CIT. Journal of Computing and Information Technology, Vol. 26, No. 4, December 2018, 251–265
doi: 10.20532/cit.2018.1004224

Security Enhanced Location-aided Level-based Disjoint Multipath Routing Algorithm for Mobile Ad Hoc Networks

Vasudevan Muthupriya and Sathyanarayanan Revathi

BS Abdur Rahman Crescent Institute of Science and Technology, Chennai, India

In mobile ad hoc networks (MANET), the location-based multipath routing protocols involves less routing overhead compared to non-location-based protocols. This paper proposes two location-based algorithms, Enhanced Location-aided Level-based node Disjoint Multipath routing (ELLDMR) and Secure Location-aided Level-based node Disjoint Multipath routing (SLLDMR), to enhance the link lifetime and the security of the MANET. The objective of ELLDMR is to build multiple paths with non-critical nodes so that the lifetime of the routing path is significantly increased. It also hides the source, destination and path identity in intermediate nodes to avoid intrusion of routing attacks in the routing path. The SLLDMR is an enhancement over ELLDMR where it aims to overcome rushing attack and exhibit secure data transmission using two-level cryptographic processes. The performances of ELLDMR and SLLDMR are simulated using NS2 where it shows a minimum routing overhead, less end to end delay and high packet delivery compared to existing Location-aided Level-based node Disjoint Multipath routing (LLDMR) algorithm and Topology Hiding multipath protocol (TOHIP).

ACM CCS (2012) Classification: Networks → Network protocols → Network layer protocols → Routing protocols

Security and privacy → Cryptography → Cryptanalysis and other attacks

Keywords: node disjoint multipath, noncritical nodes, link lifetime, routing attacks

1. Introduction

In MANET [1], the secure multipath routing protocols [2] fail to hide the topology information during route discovery and packet transmission phase. So, the adversary nodes can eventually invade into the routing path using the topology information in the routing messages. Therefore, topology exposure problem is a big challenge in MANET. Many active attacks [3], [4] like black hole attack, worm-hole attack, rushing attack, replay attacks, etc. can likely make use of this topology information and possibly get into the routing path. The existing security protocols are either cryptographic like ARAN [5], SRP [6], ARIADNE [7] or source and destination anonymous routing protocols like ANODR [8], ARMAN [9], ALERT [10]. The anonymous security routing protocols increase the routing overhead and cryptographic routing protocols are more expensive. So, topology hiding during the route discovery phase would be a better solution for preventing the inclusion of attacker nodes in the routing path. Therefore, this paper proposes two topology hiding routing algorithms, namely ELLDMR and SLLDMR. The performance of these algorithms is evaluated and compared with existing topology hiding multipath routing protocol TOHIP [11].

The ELLDMR and SLLDMR are proposed for secure route discovery and secure packet transmission in MANET. The main objective of these two algorithms is to ensure safe delivery of the packet to the destination, without any alteration or loss of data. The first algorithm ELLDMR is proposed to overcome the topology exposure problem where it hides the source, destination and routing path information in the intermediate nodes during route discovery.

Due to this anonymity, it is impossible for the attacker nodes to intrude into the routing path using false information.

The second algorithm SLLDMR is proposed for secure packet transmission using two-level encryption and decryption processes. In SLLDMR, the nodes do not depend on any centralized trusted server to generate their public or private key as in other security algorithms. This makes the attacker node difficult to forge these keys from the centralized server using fake identities. Also, the encryption or decryption are done only at the source and destination in SLLDMR, and so, they involve less cost when compared to other cryptographic algorithms.

This paper is organized as follows: Section 2 describes MANET security. Section 3 gives a survey of related work. Section 4 and Section 5 elaborate on the proposed work, ELLDMR, and SLLDMR algorithm respectively. Section 6 presents the experimental results. Finally, Section 7 concludes the proposed work with the scope for future work.

2. Security in MANET

The network layer attacks [4] are generally classified as external and internal attacks; external attacks are caused by the nodes which are outside the transmission region of the network while internal attacks are caused by the compromised nodes within the same network. Based on the severity of external or internal attacks, network layer attacks are further divided into active and passive attacks. A passive attack overhears the packet information and does not cause any damage or alteration to it. Ex: eavesdropping, traffic analysis, and monitoring. An active attack is a dangerous attack as it damages or discards the packet by not allowing it to reach the destination. Sometimes, it intends to alter the packet information and so the impact of active attacks in the network layer is more serious. Ex: jamming, spoofing, modification, replaying and DoS attacks.

Many research works were carried out to avoid these passive and active attacks. Secure routing protocols like ARAN [5], ARIADNE [7], SA-ODV [12] are cryptographic based single path routing protocols and they are expensive. But the performance of multipath routing protocols is far better than single path routing protocols as in multipath routing protocols the path, including adversary nodes, could be avoided and a different path can be chosen for secure packet transmission. The secure multipath routing protocols are mostly node-disjoint, only then the adversary nodes could be easily controlled.

3. Related Works

The on-demand Secure Routing Protocol (SRP) [13] is a node-disjoint multipath routing mainly designed for Dynamic Source Routing (DSR). The security association between source and destination is established by exchanging a secret symmetric key. This is generated using public keys of sender and receiver and, thus, mutual authentication is enabled between them.

The secure multipath routing protocol [14] is a multipath routing protocol based on the Ford-Fulkerson MaxFlow algorithm. Unlike SRP, it authenticates every intermediate node included in the routing path using digital signatures. Also, it finds all possible multiple paths between the source and destination within a TTL period. The size of the route request (RREQ) packet increases as it appends the previously received information for every broadcast. The main drawback of this protocol is that it cannot compromise with route request costs and so the delay and processing power increase.

The SecMR [15] is a Secure Multipath Routing protocol which reduces the node authentication cost by dividing the protocol into two phases. The first phase is an authentication phase, where at regular (periodic) time intervals, the neighbour nodes are verified using digital signatures. In the second phase, these authenticated nodes participate in route discovery. This increases the lifetime of route request compared to the SRP.

The cryptographic techniques employed in some of these protocols are more expensive and so they are cost effective. All of these multipath routing protocols carry the routing information during the route discovery period and thus expose the topology information to attacker nodes. TOHIP [11] is the first routing protocol to find a solution to this topology exposure problem.

This protocol is a loop-free secure node disjoint multipath routing protocol. Every node in this protocol knows only its neighbour information and is not exposed to topology information. It uses hop count and round-trip time together as the routing metric to avoid worm hole and rushing attack. To make a reliable transmission, it initiates route probe phase before transmitting the packet towards the destination.

The enhanced TOHIP [11] does neighbour authentication by obtaining the certificate from a trusted certificate server so that it can resist modification attack, impersonation attack, and fabrication attack. The drawback of this protocol is that it chooses the intermediate nodes based on the number of hop counts and does not consider their mobility parameter. Since in MANET the nodes are highly mobile in nature, it is better to choose the intermediate nodes which do not move out of the transmission region earlier when compared to other nodes. Even the location of the nodes within the transmission range is to be considered when choosing the intermediate node. Since MANET does not have proper infrastructure, having a trusted certificate server is a tricky and cost-effective process. Therefore, the existing protocol, enhanced TOHIP is not highly reliable and secure.

LLDMR [16] is the Location-aided Level-based disjoint multipath routing protocol, where like LAR [17], it identifies the intermediate nodes between the source and destination using their location information and divides them into different levels depending on the node's distance from the destination. Figure 1 shows different levels of the nodes and the inter-links and intra-links between these nodes. This algorithm predicts the occurrence of link failure and sends the notification to the source node and switches to the alternate route during packet transmission based on the node's position. The major drawback of this protocol is that it does not find all existing multipaths as it avoids duplicate RREQ broadcast. So, in case of a frequent link failure, the multiple paths found are not sufficient for packet transmission and this may lead the LLDMR to initiate a route discovery phase. Also, the algorithm has not provided any security mechanism to overcome routing attacks. In this paper, two algorithms, ELLDMR and SLLDMR, are proposed to enhance the route lifetime and security aspects of LLDMR.

4. Enhanced Location-aided Level-based Disjoint Multipath Routing Protocol (ELLDMR)

4.1. ELLDMR Data Structure

The proposed algorithm ELLDMR is an enhanced Location-aided Level-based disjoint multipath routing protocol. The route discovery phase of ELLDMR is an extension over LLDMR so that it can provide a strong link in the routing path. During the route discovery phase, the forwarding nodes for packet transmission are chosen in such a way that its path lifetime is longer and the link failure rate is less when compared to LLDMR.

Like LLDMR, the ELLDMR broadcasts Location Request packet (LREQ) to find the location of the destination. The destination node acknowledges the LREQ by sending its location information through the Location Reply packet (LREP) to the source. After learning the destination location, the ELLDMR identifies the intermediate nodes for RREQ broadcast and groups them into different levels with respect to their distance from the destination node. Figure 1 shows the intermediate nodes between the

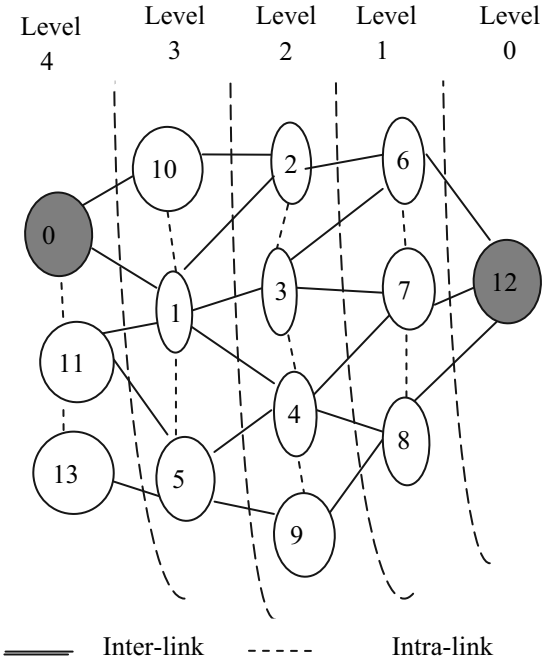

Figure 1. Inter-link and intra-link representation of intermediate nodes.

source and destination and their different levels, intra-level and inter-level nodes.

The neighbour list, information database, and routing table are the three data structures maintained by the forwarding nodes in ELLDMR. Their contents are:

- *Neighbour List:* In the neighbour list, each node maintains the neighbour (id, location, speed, direction) information.
- *Node Information Database:* Table 1 shows the record of data stored in each node. The node information database of ELLDMR includes the node's threshold value ($TH(Node_{mn})$), level's minimum threshold value ($TH\text{-}MIN(Level_n)$), and level's maximum threshold value ($TH\text{-}MAX(Level_n)$) and other information of the node. These are calculated using equation (1, 2, 3) respectively.

$$TH\left(Node_{mn}\right)=\frac{Dist\left(Node\left(x,y\right),D\left(x,y\right)\right)}{Dist\left(S\left(x,y\right),D\left(x,y\right)\right)} \tag{1}$$

$$TH\text{-}MIN\left(Level_n\right)=\frac{Min.Dist\left(Level-n,D\left(x,y\right)\right)}{Dist\left(S\left(x,y\right),D\left(x,y\right)\right)} \tag{2}$$

$$TH\text{-}MAX\left(Level_n\right)=\frac{Max.Dist\left(Level-n,D\left(x,y\right)\right)}{Dist\left(S\left(x,y\right),D\left(x,y\right)\right)} \tag{3}$$

The constant value C is defined as a change of the threshold value of the node for every second.

$$C=\frac{M}{Dist\left(S\left(x,y\right),D\left(x,y\right)\right)} \tag{4}$$

where M is the maximum distance a node can travel per second.

- *Routing table:* Table 2 shows the contents of the intermediate node's routing table, where each intermediate node maintains its own information and previous node (Prev → id) and next node (Next → id) information. The next node is the next forwarding node to which the intermediate nodes transmit the data packets received by them. Thus ELLDMR does not expose the topology information to the intermediate nodes.

Table 1. Node Information Database.

Parameter	Value
Node.Level	Level of the node
Status (0/1)	Visited / Unvisited node
Node (x, y)	Node position
S.id	Source id
$S(x, y)$	Source position
D.id	Destination id
$D(x, y)$	Destination position
Inter-link nodes	The link between adjacent level nodes.
Intra-link nodes	The link between same level nodes.
$TH(Node_{mn})$	Node threshold value
$TH\text{-}MIN(Level_n)$	The minimum threshold value of the node's level.
$TH\text{-}MAX(Level_n)$	The maximum threshold value of the node's level.

Table 2. Routing table information.

Prev → id	Node.id	Next → id

4.2. Critical and Noncritical Section Nodes

The critical section and non-critical section regions are defined as follows

- The non-critical section of $level_n$ is defined as the section *between* ($TH\text{-}MIN(level_n)$ + C) and ($TH\text{-}MAX(level_n) - C$).
- The critical section of $level_n$ is defined as the section, excluding the non-critical section of $level_n$. The critical section regions are generally the boundary region between any two levels.

In Figure 2, the regions marked with double-ended arrows are the critical section regions and excluding them are non-critical regions. Here, R is the transmission range of the network, therefore the nodes in R range is one hop nodes which are connected directly without any

intermediate nodes. The critical nodes are the nodes which lie in the critical section and the non-critical nodes lie in the non-critical region. The representation of critical and non-critical nodes is shown in Figure 2. In ELLDMR, only non-critical nodes are chosen as the forwarding nodes during the route discovery phase in order to prevent frequent link failures during packet transmission.

4.3. ELLDMR Route Discovery

The route discovery process is initiated by broadcasting the RREQ packet, mostly to the intermediate non-critical nodes in the direction of the destination. Figure 3 shows sample multiple paths discovered using non-critical nodes for the network given in Figure 2. This section discusses in detail the ELLDMR procedure to discover multiple paths using non-critical nodes. Like LLDMR, the intermediate nodes are grouped into different levels with respect to the distance from the destination. During RREQ broadcast, each intermediate node finds its next forwarding node and records it into the routing table. In ELLDMR, only the source node can send the RREQ packets to non-critical intra and inter-level nodes, all other intermediate nodes initially broadcast the RREQ only to their non-critical inter-level nodes in the direction of the destination. If the intermediate node does not find any non-critical inter-level nodes, it then broadcasts the RREQ packet to other inter-level and intra-level nodes. This can void the void [18] situation as in any other greedy routing protocol. The following are the ELLDMR route discovery steps for finding node disjoint multiple paths between any source and the destination node.

1. The source node floods the RREQ to the non-critical intra-level and non-critical inter-level nodes in the request zone.
2. The nodes in the request zone discard the duplicate RREQ, otherwise it is accepted.
3. Upon accepting the RREQ packet, the intermediate node checks whether it is a destination node.
4. If it is not a destination node,
   (i) The intermediate node marks the sender node as its previous node in the routing table and sends the reverse route notification to the sender node.
   (ii) The sender node, upon receiving the notification from its neighbour node, marks the neighbour node as its next forwarding node in the routing table.

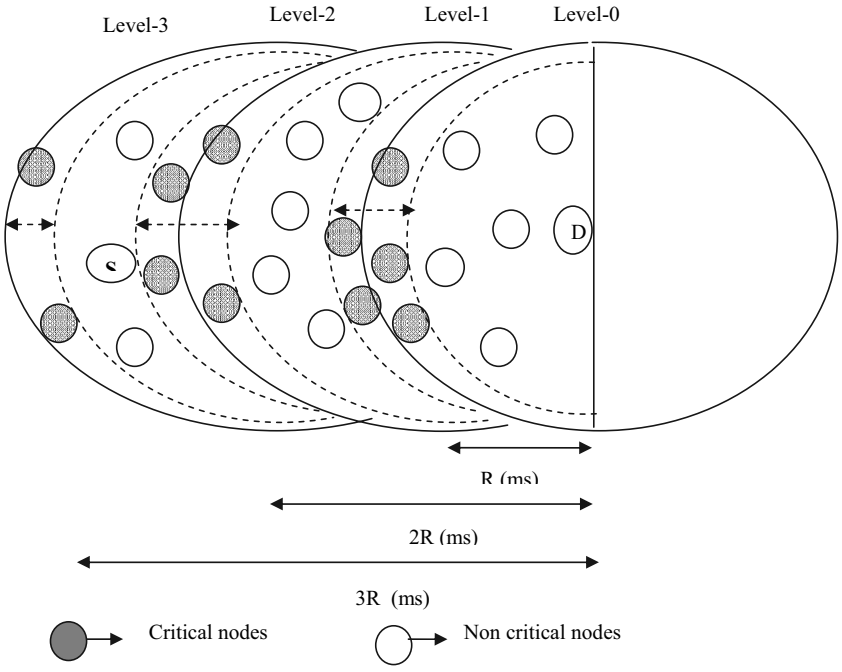

Figure 2. The network showing critical and non-critical nodes at each level.

(iii) The intermediate node then forwards the RREQ to its non-critical inter-level nodes

(iv) If the intermediate nodes have more than one non-critical inter-level forwarding node, they choose the one which has lesser mobility than others. This will ensure more lifetime for the routing link, so that the link failure will be infrequent.

(v) Then go to step 2 and repeat the process

5. If it is a destination node, it sends the reverse route to the sender node and stops the process of RREQ forwarding.
6. Then the destination node sends the route reply (RREP) packet to its previous node through the reverse route path formed using the previous node till it reaches the source node.

It finds node disjoint multipath by not accepting the duplicate RREQ by the intermediate nodes similar to LLDMR. Though the ELLDMR does not find all the existing paths between the source and destination, the infrequent link failure compromises the life of the route during packet transmission.

The following are the differences between LLDMR and ELLDMR in the route-finding process.

1. In ELLDMR non-critical intermediate nodes are given more priority for RREQ broadcast.
2. The RREP from intermediate nodes is not accepted.
3. The intermediate nodes of ELLDMR maintain only the forwarding node information in their routing table and so do not expose topology information.

4.4. Route Maintenance

The chance of a link failure is much smaller in SLLDMR than in LLDMR, because only non-critical nodes are used to find the path between the source and destination. In the rare case, when it is likely for link failure during packet transmission, like LLDMR, the proposed algorithm SLLDMR also predicts the movement of non-critical nodes to the critical region. Thus, it switches to the alternate path even before the occurrence of link failure, by giving notice to the source node.

The ELLDMR is more concerned in finding stronger disjoint routing paths than the number of disjoint routing paths. Though the ELLDMR does not discover all the available number of disjoint paths, it builds a stronger route between source and destination, thus eliminating frequent link failures and switching between the routes.

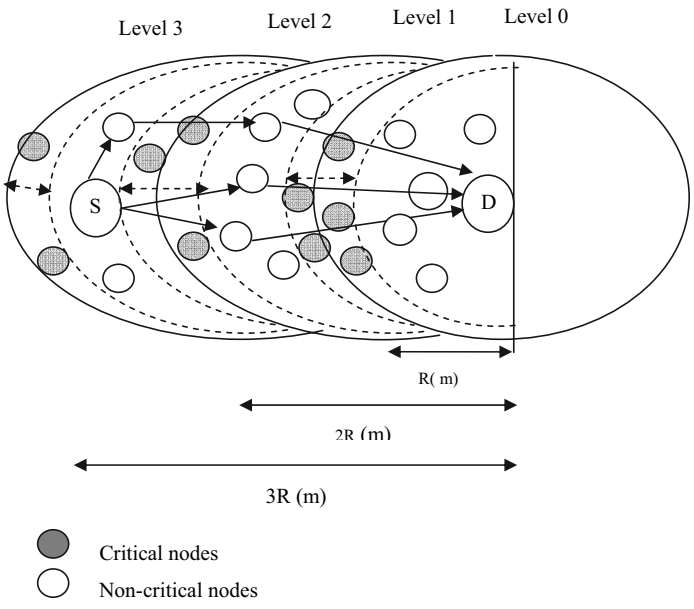

Figure 3. Multipath route discovery using non-critical nodes.

5. Secure Location-aided Level-based Disjoint Multipath Routing Protocol (SLLDMR)

5.1. Security Analysis

As said earlier, the routing in MANET is a critical issue, due to invasion of malicious nodes during the route discovery phase. Some of the routing attacks by which these malicious nodes get included in the routing path during the route discovery phase are as follows:

- *Black-hole attack:* The intermediate nodes communicate to the sender node that it has the shortest path to the destination.
- *Rushing attack:* The intermediate nodes, upon receiving the RREQ forward it immediately (avoiding inter-frame delay) to their neighbour nodes. Thus, the path through the attacker node can reach the destination earlier.
- *Worm-hole attack:* It is formed by more than one attacker node, where these attacker nodes build a tunnel between them and hide the presence of other intermediate nodes in between them. Thus, they advertise false hop-count and get intrude in the routing path.
- *Sybil attack:* The attacker node impersonates the identity of the legal nodes and gets included in the routing path.

5.2. Countermeasures Against Routing Attacks by TOHIP

The existing algorithm TOHIP has provided solution for the above-mentioned routing attacks. Due to its topology hiding factor, the identity of the legal nodes is not exposed to the attacker nodes and thus they can avoid a Sybil attack. The intermediate nodes are not allowed to send RREP messages in TOHIP and so black-hole attack is avoided. TOHIP uses hop count to resist rushing attack and so the path with smaller number of hop counts is chosen as routing path. Similarly, to overcome the worm-hole attack it uses round-trip time and fake hop-count is not taken into account during path discovery.

5.3. Issues in TOHIP

The rushing attack is one of the serious DoS attacks. According to TOHIP, the path is chosen based on the hop-count and it does not depend on the Round-Trip Time (RTT) between the source and destination. The rushing attack is likely to happen if the path chosen has an RTT between the source and destination much smaller than normal RTT. TOHIP cannot guarantee that the path formed with smaller hop-count will definitely overcome rushing attack and so there is a possibility of the rushing attack to occur in the path with a shorter hop count. Also, obtaining public and private key from a centralized trusted server in MANET is not feasible or reliable.

5.4. Counter Measures Against Routing Attacks by SLLDMR

The SLLDMR is an extension of ELLDMR. The forwarding nodes of SLLDMR also maintain only next and previous hop information in the routing table and thus they hide topology information in the intermediate nodes. SLLDMR also does not allow intermediate nodes to send an RREP message and so the SLLDMR also prevents worm-hole attack, black-hole and Sybil attack similar to TOHIP. The proposed algorithm, SLLDMR, provides a better solution to overcome the rushing attack.

5.5. Rushing Attack Prevention in SLLDMR

In SLLDMR the end to end delay of the RREQ packet from the sender node to the receiver node is the RREQ broadcast delay of the sender node. It is defined as the summation of all other delays the packet encounters from the time it is transmitted from the sender till it reaches the destination. The RREQ broadcast delay (TOT) is given as:

$$\begin{aligned} TOT = {} & transmisson\ delay\left(T_t\right) \\ & + propagation\ delay\left(T_{pp}\right) \\ & + processing\ delay\left(T_p\right) \\ & + queuing\ delay\left(T_q\right) \end{aligned} \tag{5}$$

In Figure 4, the TOTA and TOTB are the RREQ broadcast delay of the normal node (A) and rushing attacker node (M). It shows the RREQ broadcast delay of rushing attacker node (M) is less than a normal node (A). The attacker node (M) has a negligible processing delay and queuing delay compared to node (A). Therefore, in order to overcome the rushing attack, the SLLDMR compares broadcast delay of the RREQ of each intermediate node with an Estimated Broadcast Time (ERBT). If the RREQ broadcast delay of the intermediate node is less than ERBT, the RREQ is rejected, otherwise it is accepted. The ERBT is computed as given in equation 6.

$$ERBT = T_{t(RREQ)} + T_{pp(RREQ)} + T_{q(RREQ)} + T_{p(RREQ)} \quad (6)$$

where $T_{t\,(RREQ)}$, $T_{pp\,(RREQ)}$, $T_{q\,(RREQ)}$, $T_{p\,(RREQ)}$ are the transmission, propagation, queuing and processing time of RREQ packet which is determined as follows:

- $T_{t\,(RREQ)} = N/R$, where N is the number of bits, and R is the rate of transmission (bits/second)
- $T_{pp\,(RREQ)} = d/s$, where d is the distance between sender and receiver and s is the speed of light for wireless transmission
- $T_{q\,(RREQ)} = 1/(\mu - \lambda)$, where μ is the number of packets that can sustain per second and λ is the average rate at which packets are arriving to be serviced.
- $T_{p\,(RREQ)}$ is the time it takes to process the packet header.

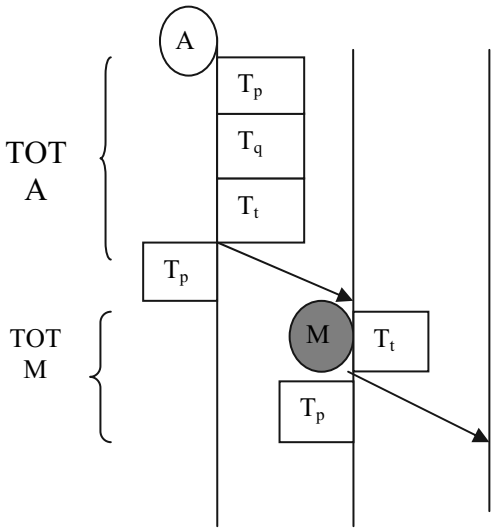

Figure 4. Comparison of RREQ end-to-end delay between a normal node (A) and rushing attack node (M).

The ERBT value is calculated based on the past history value. The intermediate node records the RREQ receiving time on the packet before broadcasting it to the next intermediate node. The difference in receiving time of the intermediate nodes gives the RREQ broadcast delay. As the rushing attacker immediately forwards the RREQ packet to the intermediate node without any processing and queuing delay, it easily gets included in the routing path. So if the broadcast delay of the RREQ is less than ERBT (Equation 5), the RREQ packet is not accepted by the intermediate node, otherwise it is accepted. In this way, the RREQ packet from the rushing attacker node is avoided and thus the occurrence of the rushing attack is prevented in SLLDMR.

5.6. Secured Packet Transmission in SLLDMR

In the enhanced TOHIP, the nodes are dependent on the centralized trusted server for their public and private key certificates and so it is not highly reliable and secure. The SLLDMR is the extension of ELLDMR, where each node can generate its own public and private key certificate. Therefore, the nodes of SLLDMR employ the self-organized public key [19] technique to generate the private and public keys. In this algorithm, only the source and destination nodes are involved in the encryption and decryption process. Thus, the SLLDMR exhibits less routing packet overhead and end to end delay compared with enhanced TOHIP. Whenever the source node wants to communicate with the destination node, both the source and destination nodes generate their own public key (PU) and private key (PR) pair before finding a path between them. The destination node transmits its public key (PUD) along with LREP to the sender node during the location discovery phase. The source node, before transmitting its data packet (M) to the destination node, encrypts it with two level encryption process. This ensures reliable and secure delivery of the data packet (M).

5.6.1. Two Level Encryption and Decryption Process

Encryption process at the source node

The data packet (M) is encrypted twice at the source node before transmission. The procedure and block diagram of two-level encryption processes at the source node are shown in Figure 5 and Figure 6.

Step 1: Encrypt (PR_S (M,S.id, D.id) = $E_1(P_1)$
Step 2: Encrypt (PU_D (E_1 (P_1), PU_S) = $E_2(P_2)$
Step 3: Source node sends the packet P = (E_2 (P_2).M) to the next forwarding node

Figure 5. Procedure for two-level encryption processes at the source node.

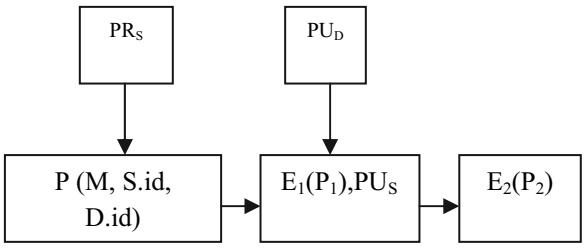

Figure 6. Block diagram showing two-level encryption processes at the source node.

During the first level of encryption, the data packet (M), source and destination identifier (S.id, D.id) are encrypted with the private key of the source node (PRs). During the second level of encryption, the encrypted data E1 (P1) and the source public key (PUS) are encrypted with the public key of the destination node (PUD). After the second encryption, the source node transmits the packet P which includes the encrypted data (E2 (P2)) and the original data packet (M) to its next forwarding node in the routing table.

Decryption process at the destination node

After receiving this data, the forwarding node upon receiving this packet (P) forwards it to its next forwarding node in its routing table until it reaches the destination node. The procedure and block diagram of two-level decryption processes at the destination node are shown in Figure 7 and Figure 8.

Step 1: Decrypt $PR_D(E_2(P_2))$ = (($E_1(P_1)$, PU_S))
Step 2: Decrypt PU_S (($E_1(P_1)$)=(M, S.id, D.id)
Step 3: Destination checks for source and destination identity.
Step 4: The resultant data (M) are compared with the original data (M)

Figure 7. The procedure shows two-level decryption process at the destination node.

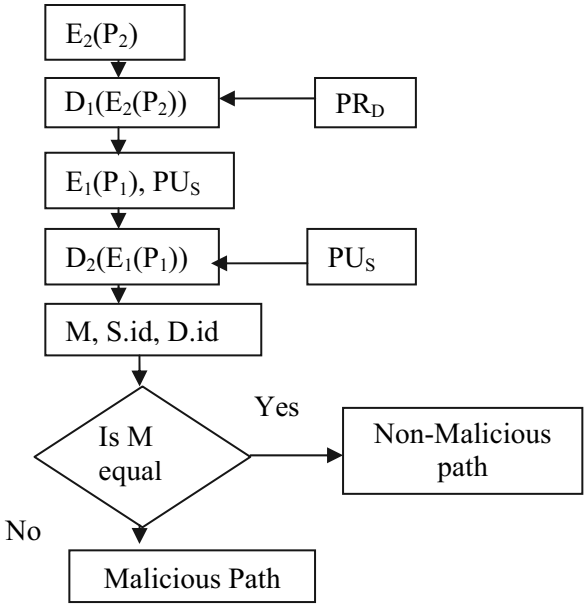

Figure 8. Block diagram showing two-level decryption process at the destination node.

The destination node, during its first level of decryption, decrypts the encrypted data (E2(P2)) with its private key and obtains the encrypted data (E1(P1)) and source public key (PUS). During the second level of decryption, destination node decrypts the encrypted data (E1(P1)) with the public key of the source node (PUS) and obtains the decrypted original data (M). Before accepting this data, it is checked with the original data (M). If both the data are same, the data is accepted, otherwise the destination node sends the notification to the source node for the change of alternate path because of the existing malicious path.

6. Performance Evaluation of ELLDMR and SLLDMR

6.1. Network Simulator NS2

NS2 network simulator is one of the best existing network simulators for evaluating the network performance of wired and wireless networks. It is a free open source discrete event simulator and can be installed easily regardless of any operating system. Nowadays, it is widely accepted in the industry and supports the simulation of Mobile Ad Hoc Networks (MANET). In the literature, most of the research work on MANET routing protocols and network functions and protocols are simulated and evaluated using NS2. Due to its flexibility and modular nature, NS2 has gained popularity in the networking research community.

6.2. Network Topology

The following network topology assumptions are used in the simulation setup of the proposed algorithms.

- Since the proposed algorithms are location-based, the GPS receiver is enabled in all the nodes. The current (x, y) position of the nodes and their node velocity are provided by these GPS receivers.
- In the simulation environment, the nodes are homogeneous where they are equipped with IEEE 802.11 transceivers with a maximum of 250 m transmission range.
- The proposed algorithm ELLDMR and SLLDMR are implemented using the NS2 simulator and topology parameters are specified in Table 3.

6.3. Result and Analysis

6.3.1. Performance Analysis of ELLDMR in the Non-adversarial Scenario

Routing Packet Overhead (RPO). In Figure 9, the average RPO of ELLDMR is compared with TOHIP and LLDMR for the different number of nodes at node velocity of 25 m/s.

Table 3. Simulation parameter.

Parameter	Values
Simulation area	1000 m × 1000 m
Number of mobile nodes	300
Simulation time	800 s
Pause time	30 s
Number of source-destination pairs	10
Packet generation rate	1 packet/s
Packet size	512 bytes
Node velocity	0, 5, 10, 15, 20, 25, 30, 35, 40 m/s
Number of attacker nodes	0 ,5,10,15,25

Figure 9 shows that in ELLDMR, there is a 9% increase in RPO compared to LLDMR for 50 nodes. It is because, unlike LLDMR, the RREP packet from the intermediate nodes is not accepted in ELLDMR. This reduces the usage of the available path from the intermediate nodes and so increases the RREQ broadcast till the destination. But the analysis shows that for an increase of 300 nodes, the RPO of ELLDMR decreases by 5% and 1.7% than TOHIP and LLDMR. It is because, in LLDMR and TOHIP, the RREQ packet is broadcasted to all the neighbour nodes and so it increases the RPO in these protocols with an increase in the number of dynamic nodes. But in ELLDMR, the RREQ is broadcasted only to the non-critical neighbour nodes. Therefore, even though the overall RPO grows with an increase in the number of

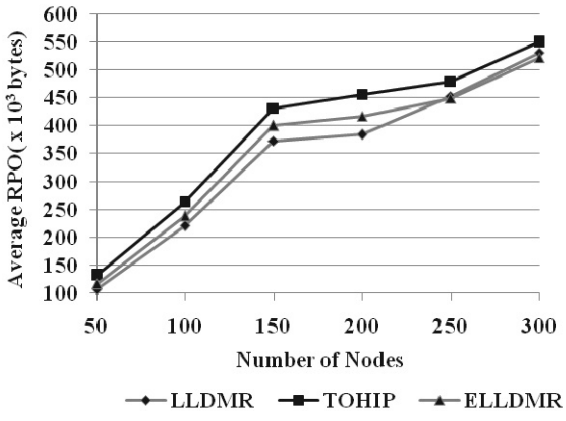

Figure 9. Number of nodes *vs*. average RPO at 25 m/s.

nodes in ELLDMR, it is comparatively lesser than LLDMR and TOHIP.

End to End delay (E2E). The comparison analysis of the average end to end delay of ELLDMR with TOHIP and LLDMR for different node velocities is shown in Figure 10. In this analysis, the MANET with 200 nodes is considered. The analysis interprets that at zero node velocity the end to end delay in ELLDMR is 3% longer than LLDMR and 3% shorter than TOHIP. But as the node velocity increases to 40 m/s, the end to end delay of ELLDMR is 9% and 13% shorter than LLDMR and ELLDMR respectively.

This is because, as said already, the ELLDMR does not accept the routing path from intermediate nodes, it takes longer E2E delay in finding the path than LLDMR during static network. But, as the node velocity increases, the link failure also increases in the MANET. As the ELLDMR uses only the non-critical nodes for building the routing path, the link lifetime of its routing link is considerably increased. So, the link breakage is less frequent in ELLDMR than in LLDMR and TOHIP. In multipath routing protocols, the frequent link failure causes switching of packet transmission between the available paths and may also sometime lead to the rediscovery of routing path which finally results in longer end to end delay during packet transmission. Therefore, at higher node velocity, the ELLDMR shows lesser end to end delay than LLDMR and TOHIP.

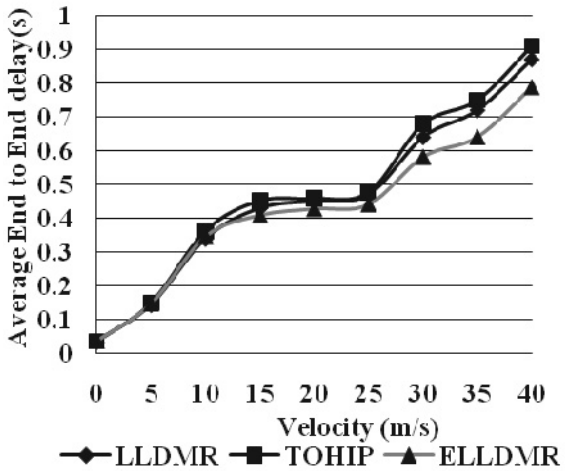

Figure 10. Node velocity *vs*. average end to end delay for 200 nodes.

Figure 11 shows the comparison of an end to end delay between LLDMR and ELLDMR for sparse network and dense network. The ELLDMR performs better in the dense network than in the sparse network. The ELLDMR takes more time for route discovery phase at the sparse network because, due to the lesser number of nodes in the network, the availability of non-critical nodes is less and so it has to include critical nodes in the routing path to avoid void [18] situation. But in the dense network, the availability of non-critical nodes is greater and so it takes less time to build the routing path in ELLDMR than LLDMR.

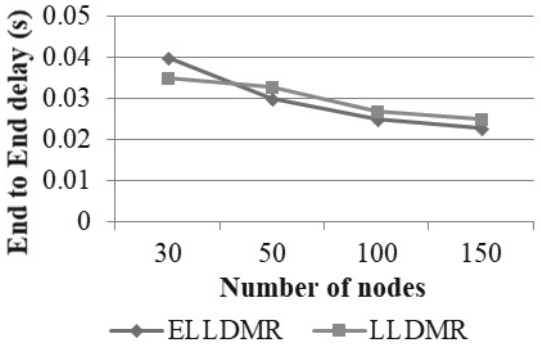

Figure 11. The number of nodes *vs*. end to end delay at 25 m/s.

Packet Delivery Ratio (PDR). In Figure 12, the PDR of ELLDMR is compared with TOHIP and LLDMR for different node velocities for a total of 200 nodes in the network.

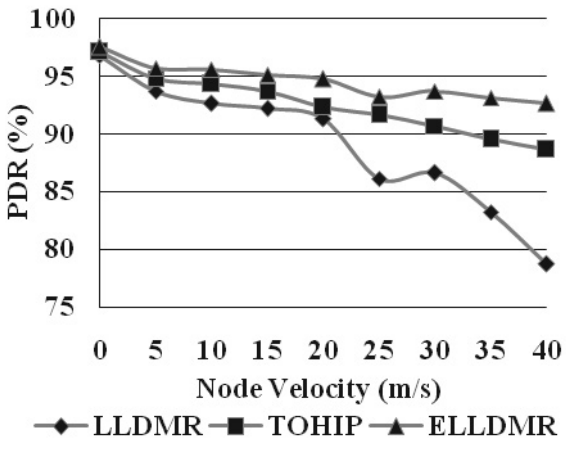

Figure 12. Node velocity *vs*. PDR for 200 nodes.

At zero node velocity, the ELLDMR, LLDMR, and TOHIP do not show much variation in PDR. But for 20 m/s node velocity, the PDR of ELLDMR increases by 2.6% and 3.8% compared to TOHIP and LLDMR and for 40 m/s, there is 4.5% and 17.7% increase in PDR respectively. This is because, as the node velocity increases, there is more link failures in MANET. The main objective of ELLDMR is to increase the link lifetime of the routing path by building the route with non-critical nodes. This reduces the frequent link failure in ELLDMR and therefore, the packet loss due to frequent link failures is reduced considerably in ELLDMR. This improves the PDR of ELLDMR when compared with the existing protocols LLDMR and TOHIP.

6.3.2. Performance Analysis of ELLDMR and SLLDMR Under Non-adversarial and Adversarial Scenario

The SLLDMR is the security protocol and is an extension of ELLDMR. Its performance is compared with unsecured protocols LLDMR and ELLDMR and with secured protocol TOHIP. In this simulation, the network of 200 nodes and 25 m/s node velocity is considered.

Routing overhead. The comparison of average RPO between SLLDMR, ELLDMR, LLDMR, and TOHIP is shown in Figure 13. In the analysis between SLLDMR, ELLDMR, and LLDMR, for zero attacker nodes, SLLDMR gives more RPO because it incorporates two level cryptographic techniques during RREQ broadcast. But as the number of attacker nodes increases during packet transmission, due to its enhanced security features, the effect of the attacker node is less in SLLDMR than in ELLDMR and LLDMR. Also, the chance of rediscovery of the route is less in SLLDMR and so, for 25 attacker nodes, the RPO of SLLDMR decreases by 5% and 13% compared to ELLDMR and LLMDR respectively.

In the comparison of RPO between the SLLDMR and TOHIP, the RPO of SLLDMR is 2% and 8% lesser than that of TOHIP for 5 and 25 attacker nodes respectively. It is because TOHIP generates public and private keys through the centralized trusted server where it involves more routing overhead for transferring the keys, but the SLLDMR incorporates self-organized public key management where nodes manage their own public key and private key. Therefore, the RPO of SLLDMR is comparatively less than that of TOHIP.

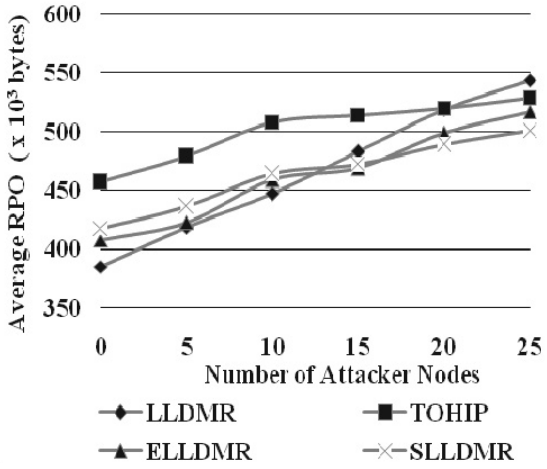

Figure 13. Number of attacker nodes *vs*. average RPO.

End to End delay. Figure 14 shows the comparison of Average E2E delay between SLLDMR, ELLDMR, LLDMR, and TOHIP. The SLLDMR and TOHIP depict similar performance for lesser attacker nodes but as the number of attacker nodes increases, the E2E of the SLLDMR decreases by 7%. It is because, as said earlier, the SLLDMR incorporates self-organized public key management technique and

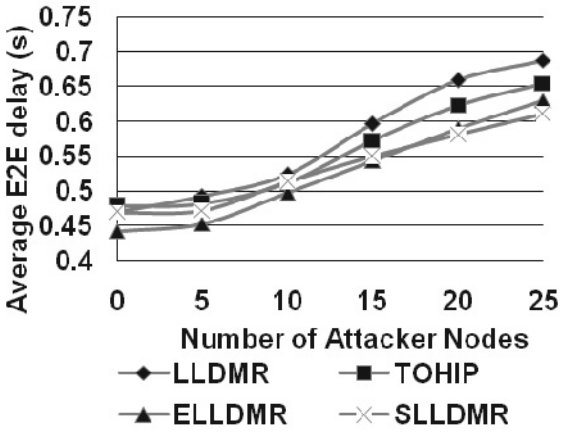

Figure 14. No. of attacker nodes *vs*. end to end delay.

also encryption and decryption are done only at the source and destination nodes. This reduces some considerable amount of time during route discovery in SLLDMR *vs*. TOHIP. Similarly, when SLLDMR is compared with LLDMR and ELLDMR, the analysis shows that the E2E of SLLDMR is overall better than the other two for the increase in the number of attacker nodes. Normally the SLLDMR takes some period of time for processing the two-level cryptographic technique. Therefore, for zero attacker nodes, it shows more E2E delay than LLDMR and ELLDMR do, but as the number of attacker nodes increases, the security in SLLDMR during packet transmission compromises the performance of LLDMR and ELLDMR. Moreover, the SLLDMR protects the forwarding nodes from rushing attack during route discovery. Therefore, the retransmission of packets due to link failure and packet loss is comparatively less in SLLDMR and so for higher attacker nodes, it shows better performance than LLDMR and ELLDMR do.

Packet Delivery Ratio (PDR). Figure 15 shows the comparison of PDR between SLLDMR, ELLDMR, LLDMR, and TOHIP. Since all these protocols are multipath routing protocols, for non-adversarial scenario i.e. for zero attacker nodes all of them give nearly 95% packet delivery. But as the number of attacker nodes increases, the ELLDMR and TOHIP perform better than LLDMR and TOHIP. It is because in these protocols, the intermediate nodes are not aware of the routing path and so they avoid network attacks like black-hole and worm-hole attacks. Also, both of them exhibit

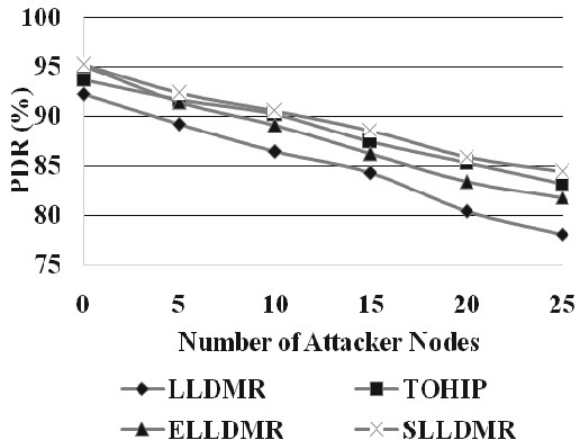

Figure 15. No. of attacker nodes *vs*. PDR.

encryption technique for packet transmission and so the PDR of SLLDMR increases by 3% and 8% compared with ELLDMR and LLDMR for 25 attacker nodes. In comparison between the SLLDMR and TOHIP, frequent link failures are less in SLLDMR and so the packet loss due to link failure is less in ELLDMR than SLLDMR. Therefore, the overall analysis depicts that the SLLDMR gives better PDR than LLDMR, ELLDMR, and TOHIP.

7. Conclusion

The major contribution of this work is to reduce the routing overhead and provide security against several routing attacks in MANET. The ELLDMR and SLLDMR hide routing information in the intermediate nodes and so they are secure against the black hole, worm hole, and Sybil attacks. Since ELLDMR uses only non-critical nodes for finding the routing path, it minimizes frequent link failure during packet transmission. The data security is very much essential in MANET as its major applications are in wireless sensor networks, data networks, tactical networks, etc. The SLLDMR uses two-level encryption and decryption processes for secure packet transmission. As it does not involve any centralized trusted server for public or private key generation, it is cost effective and reliable. The extensive simulation results show that the ELLDMR and SLLDMR have better network performance than other existing multipath routing protocols.

The limitation of the proposed algorithm is that it considers only node movement as the major cause for link failure during transmission of the packet. Since the MANETs are a network of mobile nodes, another important reason for the link failure in such a network is the node's energy dissipation. Due to limited energy and resource constraint in these nodes, its energy gets easily drained and makes the node dead. In the proposed algorithms, ELLDMR and SLLDMR have not addressed the link failure problem due to energy loss in the nodes. The future work is to select the non-critical nodes with more energy as the forwarding node while finding the node-disjoint multipath in MANET.

References

[1] S. Ali *et al*., "An Overview of Mobile Ad Hoc Networks for the Existing Protocols and Applications", *Int. J. on Applications of Graph Theory in Wireless Ad Hoc Networks and Sensor Networks (Graph-Hoc)*, vol. 2, no.1, 2010. http://dx.doi.org/10.5121/jgraphhoc.2010.2107

[2] Aboli Arun and Rachana Anil, "A Survey on Various Multipath Routing Protocols in Wireless Sensor Networks", in *Proc. of International Conference on Communication, Computing and Virtualization (ICCCV'16)*, vol. 79, pp. 610–615, 2016. http://dx.doi.org/10.1016/j.procs.2016.03.077

[3] B. Zhu *et al*., "Anonymous Secure Routing in Mobile Ad-Hoc Networks", in *Proc. of the 29th Annual IEEE Int. Conference on Local Computer Networks*, 2004, pp. 102–108. http://dx.doi.org/10.1109/LCN.2004.21

[4] V. Muthupriya and K. M. Mehata, "Review on Network Layer Attacks and Countermeasures in MANET", *Int. J. of Analog Integrated Circuits*, vol. 2, no. 1, 2016.

[5] B. Dahill *et al*., "ARAN: A secure Routing Protocol for Ad Hoc Networks", UMass Tech Report, pp. 02–32, 2002. http://dx.doi.org/10.1109/ICNP.2002.1181388

[6] P. Papadimitratos *et al*., "The Secure Routing Protocol (SRP) for Ad Hoc Networks", draft papadimitratos-secure-routing-protocol-00.txt, Dec. 2002. https://tools.ietf.org/html/draft-papadimitratos-secure-routing-protocol-00

[7] Y.-C. Hu *et al*., "Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks", in *Proc. of 8th ACM Int'l. Conf. Mobile Computing & Networking (Mobicom'02)*, 2002, Atlanta, Georgia, pp. 12–23. http://dx.doi.org/10.1007/s11276-004-4744-y

[8] J. Kong *et al*., "ANODR: Anonymous on Demand Routing Protocol with Untraceable Routes for Mobile Ad-Hoc Networks", *Proc. ACM MobiHoc*, 2003, pp. 291–302. https://www.sigmobile.org/mobihoc/2003/papers/p291-kong.pdf

[9] Ehsan Bagherian and Siavash Khorsandi, "ARMAN: A new Anonymous Routing Protocol for Mobile Ad-Hoc Networks", *IEEE*, 2009. http://www.academia.edu/680369/ARMAN_A_new_Anonymous_Routing_Protocol_for_Mobile_Ad-Hoc_Networks

[10] L. Zhao and H. Shen, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs", *IEEE transactions on mobile computing*, vol. 12, no. 6, 2013. http://ieeexplore.ieee.org/abstract/document/6175018/

[11] Y. Zhang *et al*., "TOHIP:A Topology-hiding Multipath Routing Protocol in Mobile Ad Hoc Networks", *Ad Hoc Networks*, vol. 21, pp. 109–122, 2014. http://dx.doi.org/10.1016/j.adhoc.2014.05.012

[12] M. G. Zapata, "Secure Ad-hoc On-demand Distance Vector (SAODV) Routing", *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 6, no. 3, 2002. http://dx.doi.org/10.1145/581291.581312

[13] P. Papadimitratos *et al*., "The Secure Routing Protocol (SRP) for Ad Hoc Networks", draft papadimitratos-secure-routing-protocol-00.txt, Dec. 2002.

[14] S. Yi *et al*., "Security Aware Routing Protocol", in *Proc. of IEEE Int. Conference on Network Security*, 2001. http://dx.doi.org/10.1145/501449.501464

[15] R. Mavropodi *et al*., "SecMR – a Secure Multipath Routing Protocol for Ad Hoc Network", *Ad Hoc Networks*, vol. 5, no. 1, pp. 87–99, 2007. http://dx.doi.org/10.1016/j.adhoc.2006.05.020

[16] V. Muthupriya and S. Revathi, "Location-aided Level-based Node Disjoint Multipath Routing(LLDMR) for Mobile Ad Hoc Networks", *Journal of Theoretical and Applied Information Technology*, vol. 95, no. 23, pp. 6608–6623, 2017. http://www.jatit.org/volumes/Vol95No23/22Vol95No23.pdf

[17] Y. Ko and N. H. Vaidya, "Location-aid Routing (LAR) in Mobile Ad Hoc Networks," *Wireless Networks*, vol. 6, pp. 307–321, 2000. http://dx.doi.org/10.1023/A:1019106118419

[18] B. Karp and H. T. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks", in *Proc. of Int. Conference on Mobile Computing & Networking (Mobicom'00)*, 2000, pp. 243–254. http://dx.doi.org/10.1145/345910.345953

[19] S. Capkun *et al*., "Self-organized Public-key Management for Mobile Ad Hoc Networks", *IEEE Trans. Mobile Comput*, vol. 2, no. 1, pp. 52–64, 2003. https://ieeexplore.ieee.org/document/1195151/

Received: June 2018
Revised: December 2018
Accepted: January 2019

Contact addresses:
Vasudevan Muthupriya
BS Abdur Rahman Crescent
Institute of Science and Technology
Chennai
India
e-mail: muthupriya@crescent.education

Sathyanarayanan Revathi
BS Abdur Rahman Crescent
Institute of Science and Technology
Chennai
India
e-mail: srevathi@crescent.education

VASUDEVAN MUTHUPRIYA was born in Chennai, India in 1978. She received her B.E. degree in Computer Science Engineering (CSE) from Madras University, India in 1999 and her M.E (CSE) from Madras University, India in 2003. She joined as a Lecturer the Dr. M.G.R Engineering College in 1999 and continued till May 2003. Later she joined as a Lecturer the BSA Crescent Engineering College in 2003 and became an Assistant Professor in the same institution. She has 19 years of teaching experience and her areas of interest are computer networks, wireless mobile ad hoc networks and cryptography and network security. She is currently pursuing her Ph.D. in mobile ad hoc networks in the same institution. She is a life member of the Indian Society for Technical Education (ISTE), the System Society of India.

SATHYANARAYANAN REVATHI was born in Chennai, India, in 1973. She received the B.E degree in Computer Science and Engineering (CSE) from IRTT, Erode, India in 1994, and the M.E (CSE) from MEPCO Schlenk, India in 2000. She completed her Ph.D (CSE) at Anna University in 2014. She joined, as a lecturer, the CSE department of the Engineering College in 1996. Later, she continued her service as Assistant Professor of CSE in BSA at Crescent Engineering College from 2002. Then, she became Associate Professor at the same institution in 2008. She has published a good number of papers in the international journals and conferences. She is supervising six PhD scholars, and her research areas include Internet of Things and mobile ad-hoc networks. She is an active life member of ACM and ISTE.