Cross-layered-based adaptive secured routing and data transmission in MANET

Jai Kumar Vinayagam*

JNTUA,
Ananthapuramu, A.P., India
Email: jaikumarvphd@gmail.com
*Corresponding author

C.H. Balaswamy

Department of Electronics and Communication Engineering,
Gudlavalleru Engineering College,
Gudlavalleru, A.P., India
Email: Ch.balaswamy7@gmail.com

K. Soundararajan

Department of Electronics and Communication Engineering,
T.K.R. Engineering College,
Hyderabad, India
Email: Soundararajan_jntucea@yahoo.com

Abstract: Mobile ad hoc network (MANET) is a self-organising network consisting of a group of nodes connected to each other wirelessly. Due to the self sustaining nature of MANET, it has been used in various applications and provides good communication. However, because of certain features of MANET such as wireless medium, highly dynamic topology, limited resources, etc., the network is easily prone to various attacks which hamper the communication efficiency. The nodes are attacked mainly during the routing process and the data packets are dropped or its authenticity is compromised mostly during the data transmission process. Hence, it is critical to ensure that routing and data transmission process is performed in a secure manner to ensure security of the network. In this paper, we propose to develop a cross-layered-based adaptive secured routing and data transmission technique in MANET. Initially, the multipath routing is performed securely by encrypting every message transmission, to guarantee routing security. Then the highly secured data is transmitted through secure routes to ensure data security. Then the network is examined for intrusions. In this way, network is safeguarded from attacks and hence enhancing network operations.

Keywords: mobile ad hoc network; MANET; cross-layer; adaptive; routing; data; security.

Reference to this paper should be made as follows: Vinayagam, J.K., Balaswamy, C.H. and Soundararajan, K. (2019) 'Cross-layered-based adaptive secured routing and data transmission in MANET', *Int. J. Mobile Network Design and Innovation*, Vol. 9, No. 1, pp.37–45.

Biographical notes: Jai Kumar Vinayagam at present working as an Associate Professor in ECE Department, QIS College of Engineering and Technology, Ongole. He received his Bachelor's degree in Electronics and Communication Engineering from the SSN Engineering College and MTech in Communications and Signal Processing from the Bapatla Engineering College. At present, he is pursuing his PhD from the JNTU Ananthapuramu. He has 12 years of teaching experience. His research interests include mobile wireless networks and communications such as ad hoc networks, and sensor networks.

C.H. Balaswamy is a Professor at the Department of Electronics and Communication Engineering, Gudlavalleru Engineering College, Gudlavalleru, A.P., India.

K. Soundararajan is a Professor and Dean R&D at the Department of Electronics and Communication Engineering, T.K.R. Engineering College, Hyderabad, India.

1 Introduction

1.1 Mobile ad hoc network

Mobile ad hoc networks (MANETs) are made up of a collection of mobile nodes which are linked to one another to form a connected network. In MANET, each node may enter as well as exit the network at any instant of time. MANET does not have a centralised controlling node and hence each node in the network functions as a router in order to route the data packets throughout the network. Routing is basically a process of determining the best path or route from the source to the destination. In MANET, each node participates in data packet forwarding process to enable successful communication in the network. Due to certain features of MANET like wireless connection, distributed network infrastructure, highly dynamic network topology, limited network resources, etc.; it has become susceptible to many attacks (Aluvala et al., 2016).

MANET is a self sustaining network, without any fixed network infrastructure. The nodes in this network communicate with one another by single hop connection or by multihop data transmission. However, the current routing protocols used in MANET are prone to network attacks. The security issues faced in MANET are very high when compared with the security issues faced by the conventional wireless networks. The security issue in routing is mainly due to the absence of the centralised controlling entity, which is critical in distribution of secret keys among the nodes involved in communication. Also, the nodes can be easily compromised due to the absence of fixed infrastructure, which in turn compromises the important network features like network integrity, mode privacy, and validity, when compared with the traditional wireless networks. Finally, the dynamic topology of MANET also makes security management a difficult process (Saha et al., 2012).

However, the advantages of MANET are higher than that of the conventional wireless networks. Some of the advantages are:

1 ease in building and dismantling the network

2 inexpensive communication in locations where building wired network is very difficult

3 can be set up quickly in emergency conditions (Alnumay and Ghosh, 2014).

1.2 Cross-layer-based secure routing and data transmission

In MANET, the conventional routing protocols do not perform well and the overall MANET performance is dependent on the type of routing mechanism employed in the network. In MANET, designing a routing protocol is very challenging task. Till date several types of routing protocols have been developed such as proactive routing protocol, reactive routing protocol, hybrid routing protocol, etc. (Saha et al., 2012). In critical applications, data packets should be forwarded securely and hence secure routing becomes very important. Attacks on node which are mobile is comparatively an easy task. Also, cooperative operation between nodes that are mobile is a hard process. So, it is important to design an efficient routing scheme which is secure enough to safeguard all the nodes from unnecessary risks. In the current mechanisms, the routing protocol introduces routing overhead and is very susceptible. All the nodes in network need to be observed regularly in order to detect any malicious behaviour and the detected node must be prohibited from routing the data packets (Kaliappan and Paramasivan, 2014).

In order to handle the security issue in MANET, the security needs of each function has to be analysed.

1 Authentication: to validate each node's identity and to check if it is qualified to access the network, authentication is critical.

2 Authorisation and access control: every node needs to be capable of accessing the shared resources, services as well as the personal details available in MANET, along with this each node should have the ability to refrain other nodes from getting access to its private data.

3 Privacy and confidentiality: the information transmitted between two nodes must be maintained securely by the nodes involved in communication. The location details of the nodes and also the data recorded in the nodes must be handled securely.

4 Availability and survivability: even during malicious attacks or in the existence of some issues in the network, all the network services as well as the applications should be available for access.

5 Data integrity: the intended destination is supposed to receive the data sent to it without getting manipulated by unwanted entities.

6 Non-repudiation: every node must perform its functionalities of transmitting and receiving promptly, in order to overcome any misbehaviour in the network (Aldabbas et al., 2012).

In MANET, authentication is necessary for a node to perform data transmission and reception in a secure manner and also to overcome the security risks. But in MANET, developing a secure link is a difficult due to some specific reasons like:

1 sharing of the wireless link

2 absence of proper line of defence

3 self-sustaining and dynamic topology

4 message being broadcasted

5 multihop movement of the messages

6 limited battery power and complicated calculations (Alnumay and Ghosh, 2014).

2 Related works

Aluvala et al. (2016) have proposed a new mechanism to authenticate node when a new node joins the network and prior starting the route discovery process in MANET. In this mechanism, two-step authentication process is followed: First, the transmitting node determines the ones compliment of its IP address and appends it on the RREQ message. Then the signature of the source node on the destination IP address with public key is included in the RREQ message. On receiving the message, the node verifies the source's authentication by summing the appended ones complement in the message to the IP address of the source. If the sum is all ones, then the source is considered to be authenticated. However it is not possible to decrypt the encrypted text. The unauthorised nodes are detected when it fails to append ones compliment of its IP address. After detection of unauthorised nodes, its neighbours drop the packets forwarded by it and a warning message is broadcasted in the network which contains the information of malicious node such as its IP address.

Singh et al. (2016) have presented a protocol referred as 'administrator and fidelity-based secure routing protocol' (AFSR). This protocol guarantees secure routing in MANET. Initially, based on the willingness and fidelity, an administrator node is selected. Then all the nodes in the network, communicates directly to this centralised node. In this several security issues are controlled in the network.

Rajkumar and Narsimha (2016) have proposed a certificate authority (CA) distribution and a trust-based threshold revocation technique for MANET. On the basis of the direct as well as indirect trust values, the overall trust value is estimated and then the secret key is provided to every node in the network by the certificate authority. A threshold revocation technique is developed on the basis of the trust value. This proposed technique successfully overcomes the node misbehaving issues.

Kaliappan and Paramasivan (2014) have proposed a protocol to improve the routing security in MANET by utilising the dynamic Bayesian signalling game model (SRPDBG). The proposed protocol monitors and examines the strategy profile and behaviour of the regular as well as the malicious nodes in the network. This proposed technique determines the best outcome of every strategy in every node.

Athreya and Tague (2011) have proposed the cross-layer scheme to utilise the measured RSSI value in the physical layer to specify the node neighbourhood, then the measured ETX value from the link layer as well as the node forwarding behaviour from network layer to analyse the path reliability criteria through a utility function. These three factors have been utilised as the fundamental parameters to develop a reliable as well as safe multipath routing in MANET. Experiments have been made on the proposed technique in order to examine the outcome of the conventional security attacks. However, the proposed technique has not considered the factors like packet loss, load, throughput, etc.

Iqbal et al. (2016) have presented an adaptive and cross-layer multipath routing protocol for handling the temporary issues. The application type is considered by the proposed protocol before performing the routing operation. In case of simple applications, the proposed protocol uses the technique followed by the conventional routing protocols of determining the shortest path between the source and destination node. When multimedia applications are present, the protocol selects routes with higher bandwidth and lower packet loss ratio. For security-based applications, highly secure routes are chosen. For good decision making at the network layer, cross layer technique is followed for parameter exchanging purpose.

Dhurandher et al. (2011) have proposed an algorithm referred as friend-based ad hoc routing using challenges to establish security (FACES) to estimate the trust of nodes in MANET. This is achieved by sending challenges as well as by sharing friends listing real life scenarios. All the nodes present in the friend list are considered based on the successful data transmission performed and also continuation of friendship with all the other nodes which are befriended by the proposed technique in a regular manner. In this technique, every node maintains separate friend list.

Sánchez-Casado et al. (2012) have presented an intrusion detection system for detecting malicious dropping of packets in MANET. This is performed by gathering factor's detail from the MAC and network layers. This proposed technique follows a model to determine the packet dropping attacks in various network situations which is different compared to the conventional attack detection technique. The method used to detect attack is very simple and hence eliminates the computational overhead. However, effects of route change are not included in the proposed technique.

3 Cross-layered-based adaptive secured routing and data transmission technique

3.1 Overview

In this proposal, we design a cross-layer-based secure multipath routing and data transmission protocol. In this protocol, the application layer specifies the type of security as:

1 IDS

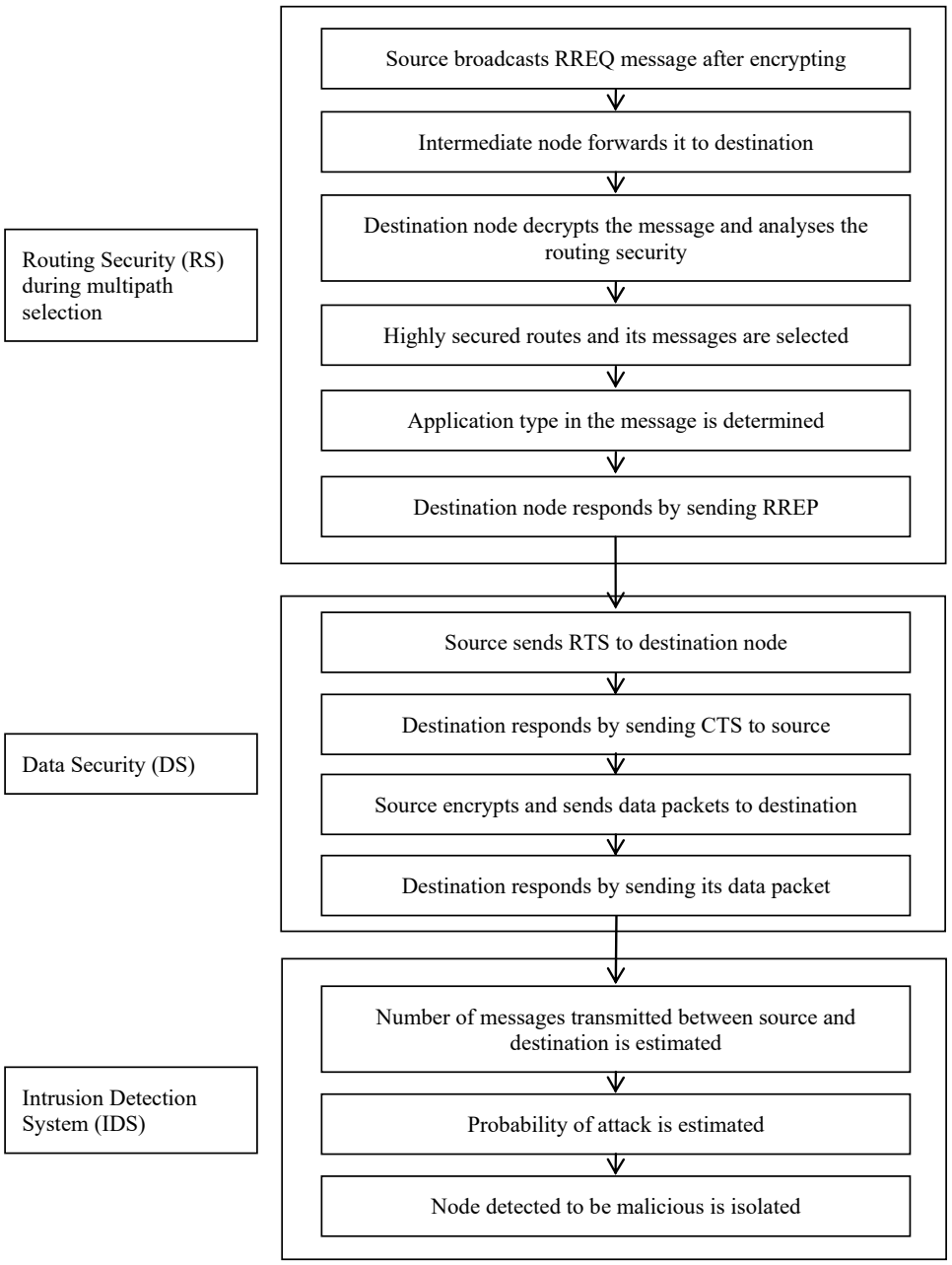
2 routing security (RS)

3 data security (DS)

4 IDS + RS + DS.

The proposed protocol adaptively selects two or more routes depending on the type of security. The basic multipath route discovery process is similar to Iqbal et al. (2016). In case of IDS, an efficient packet dropping attack is implemented in which the RTS, CTS and RREQ counts are checked as per the packet dropping detection algorithm (Sánchez-Casado et al., 2012). The information about RTS and CTS counts are passed from the MAC layer to the network layer.

Figure 1 Block diagram



In case of RS, when a source wants to send a RREQ packet, it sends a hash value and also encrypts it using the shared symmetric key with the destination. The intermediate nodes on receiving these packets encrypt the hash and append their ID with id encrypted payload of previous node and encrypt this whole message with the shared symmetric key. On receiving this message, the destination decrypts the packet in the reverse order of the ID's recorded in clear text and verifies the hash sent by S (Athreya and Tague, 2011). If they all match, then it can be concluded that the source is an authenticated one and the intermediate nodes have not altered the routing packets. In a similar manner, DS is ensured. In case of IDS + RS + DS, all the above three phases will be implemented concurrently.

3.2 RS technique during multipath selection

When a node wants to communicate with another node by sending data packets, then a path from the transmitting node, i.e., source node to the receiving node, i.e., destination node needs to be created. Selection of multiple paths from the source node to the destination node is preferred in this technique since there are possibilities for some paths to get broken, and hence the best available selected path can be used for data transmission as per the application requirement. To ensure that the selected path is secure and the source node is not a malicious node, routing to select multiple paths is performed by considering security measures. This process is described in Algorithm 1.

Algorithm 1 Routing security using multipath

Notations	*Meaning*
S	Source node
D	Destination node
RREQ	Route request message
RREP	Route reply message
ID	Identification/identity
S_{id}	Source ID
D_{id}	Destination ID
App_{Type}	Application type
HC	Hop count
P_n	Required parameter
H_x	Hash value
K_{ss_d}	Shared symmetric key for the destination
TS	Time stamp
j	Intermediate node
K_{jd}	Shared symmetric key for the intermediate node j
Def	Default application type
Mul	Multimedia application type
Sec	Secure application Type
BW	Bandwidth
Dly	Delay

1 When S wants to send data to D, it initially creates a RREQ message.

2 The RREQ message includes information S_{id}, D_{id}, App_{Type}, HC, P_n and H_x as shown in Table 1.

3 S encrypts H_x using K_{ss_d}.

4 If D is immediate neighbour of S, then S sends the RREQ message to D as shown below:

$$S \xrightarrow{RREQ\left[S, D, H_x, \{H_x, TS_S\}_{Kss\_d}\right]} D$$

5 If D is not a neighbour of S, then S broadcasts the RREQ message as shown below:

$$S \xrightarrow{RREQ\left[S, D, H_x, \{S, D, TS, H_x\}_{Kss\_d}\right]} IN$$

6 On receiving the RREQ message, j checks if its ID is already present in the message.

7 If j_{id} is already present in the message, then it indicates that the message is in an infinite loop, and hence message is discarded immediately.

8 If j_{id} is not present in the message, then it is considered to be in the correct path.

9 Next, the j checks the D_{id}.

10 Then j encrypts the hash value and appends its ID with the ID encrypted payload of previous node and then encrypts this whole message with K_{jd}.

11 If D is a direct neighbour of j, then j forwards the RREQ message to D as shown below:

$$j \xrightarrow{RREQ\left[S, j, D, H_x, \{H_x\}_{Kjd}, \{S, D, TS_S, H_x\}_{Kss\_d}\right]} D$$

12 If D is not a neighbour of j, then j broadcasts the RREQ message as shown below:

$$j \xrightarrow{RREQ\left[S, j, D, H_x, \{H_x\}_{Kjd}, \left\{j\{S, D, TS_S, H_x\}_{Kss\_d}\right\}_{Kjd}\right]} IN$$

13 In this way, j which receives the RREQ message keeps forwarding the message till it reaches the D.

14 On receiving the message, the D decrypts it in the reverse order of ID's recorded and verifies the H_x sent by S.

15 If all the values match, then D confirms that S is authenticated and all the IN along the route are valid and not malicious.

16 Then D checks the information present in App_{Type}.

17 If App_{Type} = 'Def', then D

18 considers the number of P_n set,

19 selects the n shortest paths

20 Else If App_{Type} = 'Mul', then

21 D analyses the route traversed by all RREQ messages

22 selects n paths with maximum BW and minimum Dly.

23 Else If App_{Type} = 'Sec', then

24 D analyses the route traversed by all RREQ messages

25 selects n paths that are highly secure.

26 End if

27 D responds by sending RREP message through the selected n paths.

Table 1 RREQ message fields

SID	*DID*	*App_{Type}*	*HC*	*P_1*	*P_2*	*P_3*	...	*P_n*	*H_x*

Thus, multiple paths are selected for the transmission of data from the source to the destination in a secure manner.

3.3 Data security

During the transmission of data, there are possibilities of data corruption due to various reasons. So, it is necessary to use DS technique to ensure the safety of the data being transmitted. In this technique, while transmitting the data packet, the data is encrypted using a hash value and then forwarded to the next node along the transmission path. This process is described in Algorithm 2.

Algorithm 2 Data security

Notations	*Meaning*
S	Source node
D	Destination node
RTS	Request to send
CTS	Confirm to send
H_x	Hash value
K_{ss_d}	Shared symmetric key for destination
TS	Time stamp
DP	Data packet sent from source to destination
IN_k	Intermediate node named k

K_{IN1d}	Shared symmetric key for intermediate node 1
DP_REP	Data packet sent by destination to source

1 After the selection of routes for data transmission, the S sends RTS to D through the selected routes, and initiates a timer.

2 On receiving the RTS message, the D responds by sending the CTS message to S.

3 If S does not receive any response from D before the timer expires, then S will resend RTS.

4 If S receives CTS from D before the timer expires, then S considers this time window to be appropriate for data transfer through the route.

5 Then S sends DP along with the H_x after encrypting it using K_{ss_d} to D as shown below:

$$S \xrightarrow{DP\left[S, IN_1, \ldots, IN_k, D, H_x, \{H_x, TS_S, Data\}_{Kss\_d}\right]} D$$

6 On receiving the DP message, the IN, encrypts the H_x and appends its ID with the ID encrypted payload of previous node and then encrypts this whole message with K_{ss_d}.

7 Next IN forwards it to the next node along the transmission path.

$$IN_1 \xrightarrow{DP\left[S, IN_1, \ldots, IN_k, D, H_x, \{H_x\}_{KIN1d}, \{TS_S, H_x, Data\}_{Kss\_d}\right]} D$$

8 In this way, the IN which receives the DP keeps forwarding the message till it reaches the D.

9 On receiving the message, the D decrypts it in the reverse order of ID's recorded and verifies the H_x sent by S.

10 Then D retrieves the Data from the DP.

11 Then D responds by sending the corresponding reply DP_REP to the S.

Thus, the data packet is transmitted between the source and destination securely by encrypting the data with the hash value before transmitting.

3.4 Intrusion detection system

Detection of intrusion in MANET is critical since the possible types of attacks and link failures in MANET are very high. To determine any case of intrusion, the Request To Send and Confirm To Send messages are used and its usage count is analysed. Also, the numbers of data packets transmitted and received are also used to determine the intrusion in the network. This process is described in Algorithm 3.

Algorithm 3 Intrusion detection system

Notations	*Meaning*
S	Source node
D	Destination node
RTS	Request to send
CTS	Confirm to send
$RTS_{n,i}$	Number of RTS messages sent by node i
$CTS_{n,i}$	Number of CTS messages replied by node i
$P_{rel\_col,i}$	Related collision probability of node i
$RTS_{un,i}$	Unanswered RTS messages for node i
$P_{Fwd,i}$	Probability for the packet to be forwarded
$DP_{Fwd,i}$	Data packet forwarded by node i
$DP_{Rxd,i}$	Data packet received by node i
$P_{drop,i}$	Probability of malicious packet dropping by node i
$P_{Rxd,i}$	Probability for the packet to be received by node i
$P_{atk,i}$	Probability of attack at node i
RTS_{Th}	Predefined RTS threshold value
T_{atk}	Predefined attack threshold value

1 On reception of data from D as a response to the data sent by S, the S computes RTS_n and CTS_n.

2 The IN nodes also estimate RTS_n and CTS_n. Messages forwarded by them

3 Next P_{rel_col} is estimated by each node involved in data transmission according to equation (1) given below:

$$P_{rel\_col,i} = RTS_{un,i} / RTS_{n,i} \quad (1)$$

where $RTS_{un,i} = RTS_{n,i} - CTS_{n,i}$

4 Then P_{Fwd} is estimated according to equation (2) given below:

$$P_{Fwd,i} = DP_{Fwd,i} / DP_{Rxd,i} \quad (2)$$

5 Next P_{drop} is estimated according to equation (3) given below:

$$P_{drop,i} = 1 - P_{Fwd,i} / P_{Rxd,i} \quad (3)$$

6 Then S estimates P_{atk} according to equation (4) given below:

$$\begin{aligned} P_{atk,i} &= 0 \quad \text{if } RTS_{n,i} - CTS_{n,i} > RTS_{Th} \\ &= P_{drop,i} \quad \text{else} \end{aligned} \quad (4)$$

7 To detect intrusion, the P_{atk} is compared with T_{atk}.

8 If $P_{atk,i} > T_{atk}$, then the node is considered to be malicious, and packets forwarded by it is discarded and the node is isolated.

9 If $P_{atk,i} < T_{atk}$, then the node is considered to be valid.

In this way, intrusion in MANET is detected and then it is handled by dropping the data packets received from the malicious node and then by isolating it.

4 Simulation results

4.1 Simulation parameters

The proposed cross-layered-based adaptive secured routing and data transmission (CLASR) protocol is simulated in NS2. The simulation settings and parameters are summarised in Table 2. The proposed CLASR protocol is compared with adaptive cross-layer multipath routing (ACLMR) protocol (Iqbal et al., 2016) and the performance of both the protocol is evaluated in terms of packet delivery ratio, packet drop, end-to-end delay, control overhead.

Table 2 Simulation parameters

Number of nodes	20, 40, 60, 80 and 100
Area size	1,000m × 1,000 m
MAC protocol	802.11
Simulation time	100 sec
Traffic source	Constant bit rate (CBR)
Number of data flows	5
Propagation model	Two-ray ground
Antenna model	Omni antenna
Number of attackers	1, 2, 3, 4 and 5
Packet size	512 bytes

4.2 Results and analysis

4.2.1 Varying the attackers

The number of attackers launching packet dropping attack is varied from 1 to 5 for 100 nodes.

Figure 2 Attackers vs. delay (see online version for colours)

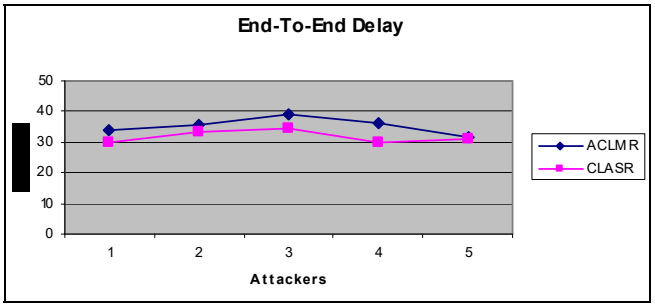


Figure 2 shows the delay occurred for CLASR and ACLMR techniques when the attackers are varied. The increase in attackers results in decrease in delay. As seen from the figure, the delay of CLASR increased from 30.12 to 30.82 and the delay of ACLMR decreases from 34.14 to 31.83. Hence, CLASR has 10% lesser delay than ACLMR technique.

Figure 3 Attackers vs. delivery ratio (see online version for colours)

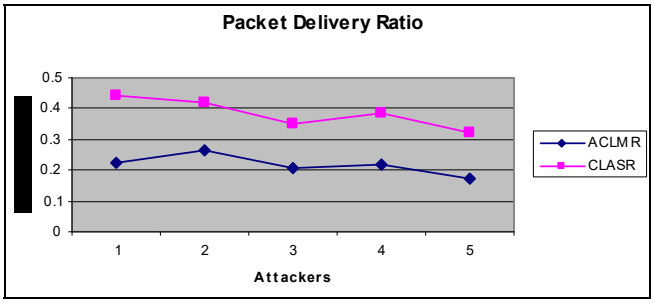


Figure 3 shows the delivery ratio occurred for CLASR and ACLMR techniques when the attackers are varied. The increase in attackers results in decrease in delivery ratio. As seen from the figure, the delivery ratio of CLASR decreased from 0.44 to 0.82 and the delivery ratio of ACLMR decreases from 0.22 to 0.17. Hence, CLASR has 43% higher delivery ratio than ACLMR technique.

Figure 4 Attackers vs. drop (see online version for colours)

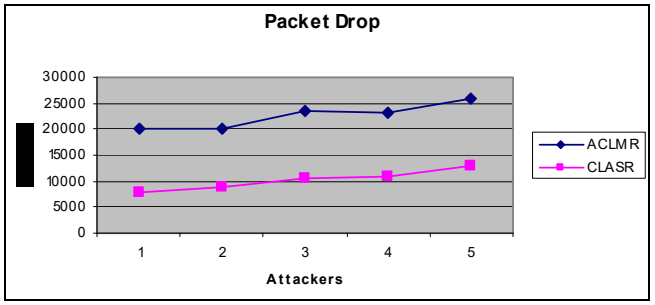


Figure 4 shows the drop occurred for CLASR and ACLMR techniques when the attackers are varied. The increase in attackers results in increase in drop. As seen from the figure, the drop of CLASR increased from 7,778 to 13,029 and the drop of ACLMR increases from 20,268 to 25,775. Hence, CLASR has 55% lesser drop than ACLMR technique.

Figure 5 Attackers vs. overhead (see online version for colours)

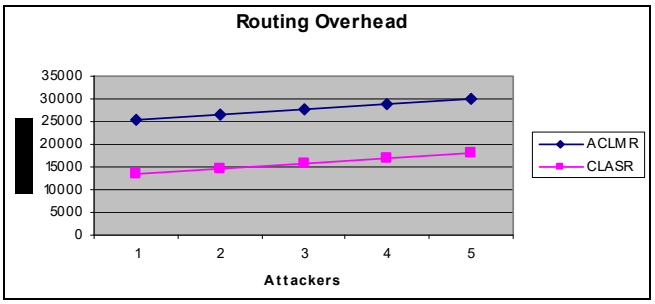


Figure 5 shows the overhead occurred for CLASR and ACLMR techniques when the attackers are varied. The increase in attackers results in increase in overhead. As seen from the figure, the overhead of CLASR increased from 13,345 to 18,202 and the overhead of ACLMR increases from 25,353 to 30,092. Hence, CLASR has 43% lesser overhead than ACLMR technique.

4.2.2 Varying the number of nodes

The number of nodes is varied as 20, 40, 60, 80 and 100 keeping two attackers.

Figure 6 Nodes vs. delay (see online version for colours)

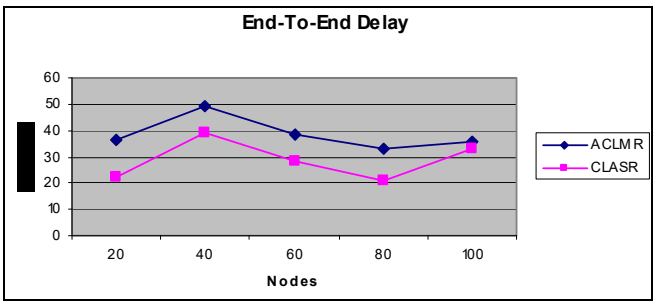


Figure 6 shows the delay occurred for CLASR and ACLMR techniques when the nodes are varied. The increase in nodes results in decrease in delay. As seen from the figure, the delay of CLASR increased from 22.36 to 33.19 and the delay of ACLMR decreases from 36.68 to 35.75. Hence, CLASR has 26% lesser delay than ACLMR technique.

Figure 7 Nodes vs. delivery ratio (see online version for colours)

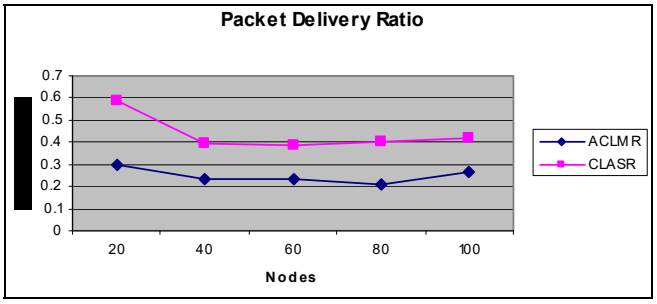


Figure 7 shows the delivery ratio occurred for CLASR and ACLMR techniques when the nodes are varied. The increase in nodes results in decrease in delivery ratio. As seen from the figure, the delivery ratio of CLASR decreased from 0.59 to 0.41 and the delivery ratio of ACLMR decreases from 0.29 to 0.26. Hence, CLASR has 43% higher delivery ratio than ACLMR technique.

Figure 8 Nodes vs. drop (see online version for colours)

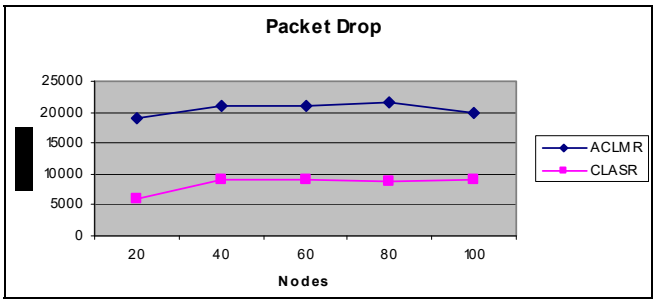


Figure 8 shows the drop occurred for CLASR and ACLMR techniques when the nodes are varied. The increase in nodes results in increase in drop. As seen from the figure, the drop of CLASR increased from 6,041 to 8,994 and the drop of ACLMR increases from 19,085 to 19,965. Hence. CLASR has 59% lesser drop than ACLMR technique.

Figure 9 Nodes vs. overhead (see online version for colours)

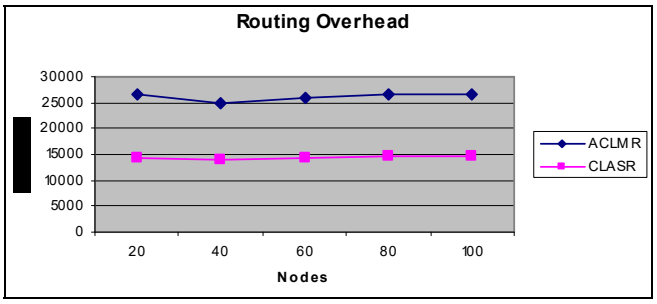


Figure 9 shows the overhead occurred for CLASR and ACLMR techniques when the nodes are varied. The increase in nodes results in increase in overhead. As seen from the figure, the overhead of CLASR increased from 14,369 to 14,555 and the overhead of ACLMR increases from 26,446 to 26,576. Hence, CLASR has 45% lesser overhead than ACLMR technique.

5 Conclusions

In this paper, we have proposed a cross-layered-based adaptive secured routing and data transmission technique in MANET. In this technique, prior data transmission, multiple routes are determined between source and destination, using request messages. Then the routes with higher security and which satisfies the application requirements are selected by the destination node and it responds through these selected routes. This helps in providing RS. Next, the source transmits data by encrypting it with the hash value to ensure DS. During data transmission, every node along the selected route monitors the number of messages transmitted and received, and then estimates the attack probability of the nodes. In this way, intrusion in the network is detected and the nodes detected to be malicious are isolated from the network. By simulation results, it has been shown that the proposed CLASR protocol reduces the packet drop due to various attacks and improves the delivery ratio.

References

Aldabbas, H., Alwada'n, T., Janicke, H. and Al-Bayatti, A. (2012) 'Data confidentiality in mobile ad hoc networks', *International Journal of Wireless & Mobile Networks (IJWMN)*, February, Vol. 4, No. 1, pp.490–499.

Alnumay, W.S. and Ghosh, U. (2014) 'Secure routing and data transmission in mobile ad hoc networks', *International Journal of Computer Networks & Communications (IJCNC)*, January, Vol. 6, No. 1, pp.111–127.

Aluvala, S., Sekhar, R. and Vodnala, D. (2016) 'A novel technique for node authentication in mobile ad hoc networks', *Perspectives in Science*, Vol. 8, No. 8, pp.680–682, Elsevier.

Athreya, A.P. and Tague, P. (2011) 'Towards secure multi-path routing for wireless mobile ad-hoc networks: a cross-layer strategy', *2011 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, IEEE.

Dhurandher, S.K., Obaidat, M.S., Verma, K., Gupta, P. and Dhurandher, P. (2011) 'FACES: friend-based ad hoc routing using challenges to establish security in MANETs systems', *IEEE Systems Journal*, June, Vol. 5, No. 2, pp.176–188.

Iqbal, Z., Khan, S., Mehmood, A., Lloret, J. and Alrajeh, N.A. (2016) 'Adaptive cross-layer multipath routing protocol for mobile ad hoc networks', *Journal of Sensors*, Volume 2016, Article ID 5486437, 18pp, http://dx.doi.org/10.1155/2016/5486437.

Kaliappan, M. and Paramasivan, B. (2014) 'Enhancing secure routing in mobile ad hoc networks using a dynamic Bayesian signalling game model', *Computers and Electrical Engineering*, Vol. 41, No. 6, pp.301–313.

Rajkumar, B. and Narsimha, G. (2016) 'Trust based certificate revocation for secure routing in MANET', *2nd International Conference on Intelligent Computing, Communication & Convergence*, pp.431–441.

Saha, H.N., Bhattacharyya, D. and Banerjee, P.K. (2012) 'A novel multipoint relay based secure routing in MANET', *International Journal of Network Security & Its Applications (IJNSA)*, November, Vol. 4, No. 6, pp.133–144.

Sánchez-Casado, L., Maciá-Fernández, G. and Garcia-Teodoro, P. (2012) 'An efficient cross-layer approach for malicious packet dropping detection in MANETs', *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, IEEE.

Singh, R., Saha, H.N., Bhattacharyya, B. and Banerjee, P.K. (2016) 'Administrator and fidelity based secure routing (AFSR) protocol in MANET', *CIT: Journal of Computing and Information Technology*, March, Vol. 24, No. 1, pp.31–43.