Coherence Key Based Node Authentication for Routing in Mobile Ad Hoc Networks

P. Gowthamarayathirumal, C. Chandrasekar, A. Sridhar

Abstract: ***Mobile Ad hoc network (MANETs) is a self-organizing multi-hop wireless network with dynamic topologies. Due to the absence of Control Authority in MANET, the network seems to be vulnerable that can be easily destroyed by the entry of malicious nodes. The presence of malicious nodes can destroy the data transmission of the network. So, finding and removing the malicious nodes is one of the critical issues in the MANET. With the help of the proposed Coherence Key Based Node Authentication for Routing (CKR) Algorithm, each and every mobile node are authenticated while updating the routing table by using the authentication key value that is generated with the help of random number with the secret key. Only the authenticated nodes (non-Malicious Nodes) are updated in the routing table and the remaining nodes which are not authenticated (malicious nodes) will be eliminated from the routing table. So that, the malicious node will not participated and could not destroy the data transmission. Thus, it makes this Multi-hop network as more trustful network.***

Keywords: Manet security, coherence key, malicious node, Authentication.

I. INTRODUCTION

Mobile Ad-hoc Networks (MANETs) consisting of self-organizing and limited powered mobile nodes with less resource accessibility and computational capabilities. MANETs used in many applications such as military operations, environmental monitoring, rescue operations etc. Every mobile node in MANET is associated with a wireless transmitter and receiver that can communicate with other nodes within its communication range [1]. Due to the limited wireless communication range and node mobility, every node in this network must cooperate with other nodes to afford interacting services among themselves. Hence, each mobile node in MANET performs as a host and also a router. The dynamic nature of MANETs creates them susceptible to different types of attacks namely black hole attack, IP spoofing, Denial of Service (DoS) attack and traffic distortion, etc., Some of the nodes may try to participate in this wireless network to reduce or destroy the data transmission of the network.

Due to the battery power of the mobile nodes, the unnecessary data transmission should be vanished. So that, the participation of the malicious nodes must be avoided to makes the network alive. The malicious nodes reduce the overall performance of the entire network. Therefore, in order to enhance the performance and lifetime of the network we have to discard the malicious nodes.

MANET does not have any control authorities to monitor and control the data transmission. Here, several. Nodes can act as mediator to transmit the data from one node to another and those nodes are called as intermediate nodes

So, every data transmission may reduce the life time of other nodes. So unwanted and redundant data transmission must be avoided. A node may act as malicious for several reasons. Some of the reasons are listed here. If a node does not want to help other data transmission, i

t may simply ignore the packets or sometime it receives the packets but it does not forward the packets to its neighbors. It makes the communication gap between the source and destination. Some of the nodes may reject to forward the data in order to save its own battery power. They refuse to use its power for others transmission. These are the malicious behavior based on the situation.

Sometimes, some of the nodes entered and participate in the network to destroy the communication and to get the data packets by representing it as the neighbor or the destination. The malicious nodes can also act as an intermediate node in the MANET data transmission. These nodes may not forward the data after it received the data. So, the network will be destroyed. Therefore, finding the malicious node and removing them from the data transmission are the major problems in the Mobile Ad-hoc Networks.

The rest of paper structure is organized as follows. Section 2 describes the related works, Section 3 explains the Coherence Key Based Node Authentication algorithm for routing the data in Mobile Ad Hoc Networks with the assist of architecture diagram, Section 4 explains the experimental settings and Section 5 analyses the performance details with the aid of parameters. Section 6 concludes this paper.

II. RELATED WORKS

Recently, many researchers designed this network for improving security of MANETs. I-Watchdog protocols were designed in [1] for attaining secure routing with prevention of denial of service attack and also detecting the congestion in MANETs. I-Watchdog protocol improves throughput with reduced end-to-end delay and packet drop. However, finding the malicious nodes entry cannot be identified before the data transmission. Many research works is intended for achieving secured routing in MANETs. For example, Trust-based Source Routing (TSR) protocol was presented in [2] to select the shortest route and to fulfill the security requirement of data packets transmission in MANETs. Besides, TSR protocol increases packet delivery ratio and diminishes average end-to-end latency. But, securing communication between the mobile nodes is remained unsolved. Fuzzy Petri NeT based

Revised Manuscript Received on January 15, 2020

Dr.P.Gowthamarayathirumal*, Assistant Professor of Computer Science, Government Arts College, Dharmapuri, Tamilnadu, India.

Dr.C.Chandrasekar, Professor, Dept. of Computer Science, Periyar University, Salem. Tamilnadu, India.

Dr. A. Sridhar, Assistant Professor, Dept. of Computer Science, Government Arts College, Dharmapuri, Tamilnadu, India

Optimized Link State Routing (FPNT-OLSR) protocol was designed in [3] to select higher trust path among all possible paths in MANETs. The FPNT-OLSR identifies malicious or compromised nodes in the network. However, attack detection performance was not efficient.

A trust based model was designed in [4] to measure the trust level of nodes and to perform secured routing in MANETs, but the secured data transmission rate was poor. An iterative algorithm was developed in [5] for trust management and performing adversary detection in delay-tolerant networks. But, the attack detection rate was not sufficient. The cooperation between trust and routing mechanism was intended in [6] to elect reliable and secure the data transmission through selecting malicious nodes. Service Authentic Trust and Coherence Key Based Secured Routing for Mobile Ad Hoc Network [7] and Service Authentic Trust and Reputation Scheme for Secured Routing in Mobile Ad Hoc Networks [8] proposed to authenticate the mobile nodes in MANET. But however, these authentications are placed after sending some packets to those nodes. Based on the forwarding capacity of the nodes, the algorithm identifies the nodes which have the malicious behavior.

Enhanced adaptive acknowledgement model was designed in [9] to enhance the performance of malicious node detection in MANETs with higher accuracy rate. An Ad hoc On-demand Multicast Distance- Vector–Secure Adjacent Position Trust Verification (AOMDV–SAPTV) was presented in [10] to find out the optimal path for routing and attaining the security in MANETs. But, avoiding different attacks was remained unaddressed. A novel method was developed in [11] to enhance the security among the nodes in MANETs through the authentication. However, it does not present more security service. A hybrid Intrusion Detection System (IDSs) scheme was intended in [12] for intrusion detection in MANETs. The hybrid IDS scheme reduces the power consumption and also attains a high detection rate. But, the false positive rate for intrusion detection was very low which affects the security of data transmission in MANETs. An Enhanced Adaptive ACKnowledgment (EAACK) intrusion-detection system was introduced in for discovering the malicious activities in MANETs. However, EAACK does not achieve energy efficient secured data transmission.

A standard ad hoc on-demand multi-path distance vector protocol was employed in [13] to provide the security against vulnerabilities and attacks in MANETs. This method did not provide optimal throughput. A Danger-Theory based Artificial Immune Algorithm was presented in [14] to enhance the security of multipath routing in MANETs through detecting the attack. But, the attack detection performance was not efficient.

III. COHERENCE KEY BASED NODE AUTHENTICATION FOR ROUTING IN MOBILE AD HOC NETWORKS (CKR)

In order to overcome the security issues due to the malicious nodes participation in the network, the Coherence Key Based Node Authentication for Routing in Mobile Ad Hoc Networks (CKR) technique is proposed. The key objective of this proposed technique is to authenticate the mobile nodes to participate in the network. The authentication is based on some key parameter from each mobile nodes. The research objective of CKR technique is formulated as follows,

- To improve the security performance in data communication in MANET.
- To identify and remove the malicious nodes in the network and to restrict the nodes to participate in the network.
- To detect the malicious nodes with higher attack detection rate.
- Discover the optimal path with no malicious nodes.
- Reduce the end to end latency by avoiding the instant route authentication.

Let consider the mobile ad hoc network with n number of autonomous mobile nodes with random mobility in random direction. The number of mobile nodes in network is represented as'$MN_i = MN_1, MN_2, MN_3 \ldots MN_n$ that lies with wireless links within the transmission range $'R'$. The data transmission from the source to destination will be transmitted by multi-hop routing techniques. It is also infrastructure less and dynamic in nature. The mobile nodes have restricted battery power and communicate through shared wireless channel, therefore it is difficult to design a secure routing protocol in MANET. In order to overcome such limitations, Coherence Key Based Node Authentication for Routing (CKR) technique is designed.

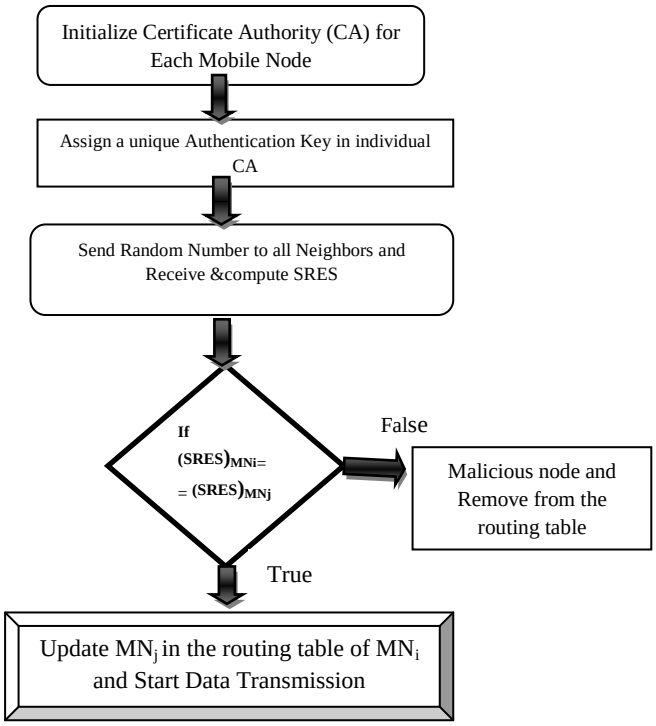

Figure 1: Architecture Diagram for Coherence key based Node Authentication

The main goal of CKR technique is to provide an authentication technique adapted for the autonomous mobile nodes in the Ad-hoc networks. The architecture diagram of CKR technique is shown in Figure 1. This authentication process in CKR technique has done while updating the routing table. There might be 2 cases are available.

In Case 1, both the sender and Receiver know each other, means that both the sender and receiver having the coherence key of others. Here, consider Node 'x' is a sender, Node 'y' is the receiver. The authentication

procedure is shown in Figure 2. Figure 3 represents the Node authentication process for case 2.

In the Case 2, sender has the coherence key of the receiver, so that the sender knows the receiver. But the receiver does not have the coherence key of the sender. So the receiver doesn't know about the sender. Now the receiver has to authenticate the sender first then only the receiver replies for the sender for further transactions.

3.1 Certificate Authority (CA)

Every mobile node has individual certificate authority to store the coherence keys of the mobile nodes. All the nodes are configured with predefined Coherence key in it. The initialization of the first generated node will only have its own coherence key. The initialization of the second node has included the coherence key of both first node and its own Coherence key. Like that, the n^{th} node has the coherence key of its own and also with the coherence key of the previous initialized nodes (MN_1, MN_2,……,MN_{n-1}).

Every node have a unique 8 bit Coherence Key (CK). Therefore we can create 2^8 keys and we can run the simulation with maximum of 256 Mobile Nodes(MN). Every Certificate Authority consists of two fields. They are Header field and Data field.

Header field consist of Individual Mobile Node ID (MN_{ID}), Certificate Authority ID (CA_{ID}), Coherence key of that particular Mobile Node ($CK(MN_i)$).

Data field consist 2 static fields and 2 dynamic fields. The static field consists of the Mobile Node ID and their 8 bit Coherence Key of authenticated Mobile Nodes. The dynamic field consist the dynamic details such as 8 bit Random Number (RN) and 16 bit Signed Response (SRES).

3.2 Coherence Key

Coherence key is defined as the unique symmetric key assigned for every mobile nodes in MANET. This key is generated and assigned randomly to the mobile nodes at the time of node initialization. All the Coherence keys generated in 8 bits and the random number is generated in 8 bits. Therefore2 power 8 will produce 256 different unique keys from the range 0 to 256 numeric values can be used here.

The computed Signed response is 16 bit value. Therefore 8 bit coherence key and 8 bit Random value is multiplied to get the signed response. The maximum value of the random number and coherence key are in between the value from 0 to 256. So we can able to generate unique coherence Key for maximum of 256 nodes.

3.3 Mobile Node Authentication

Let us consider the Mobile Node MN_j wants to update its routing table, therefore the Mobile Node MN_j is considered as the sender, and the other nodes in the network are considered as receiver. For every routing table updation, Each and every nodes in the network send a Random Number(RN_j) and compute Signed Response of the neighbors ($SRES(MN_j)$).

$$SRES(MN_j) = RN_j * CK(MN_i) \quad (1)$$

After computing the Signed Response ($SRES(MN_j)$) of the i^{th} mobile node (MN_i), the mobile node MN_j wait for the signed response of the receiver(MN_i).

Case 1: Sender (MN_j) and Receiver (MN_i) knows each other with their coherence key.

After receiving the Random Number ($RN(MN_j)$) of the mobile node MN_j, if the receiver has the coherence key of the sender ($CK(MN_j)$), then the receiver (MN_i) compute the signed response($SRES(MN_i)$) by multiplying the random number ($RN(MN_j)$) with its own Coherence key($CK(MN_i)$) and send itto the source node (MN_j).

$$SRES(MN_i) = RN_j * CK(MN_i) \quad (2)$$

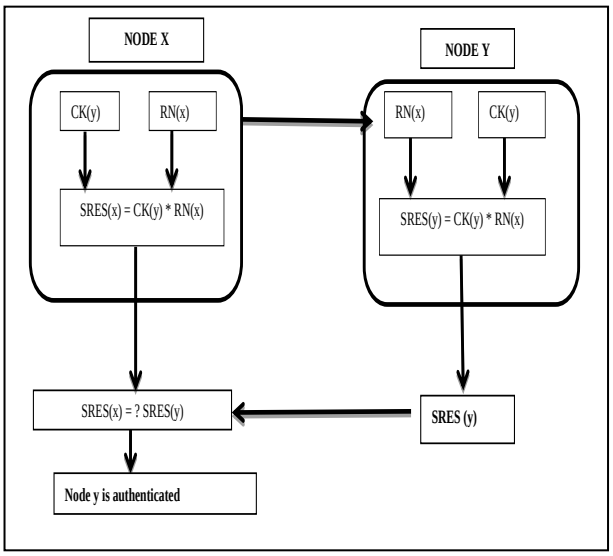

Figure 2: Node Authentication Process-I in CKR

After receiving the SRES(MNi) from the node MNi, the sender verify the value with its SRES(MNj).

$$SRES(MNj) == SRES(MNi) \quad (3)$$

If both of the responses are seems to be equal, then the Mobile Node MN_i is authenticated and updated in the routing table of the Mobile Node MN_j, otherwise the Mobile Node MN_i is considered as Malicious Node and it will be denied for further transaction with MN_j. This process is shown in the figure 2.

Case 2: Sender (MN_j) knows the Receiver (MN_i) but MN_i doesn't know about MN_j.

If case 1 is not satisfied, it implies that the receiver(MN_i) does not have the coherence key of MN_j in its certificate authority ($CA(MN_i)$), MN_j has to be authenticated by MN_i. Here, the receiver is known to the sender but the sender is not known to the receiver. Here, MN_j knows the coherence key of MN_i, but MN_i does not have the coherence key of MN_j. So, MN_i have to authenticate the Mobile node MN_j which sent the Random Number $RN(MN_j)$to MN_i. MN_i authenticates the Mobile node MN_jif and only if the MN_j has the coherence key of MN_i ($CK(MN_i)$).

In order to verify the availability of the coherence key of the receiver $CK(MN_i)$ in the sender's certificate Authority($CA(MN_j)$), the receiver MN_i replies a random number ($RN(MN_i)$) to the sender. If the sender MN_j

receives the($RN(MN_i)$) then he compute the response as

$$SRES(MN_j) = RN(MN_i) * CK(MN_i) \oplus CK(MN_j \quad (4)$$

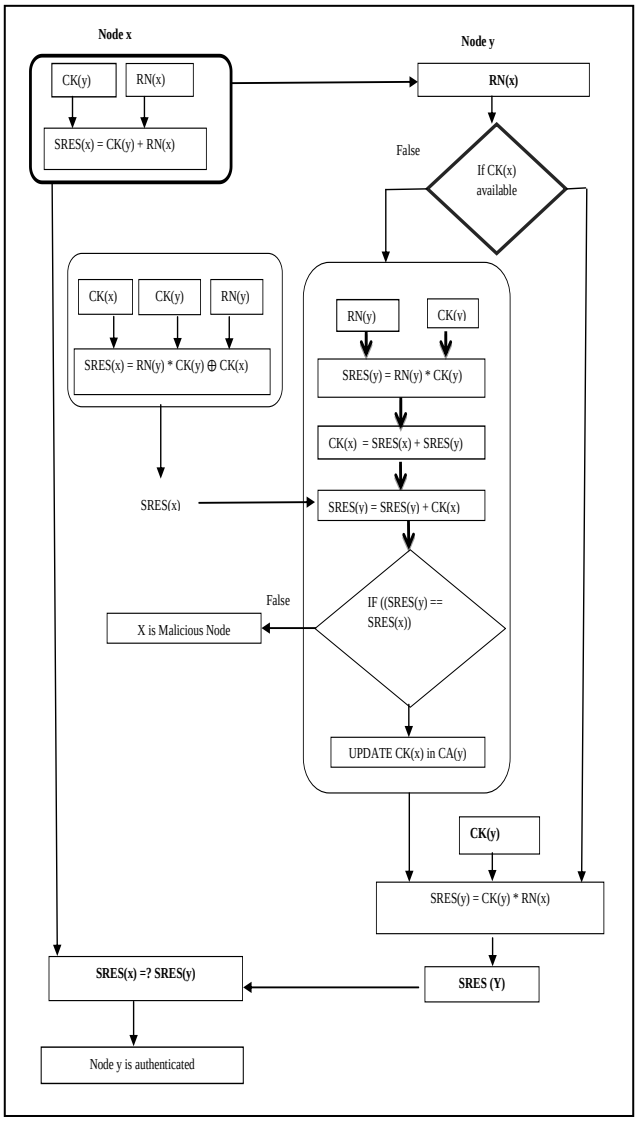

Figure 3: Node Authentication Process-II in CKR

This signed response $SRES(MN_j)$ included the key of both MN_j and MN_i with the random Number ($RN(MN_i)$) of the MN_i. Here the MN_j compute the response $SRES(MN_j)$ as random Number provided by the MN_i with its Coherence key ($CK(MN_i)$) and it will XOR the result with its own Coherence Key($CK(MN_j)$) and transmit as $SRES(MN_j)$ to MN_i to provide its own coherence key ($CK(MN_j)$) in secret manner.

$$CK(MN_j) = SRES(MN_j) \oplus SRES(MN_i) \quad (5)$$

If MN_i receives $SRES(MN_j)$, it will extract the keys and if this response included its own Coherence key($CK(MN_i)$) then the MN_i consider the remaining values as the coherence key of the MN_j.

$$SRES(MN_i)==SRES(MN_j)+CK(MN_j) \quad (6)$$

Then it will update the $CK(MN_j)$ in its Certificate Authority ($CA(MN_i)$) and it will update MN_j as authenticated node.After updating the $CA(MN_j)$, the MN_i responses ($SRES(MN_i)$) to the first message ($RN(MN_j)$) and send back to MN_j.

Now the MN_j verify the $SRES(MN_i)$ with its calculated $SRES(MN_j)$, if both of the SRES is equal, then MN_j update its routing table entry with MN_i.

Table 1: Coherence Key based Mobile Node Authentication Algorithm

Algorithm: Mobile Node Authentication using Coherence Key
Input: Mobile Nodes MN_i, i=1 to n;
Output: Authenticated Nodes & Malicious Nodes
If MNj want to communicate with MN_i
// To authenticate other nodes
// Updation of routing table of MN_j
Step 1: MN_j will send a $RN(MN_j)$ to MN_i
Step 2: MN_j COMPUTE ($(SRES(MN_j) = RN(MN_j) * Key(MN_i))$ From its $CA(MN_j)$
Step 3:IF (MN_i has the key(MN_j) in $CA(MN_i)$)
Step 4: MN_i COMPUTE ($(SRES(MN_i) = RN(MN_j) * Key(MN_i))$ From its $CA(MN_i)$ and Send $SRES(MN_i)$ to Node MN_j
Step 5:If ($SRES(MN_j) == SRES(MN_i)$)
Step 6: Node MN_i is authenticated
Step 7: Add Node MN_i in the routing table
Step 8: Transmit data;
Step 9:Else
Step 10: Node MN_i is not authenticated // Malicious
Step 11: Don't add in the routing table as intermediate nodes
// key of MN_j is not listed in MN_i
// To Authenticate (MN_j) by MN_i
Step 12: Else IF (MN_i replies a $RN(MN_i)$ to MN_j), do step 13 to step 23// node MNj not Exists in CA(i)
Step 13:MNi compute SRES(MNi) = RN(i) *key of (MNi)
Step 14: Then MNj compute SRES(MNj) = ((RN(i) * Key of MNi) ⊕ KEY(MNj))
Step 15: Send SRES(MNj) to MNi
Step 16:IF (MNj replies SRES(MNj)) to MNi do step 17 and step 18.
//MNi Compute
Step 17: Key(MNj) = SRES(MNj) ⊕ SRES(MNi)
Step 18: **IF** (SRES(MNi)==SRES(MNj)+Key(MNj)) do step 19 and step 20
//Then // MNj is trusted// authenticated
Step 19: **Update Key of (MNj) in CA of MNi**
Step 20: GOTO Step 3;
Step 21: **ELSE** GOTO Step 11 and EXIT;
Step 22:ELSE GOTO Step 11 and EXIT;
Step 23:ELSE GOTO Step 11 and EXIT;
Step 24: End if;

Thus the authentication is success. If the Signed responses does not equal or if there is no signed response received, then the MN_i is considered as malicious node and it will be eliminated from the network. By using the represented Coherence Key based Mobile Node authentication algorithm, every mobile nodes authenticates the other mobile nodes to its routing tale entry. The nodes which are failed in the above process will be restricted from the networks. Thus we eliminate all the unauthenticated or malicious node participation in the MANET network. Table 1 shows the steps involved in Coherence Key based node authentication algorithm.

3.4 Routing Table Updation

The nodes which are all authenticated using the proposed coherence key based node authentication are only considered for the data transmission in the network. The further Quality of services measures such as Shortest route, fastest route, higher bandwidth are also considered in the routing table updation as per the DSDV routing protocol.

IV. SIMULATION ENVIRONMENT

We evaluate the performance of proposed method, Coherence Key Based Node Authentication for Routing in MANET with the help of DSDV protocol. As per the nature of DSDV, it always update their routing table with the best neighbor in terms of several QOS measures. Now our proposed method deployed the routing table entries only with the authenticated mobile nodes rather than considering all the mobile nodes in the network.

It provides the reliable data transmission in the Mobile Ad hoc Network. This proposed Coherence Key Based Node Authentication for Routing method is implemented in NS-2 simulator with the network range of 1000*1000 m. The CKR Technique is employed with Destination Sequence Based Distance Vector (DSDV) as routing protocol for performing the simulation work. The simulation parameters used for conducting the simulations is shown in below Table 2.

Table 2: Simulation Parameters

Parameters	Value
Network simulator	NS 2.34
Protocols	DSDV with Coherence Key
Network range	1000 m * 1000 m
Simulation time	5 sec
Number of mobile nodes	1 – 20 nodes
Number of Malicious Nodes	0 –10 nodes
Number of Packets	1000
Mobility speed	10 m/s
Pause time	15 ms
Mobility model	Random Way Point Model
Transmission range	300m
Packet Size	512 bytes

The simulation is carried out for different time instances with diverse mobile node density and speed. In addition, the effectiveness of proposed CKR Technique is evaluated with different sizes of data for transmission along with numerous malicious adversaries for achieving communication security in MANETs. The performance of CKR Technique is compared against with the existing TSR Protocol and OLSR protocol. The performance of DSDV with CKR Technique is measured in terms of Attack detection rate, False Detection Rate for identifying the malicious nodes and QOS parameters such as latency, Packet Delivery Ratio, throughput and Routing overhead are also examined as below.

V. RESULTS AND DISCUSSIONS

In this section, the result analysis of CKR Technique is evaluated. The efficiency of CKR Technique is compared against with the existing two methods namely TSR Protocol and OLSR protocol. The performance of CKR Technique is evaluated along with the following metrics with the assist of tables and graphs that are listed below.

5.1 Certificate Authority

In the proposed CKR method, the mobile nodes are all configured with a certificate authority that contains their own Coherence key details along with coherence key of all other trusted nodes in the networks. The format of certificate authority of the mobile node 10 is represented in Table 3.

The first column of the Table 3 denotes the ID of the mobile nodes in the network. Here 10 nodes are considered for the simulation. The Mobile Node M10 is initialized after the initialization of the mobile nodes MN_1, MN_2.,…….MN_9. So, MN_{10} consist of the coherence key of previously created nine Mobile nodes.

Table 3: Certificate Authority of Mobile Node MN_{10}

CERTIFICATE AUTHORITY OF NODE M_{10}			
Mobile Node	**Coherence Key ($CK(M_{10})$)**	**Random Number $RN(MN_{10})$**	**$SRES(MN_i)$**
MN_1	01000000	00001010	0000001010000000
MN_2	01000001	00001010	0000001010001010
MN_3	01000010	00001010	0000001010010100
MN_4	01000011	00001010	0000001010011110
MN_5	01000100	00001010	0000001010101000
MN_6	01000101	00001010	0000001010110010
MN_7	01000110	00001010	0000001010111100
MN_8	01000111	00001010	0000001011000110
MN_9	01001000	00001010	0000001011010000
MN_{10}	01001001	-	-

MN_{10} wants to update the routing table, so that it verify and authenticate the neighbors in the network. So it sends a Random Number ($RN(MN_{10})$ as 00001010) to all the nodes in the network, then it calculate the Signed Response ($SRES(MN_i)$) and store in the certificate Authority. After receiving the SRES from the other nodes, MN_{10} will check the equality of the Signed response by using Eqn 3.

Table 4: Authentication of New Node

Authentication of New Node												
Steps	**Y Knows Node X & key (x).**		**X doesn't Know Y and Key(y) so it sends RN to y**									
1	Y calculate	RN* K(x)	SRES (y)	1	1	1	1	1	1	1	1	1
2	Y Fetch from its CA(y)	Key(y)	Key	1	0	0	0	0	0	1	0	0	1
3	Y compute	SRES (y) + KEY(y)	XOR 1,2	0	1	1	1	1	1	0	1	1	0
	Send the result got from step3 to X											
4	X received			0	1	1	1	1	1	0	1	1	0
5	X Compute	RN* K(x)	SRES(x)	1	1	1	1	1	1	1	1	1	1
6	Extract Key(y)	to get key (Y)	XOR 4,5	1	0	0	0	0	0	1	0	0	1
7	Extract SRES(y)	to get SRES (Y)	Add 4,6	1	1	1	1	1	1	1	1	1	1
if (eqn 5 ==7) ==>> if(SRES(x)==SRES(y)) then Update Key(y) in CA(x)												

Authentication of a new node has been done by the above steps in the Table 4.

This process includes the authentication and also the coherence key interchange in a secured manner in the dynamic network.

5.2 Attack Detection Rate (ADR)

Attack Detection Rate is the measurement uses to measures the performance of the malicious node detection algorithm to identify the Number of malicious node and normal nodes from the available malicious and normal nodes. It is computed by using Eqn 7.

$$\text{Accuracy} = \frac{TP+TN}{P+N} \quad (7)$$

Here,

TP : The True Positive represents that the Number of malicious nodes are identified as malicious.

TN: The True Negative represents that the Number of Normal Nodes are identified as Normal.

P : Positive (P) refers the total numbers of malicious nodes are available in the network.

N : Negative (N) refers the total Number of Normal nodes are available in the network.

Table 5: Attack Detection Rate Using Single Hop

Total No. of Normal Nodes: 10 Nodes								
Total No. of Malicious Nodes: 10 Nodes								
Node ID	No. of Malicious Nodes	Routing table updation at time (t)						
		Neighbour Node		Normal Nodes		Malicious		Attack Detection Rate (Accuracy)
		N	P	TN	FN	TP	FP	
MN_1	10	3	4	3	0	3	1	0.86
MN_2	10	5	2	4	1	1	1	0.71
MN_3	10	4	2	4	0	2	0	1.00
MN_4	10	6	3	4	2	3	1	0.78
MN_5	10	4	2	4	0	2	0	1.00
MN_6	10	3	2	3	0	1	1	0.80
MN_7	10	2	1	1	1	1	0	0.67
MN_8	10	1	1	1	0	1	0	1.00
MN_9	10	3	2	2	1	2	0	0.80
MN_{10}	10	2	1	2	0	1	0	1.00
Average Attack Detection Rate (Accuracy *100)								86%

The above table shows that the Attack detection rate that is computed using the equation 7. Here, the nodes in this network have mobility. Consider the route update request has been done in time t1, and the route reply comes at the time t2. The nodes which are reply the wrong SRES value are considered as malicious nodes. Some of the mobile nodes are moved away from the source node. So the node which is received and doesn't reply due to the mobility is also considered as malicious nodes. So, the false identification may happen by only considering the nodes in the single hop distance.

5.3 False Identification (FI)

It is the measurement to measure the wrongly identified nodes. This false identification may provide some wrong judgment about the good nodes but it does not affect the data transmission of the network. False identification of malicious may not be a problem, because of the nodes which doesn't reply are all treated as malicious. If the malicious node move away from the sender is also considered as malicious. Whenever that wrongly identified nodes are nodes comes to the transmission range, then it will authenticate once again while updating the routing table. So the false identification does not affect the network.

In order to reduce the false identification, multi hop routing is considered. Here, MANET is considered as multi hop network, In this multi hop scenario, the routing table of the neighborhood nodes are also updated in the routing table of all other nodes. Thus makes the network to know the route of each and every normal nodes (non-malicious nodes) in the network. And this multi hop routing by using the proposed CKR provides 100 percent attack detection rate.

5.4 Latency

Latency is one of the Quality of Service measurements which denotes the inactivity period of the node. Whenever a node initiate a data transmission to the other nodes, it has to configure themselves for attaining the data transmission [13].

Latency measures the amount of time taken for initiate a data transmission from one to another.

$$Latency = FST+LD+QD+NPD \quad (8)$$

Latency includes the time taken for Frame Serialization Time (FST), Link Media Delay (LD), Queuing Delay (QD), and Node Processing Delay (NPD).

Here, the above metrics can be calculated by the following formulas.

$$FST = S/R \quad (9)$$

$$LD = D/p \quad (10)$$

$$QD = Q / R \quad (11)$$

In the above equations,

R: link data rate (bits/second), S: Packet size (bits), D: Link distance (meters), P: Processing Delay (seconds), Q: Queue depth (bits)

Table 6: Latency in CKR

No. of Nodes	No. of Malicious Nodes	Latency (ms)		
		TSR protocol	OLSR protocol	DSDV with CKR
20	0	19	10	14.03
20	2	20	200	14.25
20	4	21	210	14.65
20	6	23	215	14.66
20	8	25	275	16.25
20	10	27	290	15.26
Average Latency		22.5	215	14.85

The simulation results are represented in the above table and in the figure. From this simulation, we can identify that the proposed method takes less latency when compared to the existing TSR protocol and OLSR protocol. Our proposed method has less latency because of the processing delay has been minimized for authenticating. The routing table updation has been done in as pre active, so it cannot make delay for route finding at the time of data transmission.

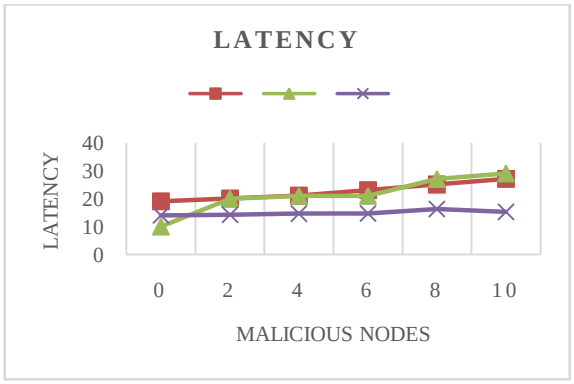

Figure 5: Latency vs Malicious Nodes

5.5 Packet Delivery Ratio (PDR)

Packet delivery ratio represents the percentage of number of packets delivered to the destination successfully. Because of the mobility, overload, route findings a packet may not reach the correct destination properly. So a network with higher PDR is considered as a good one. Packet Delivery ratio has been computed as the ratio between the total Number of Packets received (PR) and total number of Packets sent (PS) to the particular node from the source node.

PDR= (PR /PS)*100 (12)

Table 7: Packet Delivery Ratio in CKR

No. of Nodes	No. of Malicious Nodes	Packet Delivery Ratio (%)		
		TSR protocol	OLSR protocol	DSDV with CKR
20	0	82.25	79.83	84.35
20	2	81.35	77.26	83.57
20	4	76.66	80.24	82.23
20	6	72.00	77.00	80.63
20	8	64.00	69.49	79.98
20	10	57.00	60.55	78.89
Average PDR		**72.21**	**74.06**	**81.61**

Here, we insert the malicious nodes from 2 to 10 nodes out of 20 nodes in the simulation. The results shows that our proposed method Coherence Key based node Authentication in DSDV protocol produces higher Packet delivery ratio when compared to the existing protocols TSR and OLSR.

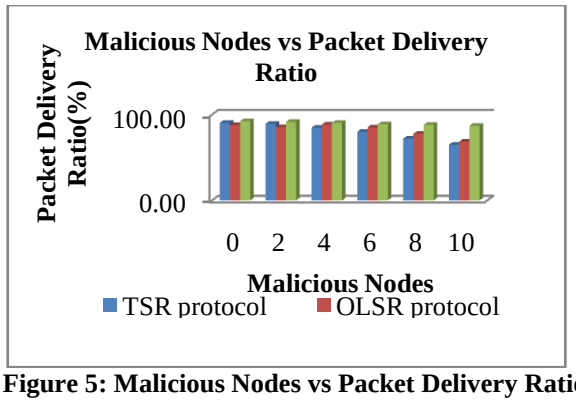

Figure 5: Malicious Nodes vs Packet Delivery Ratio

The Packet delivery ratio has been decreased in the above protocols due to the less availability of the neighbors. As we increasing the malicious nodes in the simulation, it decreases the PDR in the TSR and OLSR protocol. The node mobility and availability are also play the vital role in PDR. However, the presence of malicious nodes in the network cannot affect the data transmission and Packet delivery ratio in the proposed method due to avoiding the malicious node from the routing table.

5.6 Measurement of Throughput

In CKR technique, throughput determines the rate at which the data packet received at the destination per unit time. The throughput is measured in terms of Kilobits per second **(**Kbps) and mathematically formulated as follows,

$$Throughput = \frac{Total\ Number\ of\ packets\ received}{Time} \quad (13)$$

From the equation (13), throughput is measured.

Table 8: Throughput in CKR

No. of Nodes	No. of Malicious Nodes	Throughput(Kbps)		
		TSR protocol	OLSR protocol	DSDV with CKR
20	0	1369	1454	2301
20	2	1324	1422	2295
20	4	1246	1347	2265
20	6	1105	1304	2212
20	8	1024	1108	2177
20	10	977	1205	2149
Average throughput		**1174**	**1307**	**2233**

Table 8 describes the comparative result analysis of throughput with respect to the presence of various number of malicious nodes.

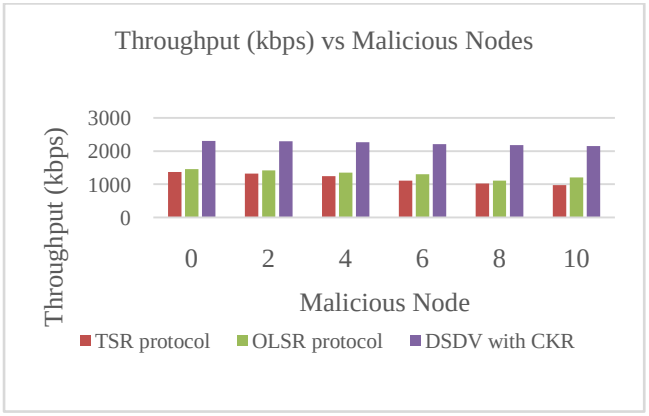

Figure 5: Malicious Nodes vs Throughput

Our proposed authentication scheme detects and restricts the presence of the malicious nodes from the data transmission of the network. The performance and the data theft is avoided in the proposed method, so the throughput of the network is very higher around 2233 kbps in the proposed technique.

VI. CONCLUSION

The proposed method "Coherence key based node authentication scheme" designed for authenticating the mobile nodes in. With the help of proposed authentication scheme, every mobile node has to be authenticated during the

routing table updation. Based on the authentication result, the nodes will be added in the routing table. It rejects the malicious nodes from the data transmission. No node will transmit the data to the non-authenticated or malicious nodes. This method destroys the malicious behaviors from the networks. Hence, The results shows that the proposed scheme produces better results when compared to the existing authentication schemes and existing protocols.

REFERENCES

1. NidhiLal, Shishupal Kumar, Aditya Saxena, Vijay Km. Chaurasiya, "Detection of Malicious Node Behaviour via I-Watchdog Protocol in Mobile Ad Hoc Network with DSDV Routing Scheme", Procedia Computer Science, Elsevier, Volume 49, Pages 264 – 273, 2015.
2. Hui Xia, ZhipingJia, Xin Li, Lei Ju, Edwin H.-M. Sha, "Trust prediction and trust-based source routing in mobile ad hoc networks", Ad Hoc Networks, Elsevier, Volume 11, Issue 7, Pages 2096-2114, September 2013.
3. Shuaishuai Tan, Xiaoping Li, Qingkuan Dong, "Trust based routing mechanism for securing OSLR-based MANET", Ad Hoc Networks, Elsevier, Volume 30, Pages 84–98, July 2015.
4. Suyash Bhardwaj, Swati Aggarwal and ShikhaGoel, "A Novel Technique of Securing Mobile Ad hoc Networks using Shared Trust Model",International Journal of Information and Computation Technology, Volume 3, Issue 9, Pages 909-916, 2013.
5. ErmanAyday, FaramarzFekri, "An Iterative Algorithm for Trust Management and Adversary Detection for Delay-Tolerant Networks", IEEE Transactions on Mobile Computing, Volume 11, Issue 9, Pages 1514 – 1531, 2012.
6. Jan Papaj and LubomirDobos, "Cooperation between Trust and Routing Mechanisms for Relay Node Selection in Hybrid MANET-DTN",Hindawi Publishing Corporation, Mobile Information Systems, Volume 2016, Article ID 7353691, Pages 1-18, 2016.
7. P.Gowthamarayathirumal, C.Chandrasekar, "Service Authentic Trust and Coherence Key Based Secured Routing For Mobile Ad Hoc Networks", IOSR Journal of Computer Engineering (IOSR-JCE) Volume 19, Issue 4, Ver. I, Pages 1-12, Jul-Aug 2017.
8. P.Gowthamarayathirumal, C.Chandrasekar, "Service Authentic Trust and Reputation Scheme for Secured Routing in Mobile Ad Hoc Networks", SIMRJ ISSN: 2455-1511 Vol. II, Issue-IV, Pages 128-140, Apr-May-June 2017.
9. Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs", IEEE Transactions on Industrial Electronics, Volume 60, Issue 3, Pages 1089 – 1098, March 2013.
10. Gautam M. Borkar, A. R. Mahajan, "A secures and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks", Wireless Networks, Springer, Pages1–18, 2016.
11. Ahmad Alomari, "Security Authentication of AODV Protocols in MANETs", Network and System Security, Springer, Pages 621-627, 2013.
12. Jan Papaj and LubomirDobos, "Cooperation between Trust and Routing Mechanisms for Relay Node Selection in Hybrid MANET-DTN",Hindawi Publishing Corporation, Mobile Information Systems, Volume 2016, Article ID 7353691, Pages 1-18, 2016.
13. Briscoe, B., Brunstrom, et all., "Reducing Internet Latency: A Survey of Techniquesand their Merits", IEEE Communications Surveys & Tutorials 18(3), pp.2149–2196 (Q3 2016).

AUTHORS PROFILE

Dr.P. Gowthamarayathirumal has completed M.C.A., M.Phil., Ph.D,SET. Currently he is working as Assistant Professor in Department of Computer Science, Government Arts College, Dharamapuri,TN. He has 4 years of teaching experience and 6 years of research experience. He has published 8 research papers, and attended several conferences and Workshops.

Dr. C. Chandrasekar has completed M.C.A., Ph.D,currently he is working as Professor in Department of Computer Science, Periyar University, Salem,TN. He has 20 years of teaching experience and 16 years of research experience, he has guided 26 Ph.D research Scholars and around 40 M.Phil research Scholars and he has published around 140 journals out of which 75 are scopus indexed and 6 are science indexed journals. He has done a UGC project around 8 lakhs, he is an deputy coordinator for UGC-SAP and sanctioned RS.54.50 lakhs for department of computer Science, Periyar University, He received travel grant from department of Science and Technology and presented a paperin sixth global conference held at Las vigas, USA.research papers, and attended several conferences and Workshops.

Dr.A.Sridhar has completed M.Sc., M.Phil., Ph.D, currently he is working as Assistant Professor in Department of Computer Science, Government Arts College, Dharamapuri,TN. He has 15 years of teaching experience and 10 years of research experience. He has guided around 10 M.Phil research Scholars. He has published 5 research papers, and attended several conferences and Workshops.