MANET Routing and Data Security with Multiple Packet Collision Control Using Acyclic Node-Links

Renuka Mohanraj

Computer Science Department, Maharishi University of Management, Fairfield, Iowa 52556, USA

Corresponding author: Renuka Mohanraj (mr.renuka@gmail.com)

Abstract: MANET (Mobile Ad-hoc Network) is an autonomous system facing several issues such as attacks due to the wireless communication media and limitation related to routing. Routing algorithm optimizes different performance metrics on single and multi-path communication. But, the problem occurs on selecting correct route path and provisioning of security for multiple packet transmission from source to destination node in MANET. Conversely, data packet transmission strategy over multiple route paths takes longer routing convergent time. All nodes in the mobile ad-hoc network is used for establishing the routing but the periodic performance fail on maintaining security level during packet transmission over multiple paths. Besides, Encryption Standard algorithms used consumes space unnecessarily. To overcome the difficulty of time and space complexity during packet transmission in MANET, PCC-MSR (Packets Collision Control based Multipath Secure Routing) method is proposed in this paper. First, Acyclic based Node-Link Routing approach in PCC-MSR is implemented to establish multiple route paths for efficient packet transfer. The collision control multiple packet transferring operation achieves minimal convergent time rate using the proposed method. Second, a method called as the Optimized Packet Cooperative Control is introduced to manage information about all packets transmitted through multiple paths. Finally, Multipath Secure Routing is carried out through H-EDES (Homomorphism based Enhanced Data Encryption Standard). H-EDES achieves higher security level with minimal space complexity rate on storing the encrypted information. Experiment is conducted on factors such as convergent time rate on multi path routing, security level on packet transfer from source to destination, and space complexity taken on encrypted data.

Keywords: Cooperative control, mobile ad-hoc network, enhanced data encryption standard, acyclic based, space complexity, collision control, security.

1. Introduction

In mobile ad hoc networks, whenever a source node wants to transmit a packet to the destination node, the source node broadcasts route request packet to its neighboring nodes. However, the neighboring node without the proper direction replies to the route request packet and further to the neighboring nodes in search for destination node. As a result, the network gets flooded with route request, route response and route error packets reducing the overall throughput.

TOHIP (TOpology HIDing Multipath routing Protocol) [1] did not carried routing information. As a result, the malicious node cannot predict the changing topology increasing the packet delivery rate. But, the problem was said to occur while identifying the correct path and ensuring security in MANET. DBRP (Distributed Beaconless Routing Protocol) [2] applied backbone-based approach to improve the packet delivery ratio by identifying the path and minimized the time taken to perform forward delay.

One of the main objectives of mobile ad hoc network is to stay connected anywhere to a network. As a result, the most important challenging tasks are to address the problems related to scalability and security of network, improving the lifetime of network and so on. To address these problems MP-OLSR (Multi Path Optimized Link State Routing) [3] used multipath dijkstra algorithm for deriving multiple
paths. However, the quality of service related to delay remained unaddressed.

EDAPR (Early Detection of congestion and Adaptive Routing) [4] was introduced to improve the performance in reduce delay and increasing the packet delivery ratio by applying bidirectional path discovery. Different routing protocols like AODV (Ad hoc on demand Distance Vector), DSR (Dynamic Source Routing) and LAR (Location Aided Routing) were introduced in Ref. [5] to improve the routing overhead. An EAODV (Extended AODV) [6] was designed to address scalability using proposed multipath routing scheme.

In MANETs (Mobile Ad-hoc Networks), congestion is one of the major issues to be handled that occurs in any intermediate node. They may occur due to resource limitation resulting in high packet loss, increasing the end to end delay and drastically affecting the time for resource utilization. DCDCR (Dynamic Congestion Detection and Control Routing) [7] identify the level of congestion using average queue and accordingly warning messages are issues to its neighbors. However, with the increase in traffic, DCDCR suffered from packet loss.

To minimize the packet loss, TCAM (Ternary Content Addressable Memory) [8] based packet classification was introduced that served the purpose of increased throughput using domain compression and prefix alignment. Another method, DCLD (Delay Controlled Load Distribution) [9] not only minimized the rate of end-to-end delay but also the packet recovery time with the aid of load balancing algorithm. A strategy called, FLDB (Fuzzy Logic Dynamic Beaconing) [10] was designed to identify the false node position with minimum delay.

Based on the aforementioned techniques and methods, we propose a PCC-MSR (Packets Collision Control based Multipath Secure Routing) method to overcome the difficulty of time and space complexity during packet transmission in MANET. The method combines the trustworthy on security and minimizes the collision rate by improving the multipath packet data delivery ratio in MANET. The method uses an Optimized Packet Cooperative Control to manage information about all packets transmitted through multiple paths and with the application of H-EDES (Homomorphism based Enhanced Data Encryption Standard) security is achieved. Extensive experiments showed that our method provided higher level of convergent time by minimizing the dropping ratio.

2. Related Works

Several routing mechanisms have induced a significant interest from the early period of design of MANET until the present time. Quality of Service was addressed in Ref. [11] based on shortest multipath based routing. However, the accurate measurement of capacity was an open issue. With the aid of EA (Evolutionary Algorithms) and AHP (Analytical Hierarchy Process) [12] optimized routing was measured. Caesar cipher was applied that resulted in average throughput gain.

POR (Position based Opportunistic Routing) [13] was introduced to address reliability and timeliness of data at the receiving end using VDVH (Virtual Destination-based Void Handling). However, security remained unaddressed. TMR (Trust-based Multipath Routing) [14] provided complete security using multiple secure route discovery improving the average latency.

With the increase in popularity of the mobile devices, routing has become a challenging task due to the dynamic network topology and critical energy efficiency and becomes further complicated with huge population of devices. As a result, multiple unicast nature of the model has to be replaced with multicast routing. A distributed algorithm was proposed in Ref. [15] using transient multicast tree for increasing the minimum residual energy during packet transmission. USOR (Unobservable Secure On-demand Routing) was designed in Ref. [16] to provide an insight into privacy from both inside and outside attacks using ID-based encryption. However, security concerns with
related to topology remained unaddressed. JATC (Joint Authentication and Topology Control) [17] addressed the throughput and authentication using discrete stochastic optimization problem.

With the objective of increasing the network throughput, MSDM (Maximally Spatial Disjoint Multipath) [18] routing was introduced that used spatially disjointed path to reduce the occurrence of collision. EEMRA (Energy Entropy-aware Multipath Routing Algorithm) [19] increased network lifetime and packet delivery ratio by reducing the average delay by evaluating the fitness of the path. COMB (Cell-based Orientation aware MANET Broadcast) [20] provided collision free transmission based on the hidden terminal problem. Though a plethora of multicast routing protocol for minimizing the collision has been designed, the difficulty of time and space complexity has yet to be solved. With this aim, packets collision control based multipath secure routing in MANET is designed in the forthcoming sections.

3. Packets Collision Control Based Multipath Secure Routing in MANET

The main objective of the proposed work (i.e., PCC-MSR method) is to establish the routing and perform end to end data delivery with high security level. Besides, multipath routing increases the reliability level by reducing the routing convergent time. In PCC-MSR method, multipath routing information is updated as the network topological structure changes. The discovery of the multiple paths route and maintenance of route path without any attacks is the significant part in our proposed method. Fig. 1 shows the multi packet transfer with control path in MANET that includes the class of routing between the source and destination node.

The multiple packets $\text{Pack}_1, \text{Pack}_2, \text{Pack}_3, ..., \text{Pack}_n$ are transferred from the source node through multiple paths $P_1, P_2, P_3, ..., P_n$ in PCC-MSR method. The paths carry different sized packets, where reliable data delivery is carried out in the proposed method. The control path is also managed in the proposed system, to carry the information about all packets. The control path is managed in PCC-MSR method using Optimized Packet Cooperative Control. The Optimized Packet Cooperative Control scheme keeps all the information securely to improve the reliability of the system. The architecture diagram of PCC-MSR method is illustrated in Fig. 2.

The PCC-MSR method in mobile ad-hoc network is capable of roaming independently without any infrastructure. The multipath basis packet transmission from source to the destination uses the Acyclic Based Node-Link Routing approach. The acyclic based consists of the vertices and directed edges to establish the route through nodes and accordingly links the path. The Acyclic based Node-Link Routing approach in PCC-MSR minimizes

Fig. 1 Multi packet transfer with control path in MANET.

Fig. 2 Architecture diagram of PCC-MSR method.
the collision rate on packet transfer through the multiple paths. The established route path also maintains all the packet information such as each route path packet count, size of the each packet and bandwidth.

Optimized Packet Cooperative Control approach manages the packet information with the high precision rate. The data delivered to the destination end through multiple paths is secured in PCC-MSR method using Homomorphism based Enhanced Data Encryption Standard. H-EDES performs the encrypted operations using ElGamal cryptosystem to improve the security rate. The padding scheme is introduced on H-EDES in order to reduce the space complexity.

In the real world scenario, a system for transmitting video over mobile ad hoc network using multipath routing is presented. In the system, the mobile ad hoc network includes multiple paths to be considered for video transmission. The total number of paths need not be equal to the streams that are being transmitted (i.e., video). So the proposed method PCC-MSR is used to maintain multiple route paths on mobile ad-hoc network. A path may carry any number of streams and the video to be transmitted in multipath routing needs to be safely transmitted to the destination so that the total packets to be delivered should be within an acceptable range.

The task of the Acyclic Based Node-Link Routing is to handle different types of routing services without any collisions between the nodes. Using Optimized Packet Cooperative Control approach, the system adapts to different network conditions due to several path constraints caused by different nodes while reaching the destination and therefore minimizes the dropping ratio. A scheme to provide high reliability is also ensured by applying control scheme in mobile ad hoc network by maintaining the flow of video to be transmitted to the destination. The security between the nodes during the video transmission is enhanced using Homomorphism based Enhanced Data Encryption Standard.

3.1 Acyclic Based Node-Link Routing

Routing topology is established in PCC-MSR method with multiple paths $P_1, P_2, P_3, ..., P_n$. When the source node needs to transfer the data packets to the destination node, the route request is sent to multiple paths in MANET. When the request is accepted, reliable route path is chosen to transfer the packets $Pack_1, Pack_2, Pack_3, ..., Pack_n$ in mobile ad-hoc network. The vertices and edges which carry the packets compute the routing based on acyclic node-link property. The acyclic non-link property is described as

$$\text{Acyclic Node Link Property} = \{P_i (\text{Node}_1 \rightarrow \text{Node}_2 ) \rightarrow Pack_1, Pack_3\}$$

(1)

The nodes in PCC-MSR are linked through the edges for packet transfer from source to destination node. In Eq. (1), path ‘1’ $P_1$ carries the packets $Pack_1$ and $Pack_3$ for reliable data delivery on destination end. The construction of acyclic based multipath routing consists of the vertex connected to mobile ad-hoc network through edges. The objective behind Acyclic Node Link property is required for the direct construction of route path in MANET using the path extension procedure. The routing path established in PCC-MSR method is extended till the destination node for reliable data delivery. The path extension is formularized as

$$\text{Extension} c(\text{flow}) = \sum_{\text{edges output}} \text{flow( edges )} - \sum_{\text{edges input}} \text{flow( edges )}$$

(2)

Acyclic based node link is extended using the PCC-MSR method with the flow of route path though the vertices ‘v’. The flow through the edges of the output vertices is extended to the input of the next vertices to extend the route path and reaches the destination node in MANET. The algorithmic description of Path Extended in PCC-MSR method is formularized as

**Algorithm: Path Extended Procedure**

**Input:** RouteReq()

**Output:** PathExtended

Initialize RouteReq $\rightarrow$ 0, flow(edges) $\rightarrow$ 0,
MANET Routing and Data Security with Multiple Packet Collision Control Using Acyclic Node-Links

Paths = \( (P_1 = P_3, P_2, P_3, \ldots, P_n) \)
Initilaize \( Pack_i = (Pack_{1}, Pack_{2}, Pack_{3}, \ldots, Pack_{n}) \)

**Begin**

1: While \( RouteReq \) <> 0
2: Assign paths \( P_i \)
3: For each \( P_i \)
4: Transfer packets \( Pack_i \)
5: While extending path ‘P’ in Acyclic flow, Do
6: Compute Extension \( c(flow) \) measure
7: Repeat
8: Evaluate Acyclic Node Link Property for reducing the collisions on packet flow ‘C’ through edges
9: Until extension step as flow path ‘P’ reaches the destination node
10: End while
11: End for
12: Return \( RouteReq () \)

The algorithmic step describes about the path extension from source to the destination using the acyclic based node-link property. The packet send from source achieves reliable data delivery by transferring through multiple paths with minimal convergent time rate in PCC-MSR method. The “flow” between the vertices in PCC-MSR method helps to reach the destination nodes with minimal dropping ratio.

### 3.2 Optimized Packet Cooperative Control

Optimized Packet Cooperative Control in PCC-MSR is used to manage the information about all routing packets transmitting through multiple paths. The optimized packet cooperative control scheme extracts the information about the route path packet count, size of each packet and bandwidth of the packet. It is said to be optimized packet cooperative control as PCC-MSR method jointly considers the packet capacity and internal network cooperative communication to improve packet delivery at destination end for minimizing the convergent time. The cooperative control maintains the packet information for optimizing overall system performance rate. The cooperative control scheme that carries the information of different packets in multiple paths on mobile ad hoc network is given as below

\[
\text{Cooperative Control of (Pack)} = N\{\text{Packcount, Packsize, Packb}\} \quad (3)
\]

The cooperative control scheme combines the physical network information and packet information to improve the reliability rate on proposed method. The ‘Pack’ packets count, size and bandwidth rate are controlled in this route path for obtaining optimized result. Bandwidth range in PCC-MSR method for packet transfer on multiple paths is described as

\[
b = \text{Max}\left(\frac{TRP}{2} + \text{Time}_{\text{tot}}\right) \quad (4)
\]

where \( \text{Time}_{\text{tot}} \) is the total time taken on packet transfer through the every route path ‘i’ and ‘TRP’ is the total route path in MANET. The bandwidth rate for packet transfer on constructed route path in PCC-MSR method achieves the maximum result rate.

### 3.3 Multipath Secure Routing

Multipath security is enhanced in PCC-MSR method using the encryption standards. To incorporate the security factor on multipath routing, an enhanced encryption scheme is used to reduce the attacks. Multipath secure routing based on Enhanced Data Encryption Standard is strong enough to create the secret keys and perform the secret information storage with minimal space complexity.

#### 3.3.1 Homomorphism Based Enhanced Data Encryption Standard

H-EDES is employed to achieve higher security level with minimal space complexity rate on storing the encrypted information. The process involved in the design of Enhanced Data Encryption Standard is strong enough to create the secret keys and perform the secret information storage with minimal space complexity.

The proposed method uses Homomorphism based Enhanced Data Encryption Standard with the aid of ElGamal cryptosystem based secret key creation. Here, the secret key ‘k’ is selected in a random manner and
evaluates the shared secret points. The shared secret points computed are embedded with the original packet ‘\text{Pack}_i’ using the padding scheme. In this way, the packet is embedded with the encrypted secret shared key ‘k’ using the ElGamal cryptosystem.

PCC-MSR method with data encryption standard uses sensitive packet information on transferring through multiple paths in MANET. The Homomorphism property used on the secret shared key creation is of the form:

\[ E(K1) = C1^{r1}, k1, h^{r1} \]  

In Eq. (5), the homomorphism ‘h’ denotes the C1^{r1} (i.e., collection of whole packets with the secret shared key ‘\text{k}’) in the cryptosystem where ‘r1’ is the random position value used along with the packet information on the encryption side. The Enhanced Data Encryption standard is used in PCC-MSR method for encrypting the data with minimal space complexity. On the destination end the packets with encrypted secret key are decrypted to attain the original message through multiple paths.

\[ \text{Original Sender Packet Information} = D(E(K1)) \]  

4. Simulation Model

We use a simulation model based on NS2. We study the performance of PCC-MSR in MANET using simulator tool NS2. In our simulation, 50 mobile nodes move in a 1,200 m × 1,200 m rectangular region for 500 seconds simulation time. Compared with a square region, the rectangular region is selected in PCC-MSR so that performance of packets collision can be easily observed. Initial locations of the nodes are obtained by using uniform distribution. PCC-MSR method in MANET assumes that each node moves independently with the same average speed. All the nodes in PCC-MSR have the same transmission range of 300 meters.

The mobility model selected for PCC-MSR method is the random waypoint model to perform multipath packet transfer in MANET. In this random waypoint mobility model, a source node selects the destination node in a random manner. The RWM uses typical number of mobile nodes for locating the movable nodes. It moves towards the direction of the destination node with a perfect balance between the minimal speed and maximal speed. Once the source node reaches the destination, the node remains there for a pause time between 0 s and 600 s. The dynamic changing topology uses DSR (Dynamic Source Routing) protocol to perform the experimental work. Moving speed of the mobiles in the MANET is about 2.5 m/s of each mobile node.

The traffic simulated using PCC-MSR method is CBR (Constant Bit Rate). The size of all data packets was considered to be 512 bytes with 35 source nodes and 35 destination nodes were selected in a random manner. The time interval for multipath packet transfer was set to 350 ms. A packet is said to be dropped in PCC-MSR when no acknowledgement is said to be received after several retransmissions. For each scenario, seven runs were performed and the results were averaged.
5. Simulation Results

5.1 Performance Metrics

The performance of PCC-MSR method in MANET is compared with the existing TOHIP [1] and DBRP [2] in MANET. The performance is evaluated according to the following metrics.

5.1.1 Convergent Time on Multipath Routing

Convergent time on multipath routing using PCC-MSR method includes the packet capacity and internal network cooperative communication. It is measured in terms of milliseconds and is calculated as follows.

\[
CT = Time(Pack_{count}, Pack_{size}, Pack_{b})
\]  

(7)

5.1.2 Security Level on Packet Transfer Based on Dropping Ratio

The security level of packet transfer based on dropping ratio using PCC-MSR method 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 is evaluated as given below:

\[
DR = \frac{\text{Packets}_{send} - \text{Packets}_{recv}}{\text{Packets}_{send}} \times 100
\]  

(8)

5.1.3 Multipath Packet Data Delivery Ratio

Multipath packet data delivery ratio in PCC-MSR method measures the ratio of the number of actually received multipath data packets to the incoming multipath data packets. It is measured in terms of percentage.

\[
MPDR = \frac{\text{Multipath Packets}_{recv}}{\text{Multipath Packets}_{send}} \times 100
\]  

(9)

5.2 Performance Comparison of Convergent Time on Multipath Routing

Fig. 4 shows the result of convergent time on multipath routing versus the varying number of mobile nodes. To better perceive the efficacy of the proposed PCC-MSR method, substantial experimental results are illustrated in Fig. 4. The PCC-MSR method is compared against the existing TOHIP [1] and DBRP [2].

Results are presented for different number of mobile nodes. The convergent time on multipath routing for several mobile nodes measures the time taken for convergence on multipath routing as in Eq. (1). Higher, the number of mobile nodes, more successful the method is. The results reported here confirm that with the increase in the number of mobile nodes, the convergent time on multipath routing also increases. The process is repeated for 35 mobile nodes for conducting experiments.

As illustrated in Fig. 4, the proposed PCC-MSR method performs relatively well when compared to two other methods TOHIP [1] and DBRP [2]. The method had better changes using the path extended procedure that eventually considered the packet count, packet size and bandwidth rate of the packets on multipath rapidly by 10-42% when compared to TOHIP [1]. Moreover, Optimized packet cooperative control in PCC-MSR method jointly considers the packet capacity and internal network cooperative communication resulting in increasing the convergent time on multipath routing by 13-71% when compared to DBRP [2].

5.3 Performance Comparison of Security Level on Packet Transfer Based on Dropping Ratio

In order to increase the security level on packet transfer based on dropping ratio on multipath routing, the packets sent and packets received to handle varied traffic condition on multipath routing is considered. In the experimental setup, the number of packet sent ranges from 3 to 21. The results for 7 packets of equal size of 512 bytes are illustrated in Fig. 5. The resultant dropping ratio using our method PCC-MSR offer comparable values than the state-of-the-art methods.
The resultant dropping ratio is the ratio of the different between packets sent and packets received to the total packets sent in MANET.

The targeting results of dropping ratio to measure the security level using PCC-MSR method is compared with two state-of-the-art methods [1, 2] in Fig. 5 is presented for visual comparison based on the number of packets placed. Our method differs from TOHIP [1] and DBRP [2] in that we have incorporated Optimized Packet Cooperative Control that efficiently send the packet on multipath routing to its intended destination nodes by improving the dropping ratio or security by 3-7% than when compared to TOHIP. In addition with the application of control path based on packet size, count and bandwidth further reduces the dropping ratio and increases the security level by 10-16% when compared with the DBRP [2].

5.4 Performance Comparison of Multipath Packet Data Delivery Ratio

Fig. 6 given below shows the multipath packet data delivery ratio for PCC-MSR method, TOHIP [1] and DBRP [2] versus increasing number of packets from 3 to 21. The multipath packet data delivery ratio improvement returned over TOHIP and DBRP decreases gradually as the number of packets gets increased though not linear because of the multipath nature and changes in the topology.

As illustrated in Fig. 6, for example when the number of packets sent is 9, the percentage improvement of PCC-MSR method compared to TOHIP is 12.61% and compared to DBRP is 19.64%, whereas when the number of packets sent is 18 the improvements are around 15.99 and 24.95% compared to TOHIP and DBRP respectively. The reason is because of the application of Acyclic based Node-Link Routing. Besides, the selection of reliable route path in PCC-MSR is performed based on acyclic node-link property where the nodes are linked through the edges for efficient packet transfer resulting in increased multipath packet delivery ratio by 11-15% compared to TOHIP.

Moreover, the output vertices are extended to the input of the next vertices that in a way extends the route path by increasing the multipath packet delivery ratio by 17-32% compared to DBRP.

6. Conclusions

A Packets Collision Control based Multipath Secure Routing method to overcome the difficulty of time and space complexity during packet transmission in MANET is introduced. We then showed how this method can be extended to incorporate multiple route paths for efficient packet transfer using Acyclic based Node-Link Routing approach. Two different approaches namely Optimized Packet Cooperative Control and Homomorphism based Enhanced Data Encryption Standard are provided. The Optimized Packet Cooperative Control works on managing information about all packets transmitted through multipath in MANET. Using the cooperative control scheme the security level on packet transfer from source to destination is reduced. The Homomorphism based Enhanced Data Encryption Standard constructs
an Elgamal cryptosystem based secret key creation and the Homomorphism property to compare this method to ongoing traffic activity. We presented a rigorous framework to identify multipath packet data delivery ratio using Acyclic based Node-Link Routing. In our experimental results, the Packets Collision Control based Multipath Secure Routing showed a better performance than the state-of-the-art-works over the parameters, convergent time on multipath routing, security level and multipath packet data delivery ratio.

References