the correct path and guaranteeing the security in MANET. An optimal path breaks when link availability reduces. As routing is nondeterministic polynomial (NP) hard, improved ad hoc on-demand multipath distance vector

(AOMDV) was designed in [2] with link availability, queuing delay, mobility, and bit error rate. Though the energy consumption in multipath routing was less, the collision avoidance was not addressed.

An altruistic backoff (AB) is a new collision avoidance mechanism designed in [3] for eliminating the collisions after beacon transmission. Due to an early backoff, senders consumed less time in idle waiting for beacon message. But, the data security was remained unaddressed. An anonymous multipath routing protocol is introduced in [4] depending on secret sharing. The protocol presents the identity anonymity depending on the cryptograph technology and secret sharing of data in MANET. However, it failed to reduce the successful probability of active attacks during routing process.

A high secure and efficient routing scheme in [5] used the properties of anonymity, security, verification, nonrepudiation and unforgeability. In addition, confidentiality and flexibility for multipaths in MANET makes the ad hoc environment as secured one. But, the collision avoidance was not at required level during multipath transmission. An efficient collision avoidance and path following technique was designed in [6] for intelligent and efficient autonomous mobile robot system. A new technique was introduced for collision avoidance in mobile robotic systems. But, the data security was not enhanced while transmitting the information.

Trust model from ad-hoc on-demand multi-path distance vector routing (AOMDV) protocol [7] was designed called ad hoc on-demand trusted multi-path distance vector routing (AOTMDV) protocol. The new protocol presents flexible and feasible approach for selection of shortest path with security needs of data packets transmission. But, the collision avoidance remained unaddressed. An energy-aware multipath routing scheme with particle swarm optimization (EMPSO) [8] employed continuous time recurrent neural network (CTRNN) for addressing the optimization issues. CTRNN identifies the optimal loop-free paths to address the link disjoint paths in MANET. However, the dropping ratio was high during the data packet transmission.

A collision-free data aggregation based on TDMA was introduced in [9] for fault-tolerant network in wireless sensor networks (WSNs) to increase the latency. However, the security level during the data aggregation remained unaddressed. Position based Opportunistic Routing (POR) [10] solved the reliability issues and data timeliness at receiving end by Virtual Destination-based Void Handling (VDVH). However, the data security level based on dropping ratio remained unaddressed. Trust-based Multipath Routing (TMR) [11] increased the security level using multiple secure route discoveries improving the average latency. But, the throughput remained unsolved.

The contribution of research work is classified as follows. Hybrid Coordination Function based Poly Data Flag Encryption (HCF-PDFE) technique is introduced to increase the collision avoidance rate and security level based on dropping ratio during the data packet transmission in MANET. In HCF-PDFE Technique, the HCF scheme is used to avoid the collision occurrence in both cyclic and acyclic node links using DCF scheme and PCF scheme respectively. This in turns helps to improve the throughput and collision avoidance rate. After the collision avoidance, Poly Data Flag Encryption and Decryption model, the data packets are sent to the destination in secured manner. After encrypting the data packets with the flag value, it is sent to the destination. In destination node, Poly Data Flag Decryption process is carried out. This in turn helps to increase the security level based on dropping ratio.

The rest of the paper is organized as follows. Section 2 explains about certain review of related work in a brief manner. Section 3 presents the proposed Hybrid Coordination Function based Poly Data Flag Encryption (HCF-PDFE) technique with a neat diagram and algorithmic description. Section 4

provides with the experimental evaluation followed by Section 5 which includes the discussions involved in the design of HCF-PDFE technique with the help of table and graphical form. Finally, conclusion is included in Section 6.

2. RELATED WORKS

An energy Entropy Multipath Routing optimization algorithm with Genetic Algorithm (EMRGA) in MANET is designed in [12]. The main objective of the protocol is to identify the minimal node residual energy of every route in path selection process by reducing the node residual energy. But, the collision avoidance is not carried out during the routing process. An unobservable secure routing scheme (USOR) [13] presents complete unlinkability and content unobservability for all packets. USOR uses mixture of group signature and ID-based encryption for route discovery. However, unobservable secure routing scheme failed to improve the data security level. A multipath routing scheme using simulated annealing approach is designed in [16]. The designed metaheuristic approach attained reciprocal benefits in hostile dynamic real world network situation. But, the security level of multipath routing scheme was not enhanced.

An efficient and stable multipath routing in MANET was designed in [14] with congestion awareness. In designed approach, the network calculates the residual energy and stability of links in network. However, the routing overhead issues are not addressed. Maximally Spatial Disjoint Multipath routing protocol (MSDM) was designed in [15] for AOMDV protocol. MSDM identified the paths that were spatially separated. Many packets were sent in the disjointed paths to minimize the probability of collision existence and allocate concurrent transmission over many selected paths. However in MSDM, collisions were only reduced not avoided. An improved multipath routing protocol termed Receiver-based ad hoc on demand multipath routing protocol (RB-AOMDV) [17] was introduced with higher reliability of AOMDV protocol and minimum re-established discovery time. But, the packet drop during the multipath routing protocol was high.

A new technique was designed in [18] for improving the data security level by trust-based multi-path routing. The trust-based multi-path routing guaranteed the secure discovery of multiple paths from source to destination. A secure routing protocol was introduced in [19] by combining multipath routing and secret sharing. It selected the secure multiple disjoint routes through combining many metrics to preserve the data security and increases the efficiency in whole transmission process. But, the routing overhead was high in secure routing protocol. IEEE 802.11e Medium Access Control (MAC) introduced the Enhanced Distributed Channel Access (EDCA) mechanism in [20] for better QoS in multimedia applications.

Based on the above mentioned methods and techniques, an efficient Hybrid Coordination Function based Poly Data Flag Encryption (HCF-PDFE) technique is developed to increase the collision avoidance rate and security level during the data packet transmission in MANET.

3. MULTIPATH COLLISION AVOIDANCE USING HYBRID CO-ORDINATION FUNCTION FOR EFFICIENT ROUTING AND DATA SECURITY

With availability of efficient routing, collision avoidance and data security are the major topics analyzed in MANET. Let us consider 'n' mobile nodes distributed randomly in '$m * m$' square area as simple graph '$G = (V, E)$' within the transmission range 'R'. MANET consists of 'n' number of mobile nodes represented as '$V = \{v_1, v_2, \dots, v_n\}$' and '$E = \{e_1, e_2, \dots, e_n\}$' represents links between mobile nodes. The data packets $(D1, D2, D3, \dots, Dn)$ are sent to the destination node in multiple paths $(P1, P2, P3, \dots, Pn)$. The multipath collision avoidance and data security issues for MANET is addressed by implementing Hybrid Coordination

Function (HCF) scheme and Poly Data Flag based Encryption and Decryption model in HCF-PDFE technique. The key aim of HCF-PDFE technique is to increase the collision avoidance rate and increase the data security level while routing the data in MANET. The overall architectural diagram of HCF-PDFE technique is depicted in Figure 1.

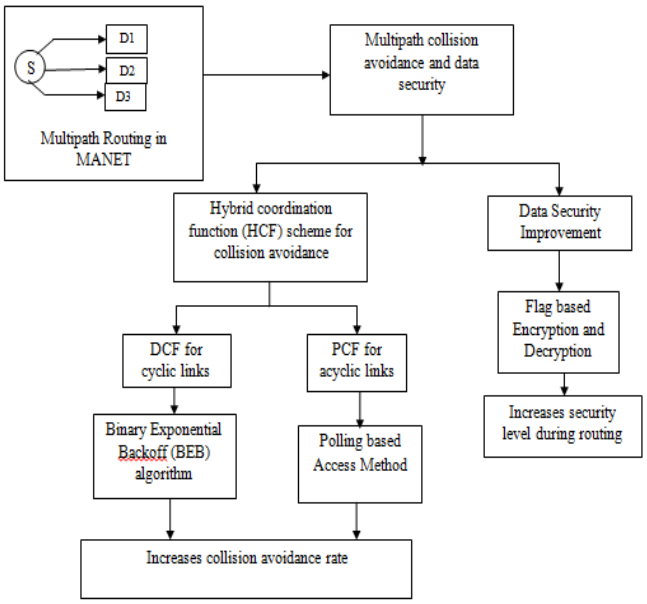

Figure 1. Architecture Diagram of Hybrid Coordination Function based Poly Data Flag Encryption Technique

Figure 1 shows the architecture diagram of HCF-PDFE technique. During the multipath data transmission in MANET, the collision occurs. In order to increase the collision avoidance rate and improve the data security level, Hybrid Coordination Function based Poly Data Flag Encryption Technique is proposed. The elaborate description of Hybrid Coordination Function based Poly Data Flag Encryption technique is explained in the following sections.

3.1 Hybrid Coordination Function for Collision Avoidance in HCF-PDFE Technique

HCF is mainly used in HCF-PDFE Technique for collision-free MANET environment. Collision Avoidance mechanism is mainly used for minimizing the hidden mobile nodes. Hybrid coordination function (HCF) scheme in HCF-PDFE Technique are the combination of standard DCF in cyclic networks and PCF schemes in acyclic networks for collision avoidance. The process of DCF and PCF is chosen based on the number of nodes taken for data packet transmission. When the data packets transmitted between two nodes, DCF scheme is chosen for collision avoidance in cyclic node links. When the data packets transmitted between more than two nodes, PCF scheme is selected for collision avoidance in acyclic node links. The detailed explanation about DCF and PCF Scheme is described in following sub sections.

3.1.1 Distributed Coordination Function (DCF) for Collision Avoidance during cyclic Links

DCF is a protocol used for data packet transmission between two nodes. DCF is a mandatory protocol where nodes sends the data packet together and change the access to wireless medium. DCF use Carrier Sensing Multiple Access (CSMA) with Binary Exponential Backoff (BEB) algorithm for avoiding the collision during the data packet transmission. When more number of packets is sent at the same time to the same node, the collision occurs. Collision Avoidance mechanism uses the Request to Send (RTS) and Clear to Send (CTS) to create the connection between two nodes (i.e., source and destination) for data packet transmission as shown in Figure 2.

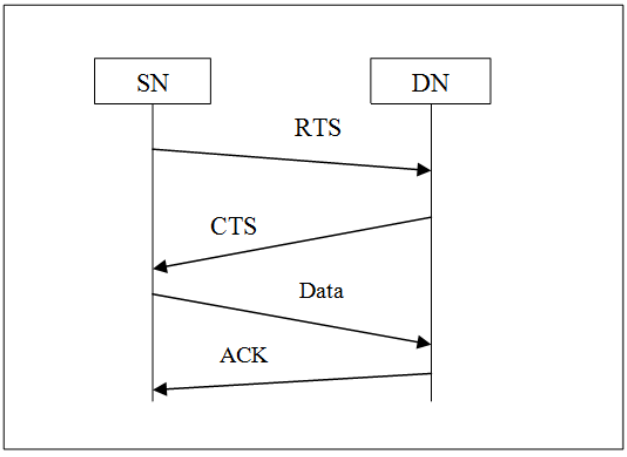

Figure 2. RTS and CTS message flow diagram

DCF has possible virtual carrier sense mechanism which swaps the Request-to-send (RTS) and Clear-to-send (CTS) data between source and destination node in data packet transmissions process. DCF comprises the positive acknowledge scheme for sending successful data packet delivery message to the destination node. DCF functions on two modes of operations in HCF-PDFE Technique, namely BASIC access mode and COLAV access mode. In BASIC access mode, there is no preceding handshake before sending the data packets to the destination node. In COLAV Access Mode, handshaking between source and destination takes place before data packet transmission by RTS/CTS mechanism. RTS/CTS mechanism in HCF-PDFE Technique minimizes the collision and hidden mobile node issues.

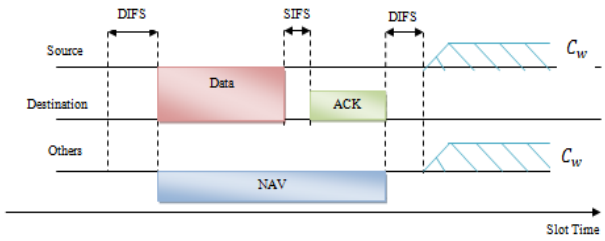

Figure 3 DCF Operations in BASIC Mod

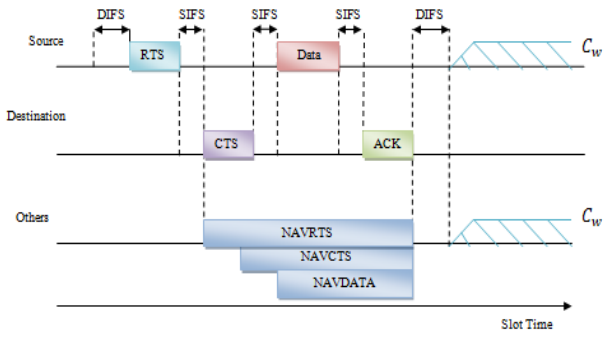

Figure 4 DCF Operations in COLAC Mode

Figures 3 and 4 represent the operations of DCF in BASIC and COLAV mode in HCF-PDFE Technique. Before sending the data packets to the destination node, it is to be checked whether the transmission channel is busy or idle. Any node with data packets for transmission performs Clear Channel Assessment (CCA) where it listens to transmission channel for DCF Inter Frame Space (DIFS). When the transmission channel is sensed idle for DIFS period, the node seizes the transmission channel and starts the data transmission in HCF-PDFE Technique. When the transmission channel is sensed busy, node executes the BEB algorithm. In any node when collision occurs during failure detection, back-off time is set as a random value in range of [0, C_w].

$$Backoff\ time = random\,(0, C_w] * \text{slot time} \qquad (1)$$

From (1), backoff time is calculated by selecting the random value ranges from 0 to C_w . C_w is denoted as contention window. As long as transmission channel is sensed idle, back-off time is reduced with one second. In timer expiration, the node sends the data again. After the reception of data, the destination node sends an ACK message after Short Inter Frame Space (SIFS). SIFS is essential to balance the propagation delays and radio transceivers to switch from receiving to transmitting mode. SIFS is lesser than DIFS and acknowledgements are provided first priority over data traffic. The nodes increases the Network Allocation Vector (NAV) based on the time channel to be occupied. This mechanism is mainly aimed to reduce the hidden terminal problem in cyclic node links. The algorithmic process of Binary Exponential Backoff (BEB) algorithm is shown in below,

Algorithm 1 : Binary Exponential Backoff (BEB) Algorithm

Input: Data Packets ($D1, D2, D3, ..., Dn$), Flag ($F1, F2, F3, ... Fn$), Multipath ($P1, P2, P3, ..., Pn$)

Output: Improved Collision avoidance rate and Throughput

Step 1 :Begin

Step 2 : For each packet transmission

Step 3 : Checks the transmission channel state before data transmission

Step 4 : **If** (channel state is idle) then

Step 5 : Sends data packets to the destination without collision

Step 6 : **Else**

Step 7 : Calculates backofftime using (1) and waits for time expiration and goto step 3

Step 8 : **End if**

Step 9 : Sends acknowledge message to source node after receiving the data packets

Step 10:End for

Step 11:End

Algorithm 1 explains Binary Exponential Backoff (BEB) Algorithm for increasing the

collision avoidance rate in DCF scheme. But, DCF failed to solve the hidden mobile node issues in acylic node links. For collision avoidance in acylic node links, PCF is discussed in next sub section.

3.1.2 Point Coordination Function (PCF) for Collision Avoidance during Cyclic Links

Point Coordination Function (PCF) scheme in HCF-PDFE Technique is an optional coordination function of IEEE 802.11 Standard. PCF is a protocol designed for infrastructure based networks in acyclic node links. PCF is polling based access method where the access point (AP) polls all nodes to send out the data packets. PCF method presents better results under heavy data traffic and addresses the hidden mobile node issues in acyclic node links. PCF is located directly above DCF. PCF access mode functions on infrastructure based networks where an AP successively polls nodes to send out the data packets and collisions are totally avoided HCF-PDFE Technique.

Channel access in PCF access mode is integrated and point coordinator transmits the CF-Poll data packets to PCF for data frame transmission in HCF-PDFE Technique. When the polled node does not have any data packets to send, then it sends the null data to the destination node in HCF-PDFE Technique. In PCF, slot time is classified into two types, namely Contention Free Periods (CFP) and Contention Periods (CP) as described in figure 5. In CFP, AP sends poll messages to provide transmission possibility to the mobile nodes. In Contention Periods (CP), DCF is performed in cyclic process. A CFP is initiated and maintained by AP through transmitting the beacon (B) to the destination node in HCF-PDFE Technique. The first beacon after CP (DCF access) is sent after PCF Inter Frame Space (PIFS) in HCF-PDFE Technique. The time period of PIFS is lesser than DIFS but higher than SIFS ($DIFS > PIFS > SIFS$).

$$PIFS = SIFS + Slot\ time \quad (2)$$

From (2), PIFS is calculated by adding SIFS with slot time. PIFS presents at the beginning of CFP with less priority than control packets transmission and higher priority than data packets transmission. The transmitted beacons include information based on the time period of CFP and CP. The transmitted beacons allow new arrived node to link with AP in CFP process. The CFP is terminated when AP sends CF End (CE) control packet.

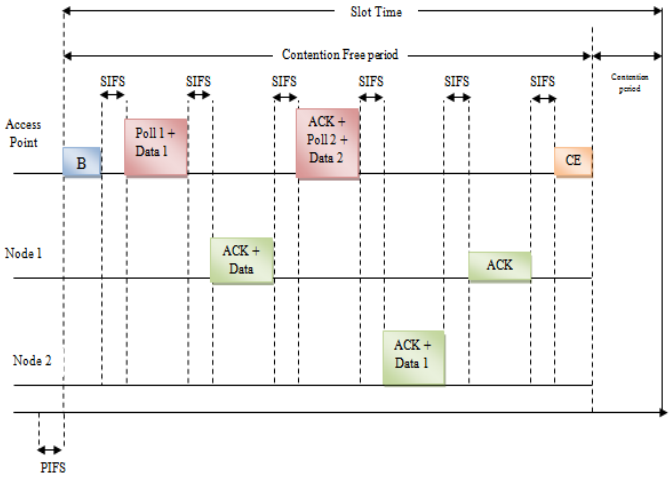

Figure 5 Operation of PCF with CFP & CP

When mobile ad-hoc networks suffer from hidden mobile node issues, it failed to observe other nodes on extreme edge of geographical radius of mobile ad-hoc network. By locating the AP in middle reduces the distance and all mobile nodes view the AP. In addition it also reduces the distance between two nodes on extreme edges of cyclic mobile node links. By this way the collision avoidance is carried out in HCF-PDFE Technique.

3.2 Improved Data Security using Poly Data Flag based Encryption and Decryption Model

Once collision avoidance is carried out using Hybrid coordination function (HCF) scheme in MANET, the data security has to be improved. In HCF-PDFE technique, the data security level of MANET is increased using Poly Data Flag based Encryption and Decryption model. The source node sends the data packets to the destination in multiple paths after encryption process. In encryption process, data gets encrypted using the flag value. In Poly Data Flag based Encryption process, the encrypted data from all the paths are collected and

sent to the destination. In the destination node, the collected data packets from multiple paths get decrypted using Poly Data Flag based Decryption process. The data packets and flag value are obtained separately after the Poly Data Flag based Decryption in HCF-PDFE technique. The HCF-PDFE technique for improved data secured routing is shown in below Figure 6.

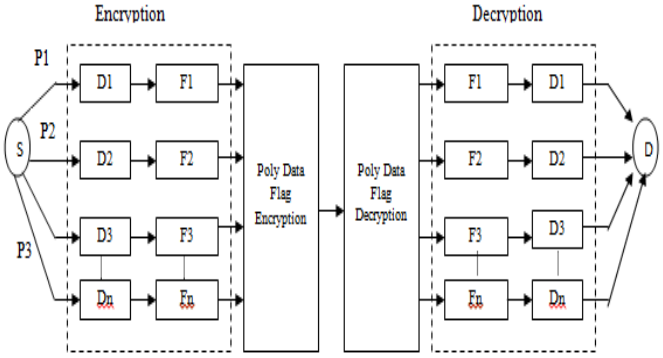

Figure 6 Poly Data Flag based Encryption and Decryption Model

In MANET, the data is to be sent in secured manner using Poly Data Flag based Encryption and Decryption Technique. From the source, many data packets $(D1, D2, D3, \dots, Dn)$ are sent to the destination in multipath $(P1, P2, P3, \dots, Pn)$. Before sending the data packets in multiple paths to the destination, the data has to be encrypted with the flag value $(F1, F2, F3, \dots Fn)$ using Poly Data Flag Encryption process. For every data packets, the flag value is different. The encrypted data of HCF-PDFE technique as formulated as,

$$E(D1_{p1}) = D1 \oplus F1 \quad (3)$$

From (3), $E(D1_{p1})$ represents the encrypted data packets in path$P1$. In similar way, the data packets are encrypted for all paths are termed as Poly Data Flag Encryption (DFE).

$$Poly\,(DFE) = [E(D1_{P1}), E(D2_{P2}), E(D3_{P3}), \dots \dots E(Dn_{Pn})] \quad (4)$$

From (4), $Poly(DFE)$ is the collection of all encrypted data from all paths in MANET. After the encryption process, the data are sent to the destination in secure manner. In the destination node, the encrypted data gets decrypted using Poly Data Flag Decryption process. The Poly Data Flag Decryption (DFD) process of HCF-PDFE technique using the flag value is mathematically formulated as,

$$Poly\ (DFD) = [D(D1_{P1}), D(D2_{P2}), D(D3_{P3}), \dots \dots D(Dn_{Pn})] \quad (5)$$

From (5), $Poly(DFD)$ is the combination of all decrypted data from all paths in MANET. After that, the data sent in particular path is identified separately in secured manner. The decrypted data of HCF-PDFE technique in single path is identified as formulated as,

$$D(D1_{p1}) = F1 \oplus D1 \quad (6)$$

From (6), the data and flag value is obtained separately at the destination node using Poly Data Flag based Encryption and Decryption technique in MANET. The algorithmic process of Poly Data Flag based Encryption and Decryption Algorithm is shown in below,

Algorithm 2 : Poly Data Flag based Encryption and Decryption Algorithm

Input: Data $(D1, D2, D3, \dots, Dn)$, Flag $(F1, F2, F3, \dots Fn)$, Multipath $(P1, P2, P3, \dots, Pn)$

Output: Improved Data Security

Step 1:Begin

Step 2: Source node generates data and flag value

Step 3: Data to be transmitted is encrypted using (3)

Step 4: Encrypted data of all paths are collected using (4)

Step 5: Poly Data Flag based Decryption is carried out using (5) in destination node

Step 6: Individual data are decrypted using (6)

Step 7: Data and Flag of all multiple paths are obtained separately at the destination **node**

Step 8:End

Algorithm 2 explains Poly Data Flag based Encryption and Decryption Algorithm in order to increase the security level based on dropping ratio during the data packet transmission in MANET. In this algorithm, the data packets are sent to the destination in secured manner after the poly flag based encryption and decryption model. Therefore, the proposed HCF- PDFE

technique effectively performs the secured routing between source and destination node in multiple paths with minimum routing overhead and also improves the collision avoidance rate.

4. SIMULATION SETTINGS

The simulation performance of the proposed Hybrid Coordination Function based Poly Data Flag Encryption technique is implemented in NS-2 simulator. The nodes were placed within the size of 1200 m * 1200 m square area with velocity of 0 – 50 m/s. HCF-PDFE technique uses the Random Way Point (RWM) Mobility model. In random waypoint mobility model, a source node chooses the destination node in random manner. RWM uses many mobile nodes for positioning the movable nodes. For the experimental work, Dynamic Source Routing (DSR) protocol is used as routing protocol for HCF-PDFE technique that increases the collision avoidance rate and performs secured data routing between the source and destination in multiple path in MANET. The simulations parameters are listed in Table 1.

Table 1 Simulation Parameters

Parameter	Value
Simulator	NS-2.31
Number of nodes	50,100,150,200,250,300,350,400,450,500
Network area	1200m*1200m
Number of Packets	10,20,30,40,50,60,70,80,90,100
Simulation period	600s
Node speed	2 -25m/s
Node pause time	0 – 300 seconds
Routing protocol	Dynamic Source Routing (DSR)
Number of runs	10

5. SIMULATION RESULTS AND ANALYSIS

Hybrid Coordination Function based Poly Data Flag Encryption (HCF-PDFE) technique is evaluated with existing Topology-Hiding multipath routing Protocol (TOHIP) [1] and Ad-hoc On-demand Multipath Distance Vector (AOMDV) [2]. The experimental evaluation is carried out with the different parameters such as routing overhead, security level on data packet transfer, throughput, and collision avoidance rate. Performance is measured with tables and graph values.

5.1 Impact of Routing Overhead

Routing overhead using HCF-PDFE is a measure of time taken to perform routing without any collision from source to destination with respect to the number of mobile nodes. It is measured in terms of milliseconds. Routing overhead is formulated as follows.

$$RO = \sum_{i=1}^{n} MN_i * Time\ (MN_i) \quad (7)$$

From (7), the routing overhead 'RO' is measured using the mobile nodes 'MN_i' and the time taken for routing without any collision respectively. Lower the routing overhead, more efficient the method is said to be.

Table 2 Tabulation for Routing Overhead

Number of Mobile Nodes (Number)	Routing Overhead (ms)		
	HCF-PDFE Technique	TOHIP	AOMDV
50	25	32	42
100	29	37	46
150	31	39	48
200	33	41	50
250	36	43	52
300	38	46	55
350	41	49	59
400	44	52	62
450	47	55	65
500	50	58	70

Table 2 illustrates the routing overhead with respect to number of packets ranging from 10-100 during the multipath routing in MANET based on three different methods, namely Hybrid Coordination Function based Poly Data Flag Encryption (HCF-PDFE) technique, Topology-Hiding multipath routing Protocol (TOHIP) [1] and Ad-hoc On-demand Multipath Distance Vector

(AOMDV) [2]. The proposed HCF-PDFE technique has lesser routing overhead than the existing methods.

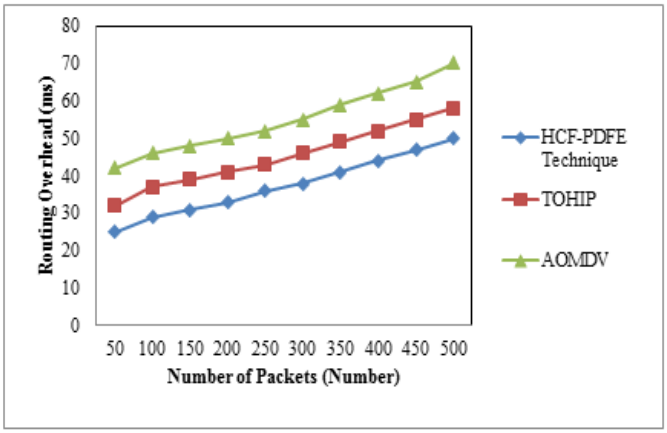

Figure 7 Measure of Routing Overhead

Figure 7 shows comparative analysis for routing overhead with respect to different number of nodes with existing TOHIP [1] and AOMDV [2]. Figure 7 proves that the proposed HCF-PDFE technique significantly improves the routing overhead performance than TOHIP [1] and AOMDV [2]. The packets in the range of 50 to 500 are taken for experimental purpose in HCF-PDFE technique. By using hybrid coordination function (HCF) scheme, the routing overhead gets reduced in HCF-PDFE technique. The HCF scheme is used for both acyclic links and cyclic links in MANET. The routing overhead is reduced by 17 % and 32% in HCF-PDFE technique compared to existing TOHIP [1] and AOMDV [2] respectively.

5.2 Impact of Throughput

Throughput determines the rate of successful packet delivery over period of time interval in MANET. Throughput rate is the ratio of packets received by the destination node to the packets sent by the source node. It is measured in terms of percentage (%) and is formulated as given below.

$$T = \frac{r_r}{n} * 100 \qquad (8)$$

From (8), the rate of throughput 'T' is measured using number of packets sent 'P_s' and number of packets received 'P_r'. Higher the throughput, more efficient the method is said to be.

Table 3 Tabulation for Throughput

Number of Packets (Number)	Throughput (%)		
	HCF-PDFE Technique	TOHIP	AOMDV
10	75	67	60
20	77	69	62
30	79	70	64
40	81	72	65
50	82	74	67
60	83	75	67
70	87	79	70
80	89	81	72
90	92	83	74
100	95	85	75

Table 3 illustrates the throughput with respect to number of packets ranging from 10-100 during the multipath routing in MANET based on three different methods, namely Hybrid Coordination Function based Poly Data Flag Encryption (HCF-PDFE) technique, Topology-Hiding multipath routing Protocol (TOHIP) [1] and Ad-hoc On-demand Multipath Distance Vector (AOMDV) [2]. The proposed HCF-PDFE technique has higher throughput than the existing methods.

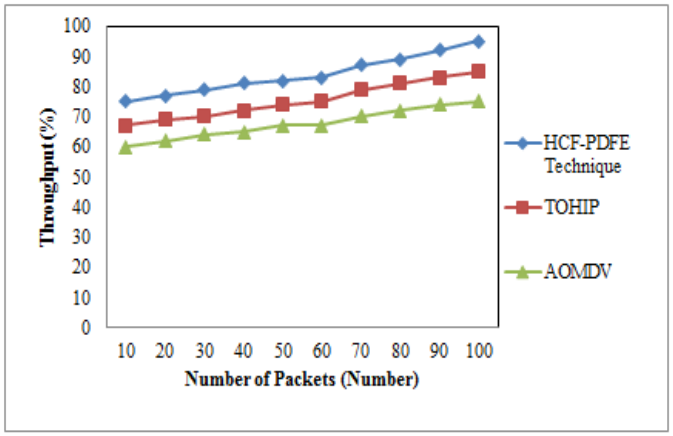

Figure 8 Measure of Throughput

Figure 8 describes comparative analysis for throughput with respect to different number of packets with existing TOHIP [1] and AOMDV [2]. The packets in the range of 10 to 100 are taken for experimental purpose in HCF-PDFE technique.

Figure 8 proves that the proposed HCF-PDFE technique significantly improves the throughput performance than TOHIP [1] and AOMDV [2]. The throughput level of HCF-PDFE technique is increased by using hybrid coordination function (HCF) scheme. By using this scheme, the data sent at the source node is received at destination node without any packet loss. In this scheme RTS and CTS are used for effective packet delivery at the receiving end during the multipath packet transmission in MANET. The throughput in HCF-PDFE is increased by 11 % and 24% technique compared to existing TOHIP [1] and AOMDV [2] respectively.

5.3 Impact of Security Level based on dropping ratio

The security level during the data packet transfer based on dropping ratio using HCF-PDFE technique is the ratio of difference between the packet sent in multipath and packet received to the actual packets sent. The dropping ratio is measured in terms of percentage (%) and formulated as,

$$DR = \frac{Packets_{send} - Packets_{recd}}{Packets_{send}} * 100 \quad (9)$$

From (9), the dropping ratio 'DR' is measured using packet sent and packet received while routing to the destination node from source node. Lower the dropping ratio, more efficient the method is said to be.

Table 4 Tabulation for Security Level based on dropping ratio

Number of Packets (Number)	Security Level based on dropping ratio		
	HCF-PDFE Technique	TOHIP	AOMDV
10	80	70	60
20	82	72	63
30	84	74	65
40	85	75	66
50	88	78	69
60	90	80	72
70	91	82	74
80	92	83	76
90	94	84	77
100	95	85	79

Table 4 illustrates the security level based on dropping ratio with respect to number of packets ranging from 10-100 during the multipath routing in MANET based on three different methods, namely Hybrid Coordination Function based Poly Data Flag Encryption (HCF-PDFE) technique, Topology-Hiding multipath routing Protocol (TOHIP) [1] and Ad-hoc On-demand Multipath Distance Vector (AOMDV) [2]. The proposed HCF-PDFE technique has higher security level based on dropping ratio than the existing methods.

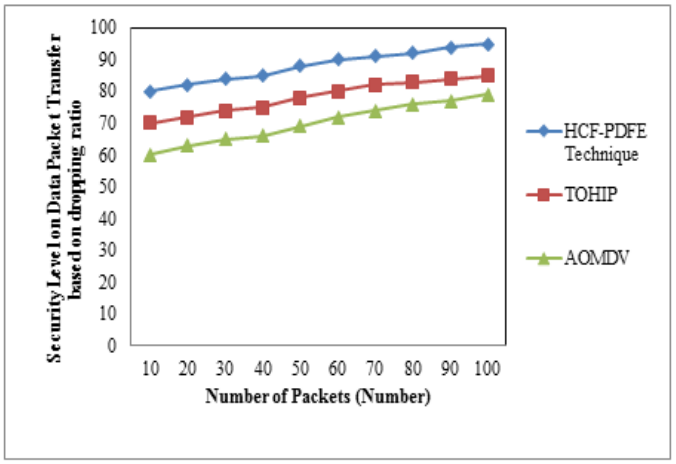

Figure 9 Measure of Security Level based on dropping ratio

Figure 9 describes comparative analysis for security level based on dropping ratio with respect to different number of packets with proposed HCF-PDFE technique and existing TOHIP [1] and AOMDV [2]. The packets in the range of 10 to 100 are taken for calculating the security level experimental purpose in HCF-PDFE technique. Figure 9 proves that the proposed HCF-PDFE technique significantly increases the security level with less dropping ratio than TOHIP [1] and AOMDV [2]. The security level of HCF-PDFE technique is increased after performing the encryption and decryption process during the multipath packet transmission in MANET. By using this model, the packet dropping ratio during the routing process gets minimized. The security level based on dropping ratio in HCF-PDFE is increased by 12 % and 26% technique compared to existing TOHIP [1] and AOMDV [2] respectively.

5.4 Impact of Collision Avoidance Rate

Collision avoidance rate is defined as the rate at which the collision gets avoided during routing the packets to the destination node from source. Collision avoidance rate minimizes the immediate trials to access the same node. It is measured in terms of percentage (%).

Table 5 Tabulation for Collision Avoidance Rate

Methods	Collision Avoidance Rate (%)
HCF-PDFE Technique	95.23
TOHIP	82.69
AOMDV	78.19

Table 5 illustrates the collision avoidance rate during the multipath routing in MANET based on three different methods, namely Hybrid Coordination Function based Poly Data Flag Encryption (HCF-PDFE) technique, Topology-Hiding multipath routing Protocol (TOHIP) [1] and Ad-hoc On-demand Multipath Distance Vector (AOMDV) [2]. The proposed BHS-SMM technique has higher collision avoidance rate than the existing methods.

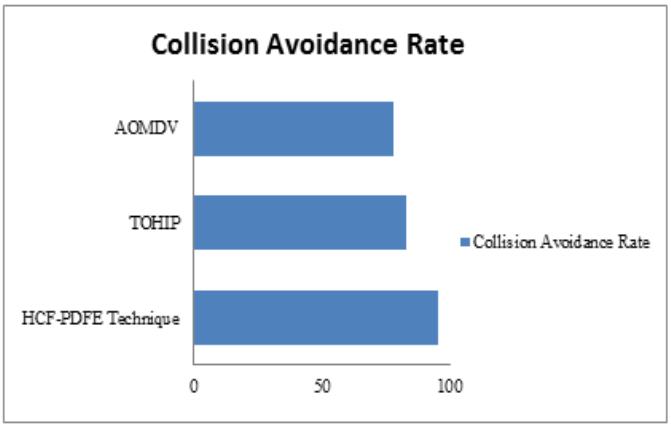

Figure 10 Measure of Collision Avoidance Rate

Figure 10 describes comparative analysis for collision avoidance rate with respect to different number of packets with proposed HCF-PDFE technique, TOHIP [1] and AOMDV [2]. The packets in the range of 10 to 100 are taken for calculating the collision avoidance rate in HCF-PDFE technique. Figure 10 proves that the proposed HCF-PDFE technique significantly increases the collision avoidance rate than TOHIP [1] and AOMDV [2]. The collision avoidance rate of HCF-PDFE technique is increased using the hybrid coordination function. Collision avoidance is carried out by DCF and PSF during the multipath routing process in MANET. The collision avoidance in HCF-PDFE is increased by 15 % and 21% technique compared to existing TOHIP [1] and AOMDV [2] respectively.

6. CONCLUSION

An efficient technique called Hybrid Coordination Function based Poly Data Flag Encryption (HCF-PDFE) Technique is proposed to avoid the collision and to increase the data security level in MANET. The proposed HCF-PDFE technique uses hybrid coordination function scheme for avoiding the collision and for improving the throughout level in MANET during data packets transmission. After the collision avoidance in HCF-PDFE Technique, the data security level is increased by using Poly flag data based encryption and decryption technique. In this technique, the data packets are encrypted with value and poly data flag encryption collects all the encrypted value. After collecting the encrypted data from multiple paths, it gets routed to the destination node. In the destination node, the poly data flag decryption decrypts the data packets and flag value separately. In addition, it helps to increase the security level based on the dropping ratio and reduces the routing overhead during the packet transmission in MANET in HCF-PDFE technique. The simulation is carried out for different parameters such as routing overhead, throughput, security level based on dropping ratio and collision avoidance rate. The results show that HCF-PDFE technique offers better performance with an improvement of collision avoidance rate by 18% and security level based on dropping ratio by 19% compared to existing methods.

REFERENCES

[1] Yujun Zhang, Tan Yan., Jie Tian, Qi Hua, Guiling Wang, Zhongcheng Li, "TOHIP: A topology-hiding multipath routing protocol in mobile ad hoc networks," Ad Hoc Networks, Elsevier, Volume 21, October 2014, Pages 109–122

[2] Prabha R. and Ramaraj, "An improved multipath MANET routing using link estimation and swarm intelligence", EURASIP Journal on Wireless Communications and Networking, Springer, Volume 173, December 2015, Pages 1-9

[3] Xenofon Fafoutis, Charalampos Orfanidis, and Nicola Dragoni, "Altruistic Backoff: Collision Avoidance for Receiver-Initiated MAC Protocols for Wireless Sensor Networks", Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks Volume 2014, Pages 1-11

[4] Siguang Chen and Meng Wu, "Anonymous multipath routing protocol based on secret sharing in mobile ad hoc networks", Journal of Systems Engineering and Electronics, Volume 22, Issue 3, June 2011, Pages 519 - 527

[5] Wei-Chen Wu and Horng-Twu Liaw, "A Study on High Secure and Efficient MANET Routing Scheme", Hindawi Publishing Corporation, Journal of Sensors, Volume 2015, February 2015, Pages 1-10

[6] Marwah M. Almasri, Abrar M. Alajlan, Khaled M. Elleithy, "Trajectory Planning and Collision Avoidance Algorithm for Mobile Robotics System", IEEE Sensors Journal, Volume 16, Issue 12, June 2016, Pages 5021 - 5028

[7] Hui Xia, Zhiping Jia, Lei Ju, Xin Li, Edwin H.-M. Sha, "Impact of trust model on on-demand multi-path routing in mobile ad hoc networks", Computer Communications, Elsevier, Volume 36, 2013, Pages1078–1093

[8] Y. Harold Robinson and M. Rajaram, "Energy-Aware Multipath Routing Scheme Based on Particle Swarm Optimization in Mobile Ad Hoc Networks", Hindawi Publishing Corporation, The Scientific World Journal, Volume 2015, November 2015, Pages 1-9

[9] Arshad Jhumka, Matthew Bradbury, Sain Saginbekov, "Efficient fault-tolerant collision-free data aggregation scheduling for wireless sensor networks", Journal of Parallel Distributed Computer Systems, Elsevier, Volume 74, Issue 1, January 2014, Pages 1789–1801

[10] Shengbo Yang, Chai Kiat Yeo, and Bu Sung Lee, "Toward Reliable Data Delivery for Highly Dynamic Mobile Ad Hoc Networks", IEEE Transactions on Mobile Computing, Volume 11, Issue 1, January 2012, Pages 111 - 124

[11] Poonam Gera, Kumkum Garg, and Manoj Misra, "Trust-based Multi-Path Routing for Enhancing Data Security in MANETs", International Journal of Network Security, Volume16, Issue 2, March 2014, Pages 102-111

[12] Rui Yang, Ying Song, Gui Chao, Baolin Sun, "Energy Entropy-Aware Multipath Routing Algorithm in MANET", International Journal of Advancements in Computing Technology (IJACT) Volume 4, Issue 15, September 2012.

[13] Zhiguo Wan, Kui Ren, and Ming Gu, "USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks", IEEE Transactions on Wireless Communications, Volume 11, Issue 5, March 2012

[14] A. Pratapa Reddy and N. Satyanarayana, "Energy-efficient stable multipath routing in MANET", Wireless Networks, Springer, April 2016, Pages 1–9

[15] Wesam Almobaideen, Roba Al-Soub, Azzam Sleit, "MSDM: Maximally Spatial Disjoint Multipath Routing Protocol for MANET", Communications and Network, Scientific Research, Volume 5, Issue 4, 2013, Pages 1-7

[16] Sungwook Kim, "Adaptive MANET Multipath Routing Algorithm Based on the Simulated Annealing Approach", The Scientific World Journal, Hindawi Publishing Corporation, Volume 2014, June 2014, Pages 1-8

[17] Abdulaziz Al-Nahari and Mohd Murtadha Mohamad, “Receiver-Based Ad Hoc on Demand Multipath Routing Protocol for Mobile Ad Hoc Networks”, PLoS ONE, Volume 11, Issue 6, 2016, Pages 1-18

[18] Poonam Gera, Kumkum Garg, and Manoj Misra, “Trust-based Multi-Path Routing for Enhancing Data Security in MANETs”, International Journal of Network Security, Volume 16, Issue 2, March 2014, Pages 102-111

[19] Minghu Wu, Siguang Chen, and Jiaping Liao “Data security in MANETs by integrating multipath routing and secret sharing”, Proceedings of the 2nd international Asia conference on Informatics in control, automation and robotics, Volume 1, 2010, Pages 72-75

[20] Sujatha. P. Terdal, V. D. Mytri, A. Damodaram, Uday. S. B, “Enhanced Multipath Routing with Congestion Avoidance for 802.11E based Mobile Ad-hoc Networks”, International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC), Volume 2, Issue 3, September 2011, Pages 141-152

Renuka Mohanraj received her Ph.D in CS from the Mother Teresa University, Kodaikanal, India in 2013. She is an Assistant Professor in the Department of Computer Science at Maharishi University of Management, Fairfield, Iowa. Area of research includes in mobile ad hoc networks with the particular focus on the topics Secure QoS routing, Congestion control and Data Security.