IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 4, Ver. IV. (Jul.-Aug. 2017), PP 40-51
www.iosrjournals.org

Service Authentic Trust and Coherence Key Based Secured Routing For Mobile Ad Hoc Networks

[1]P.Gowthamarayathirumal[*], [2]Dr. C.Chandrasekar
[1]*Research Scholar, Department of Computer Science, Periyar University, Salem, TN, India*
[2]*Professor, Department of Computer Science, Periyar University, Salem, TN, India*
Corresponding Author: [1]P.Gowthamarayathirumal

Abstract: *Mobile Ad hoc Networks (MANETs) is a self-organized system which includes of multiple mobile nodescommunicated through a wireless medium. MANETs is weakens to malicious attacks owing to the openness in network topology. Therefore, secured routing techniques are required for reliable data packet transmission. A Service Authentic Trust and Coherence key based Routing (SAT-CKR) technique is proposed for providing security in MANETs during communication. SAT-CKR technique is designed to identify the optimal routing path that decides the qualitative of the path (i.e.) both reliable and energy conserving. Initially, The SAT-CKR technique estimates the trust values for every mobile node in network based on the energy, mobility, and trust rate. With help of measured trust value, then SAT-CKR technique effectually detects the malicious attacksnode in MANETs. This in turn assists for SAT-CKR technique to improve the attack detection rate and to reduce the energy utilization.Next, SAT-CKR technique constructs coherence key for each mobile node in network with objective ofimproving communication security. Withhelp of formulatedcoherence key, SAT-CKR technique select the optimal path through authenticating the mobile nodes. This helps for SAT-CKR technique to enhance the communication security and to lessen the routing overhead in MANETs. The efficacy of SAT-CKR technique is evaluated in terms of attack detection rate, energy consumption, routing overhead and communication security level.The simulation results expose that the proposed SAT-CKR techniqueis able to enhance the attack detection rateand also minimizes the energy consumption when compared to state-of-the-art works.*

Keywords: *Mobile Ad hoc NETworks (MANETs), mobile nodes, malicious attacks,trust value, coherence key, optimal path*

Date of Submission: 17-07-2017 Date of acceptance: 29-07-2017

I. Introduction

A Mobile Adhoc Networks (MANETs) is a set of mobile nodes which are connected with each other through the wireless links.Secure routing isasignificant issue in MANETs. Theanalysis of ad hoc networks isusing the cooperation and trust betweenmobile nodes. Therefore, it is important to estimate trustworthiness of nodesand to reduce the effects of malicious attacks in routing and to improve security in ad hoc networks. Besides, the trust value evaluation also reduces the packet loss rate due to malicious attacks node.

Manyresearch works isintended for achievingsecured routing in MANETs. For example, Trust-based Source Routing (TSR) protocol was presented in [1] to select the shortest route and to fulfill the security requirement of data packets transmission in MANETs.Besides, TSR protocolincreases packet delivery ratio and diminishes average end-to-end latency. But, securing communication between the mobile nodes is remained unsolved.Fuzzy Petri NeT based Optimized Link State Routing (FPNT-OLSR) protocol was designed in [2] to select higher trust path among all possible paths in MANETs. TheFPNT-OLSR identifies malicious or compromisednodes in network. However, attack detection performance was not efficient.

A trust based model was designed in [3] to measure the trust level of nodes and to perform secured routing in MANETs.However, secure data transmission rate was poor.An iterative algorithm was developed in [4] for trust management and performing adversary detectionin delay-tolerant networks. But, attack detection rate was not at required level.The cooperation between trust and routing mechanism was intended in [5] to elect reliable and secure the data transmission through selecting malicious nodes.

An enhanced adaptive acknowledgement model was designed in [6] 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 [7] 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 [8] to enhance the security among the nodes in MANETsthrough the authentication. However, it does not present more security service.

A Trust-based routing method using a mobility-based clustering approach was intended in [9]toidentify the trustworthy route from the source node to the destination nodewith aid of end-to-end trust calculation.But, energy utilization was higher.Trust similarity based routing scheme was developed in [10] to enhance the performance ofreliable packet forwarding over multi-hop routes in the occurrence of possible malicious behaviors in MANETs. However, routing overhead and data loss rate was higher.

In order to solve the existing issues, Service Authentic Trust and Coherence key based Routing (SAT-CKR) technique is proposed. The major contribution of SAT-CKRtechnique is formulated as follows,

- To improve the performance of malicious attack detection in MANETs with minimum energy consumption, trust value of mobile is determined inSAT-CKR technique. The trust value of mobile node is calculated using the node energy, mobility and trust rate. TheSAT-CKR technique assigns threshold trust value for identifying the malicious node in network. Thus, mobile nodes with higher trust values are considered as optimal node for reliable data transmission. Besides, mobile nodes with low trust values are considered as malicious attack node.
- To improve the security level of communication in MANETs with minimum routing overhead, coherence key is generated in SAT-CKR technique. By using the coherence key, SAT-CKR technique authenticates the mobile nodes in network for securing the communication between them. The mobile node authentication is performed through matching their coherence key. Thus, SAT-CKRtechnique selects the optimal path for transmitting data with reduced data packet loss rate.

The rest of paper isordered as follows. Section 2 explains a Service Authentic Trust and Coherence key based Routing (SAT-CKR) technique with the help of architecture diagram. Section 3 and Section 4 describes the experimental settings and details performance analysis with the assist of parameters. Section 5 portrays the related works. Finally, Section 6 concludes this paper.

II. Service Authentic Trust And Coherence Key Based Secured Routing

Secure data transmission against the malicious attacks is aconsiderable issue in MANETs.The malicious behavior of nodes minimizes the node trust level whichleads to an insecure data transmission in MANETs. Besides, the malicious attack node utilizes the more amountof energy for transmitting the data packets.Thisreducesthe lifetime of network. Therefore, there is a requirement for new secured routing technique in order to improve the attack detection rate and to reduce the energy utilization of data transmission in MANETs. In order to overcome the above mentioned limitations, Service Authentic Trust and Coherence key based Routing (SAT-CKR) technique is designed.

The SAT-CKR technique determines the trust values for each mobile nodein order to detect the malicious attack nodes in network. In SAT-CKR technique,the trust value of the mobile node is estimated based on the energy, mobility,and trust rate. This helps for proposed SAT-CKR techniqueto efficientlyidentifythe malicious node inMANETs with higher attack detection rate. In addition, SAT-CKR techniqueformulatescoherence key for each mobile nodein network to achieve secured communication between the mobile nodes with reduced routing overhead and to select the optimal path for secured routing. The overall architecture diagram of SAT-CKR technique forperforming secured routing is shown in below Figure 1.

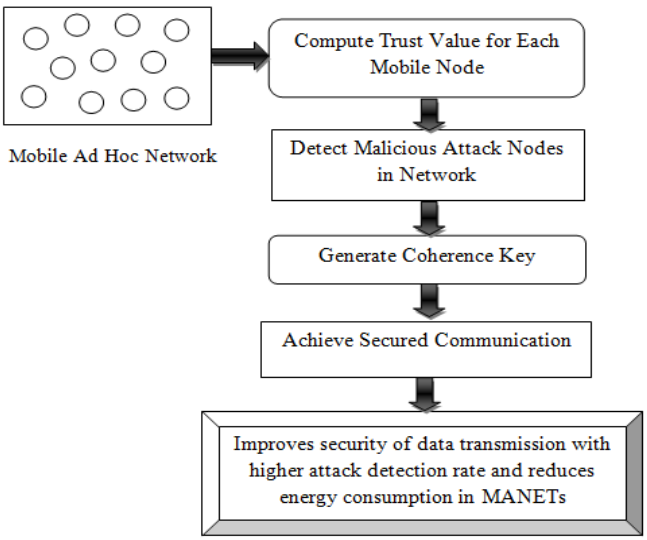

Figure 1 Architecture Diagram of Service Authentic Trust and Coherence Key Based Secured Routing For MANETs

As shown in Figure 1, SAT-CKR technique initially measures trust value for each mobile node in MANETs through considering the energy, mobility, and trust rate of mobile nodes. With the help of determined trust value of mobile nodes, then SAT-CKR technique significantly identifies the malicious attack nodes in network. Thus, SAT-CKR technique enhances the attack detection rate and also minimizes the energy consumption of data packet forwarding. Finally, SAT-CKR technique creates the coherence key with objective of enhancing communication security between the mobile nodes in MANETs. This helps for SAT-CKR technique to identify the best path for transmitting the data packets fromsource node to destination.Therefore, SAT-CKR technique increases the secure data transmission rate and reduces routing overhead in MANETs. The elaborate description about SAT-CKR technique is explained in below subsections.

2.1 Service Authentic Trust Based Malicious Attack Node Detection

Trust is a one of the significant factor tobe consideredforachieving secured routing in MANETs. The trust value is used for node authentication, access control and performing trust routing. ThereforeSAT-CKR technique evaluates trust value in order tofind out the malicious attack nodes in network and to improve theperformance of routing in MANETs with minimum energy utilization.In SAT-CKR technique, the trust value of the mobile node is calculated based on the energy, mobility, and trust rate.The following diagram shows the process involved in service authentic trust based malicious node detection.

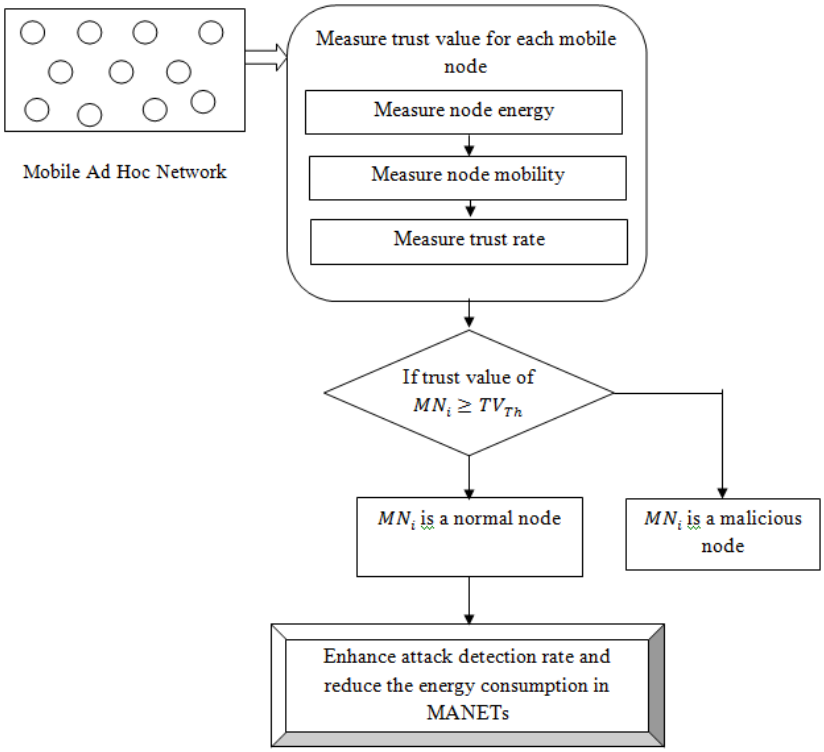

Figure 2 Process of Service Authentic Trust Based Malicious Node Detection for Achieving Secured Routing in MANETs

As shown in Figure 2, SAT-CKR technique initially calculates trust value for all the mobile nodes in networks based on energy, mobility and trust rate. Next, trust value for all the mobile nodes is compared with threshold trust value 'TV_{Th}'. Ifthetrust value of the mobile nodes is greater than theTV_{Th}, then the node is considered as normal. Otherwise the node is considered as malicious. This assists for SAT-CKR technique to increase the attack detection rate in MANETs. This also helps for SAT-CKR technique to choose the optimal mobile node for data packet transmission.

In trust value determination, node energy value is considered for selecting the optimal mobile node with higher residual energy and to reduce the energy consumption of data packet transmission.Selection of higher energy node avoids the path breakdowns during the data packets transmission. The residual energy measures the remaining energy in the mobile node.Therefore, the residual energy of mobile node (RE_{MN_i}) iscalculated using below mathematical representation,

$$RE_{MN_i} = IE_{MN_i} - (N_S \times T_P) \quad (1)$$

From the equation (1), energy value of mobile node is measured where as IE_{MN_i} designates an initial energy of a mobile node before the route discovery process and N_S indicates the number of bytes broadcasted. Here T_P denotes a transmission power (i.e. energy) required per byte.Besides, the mobility of the nodes is considered to select the optimal mobile nodes with higher mobility and to enhance the routing performance. The performance of MANETsis measured in terms of throughput, latency, and scalability which areinterconnected to the capability of the routing in adapting to changes in the network topology owingto mobility of the nodes. Thus, determination of node mobility is important for performing topology aware routing in MANETs. Therefore, the mobility of nodes is estimatedwith help of below mathematical formula,

$$M_{MN_i}(t) = \frac{1}{N}\sum_{i=0}^{N-1} M_i(t) \quad (2)$$

From the equation (2), Nrepresents the number of mobile nodes in network whereas $M_i(t)$indicates the relative movements of other nodes as seen by mobile node i which is mathematically estimated as,

$$M_i(t) = \frac{1}{N-1}\sum_{j=0}^{N-1} \frac{d}{dt} F(d_{ij}(t)) \quad (3)$$

Thus, $M(t)$presents the average movement of mobile nodes in the network at time t. With the aid of computednode mobility, the mobile node with higher speed is selected as optimal for performing topology aware routing in MANETs.

In addition, the trust rate of mobile nodes is calculateddepends on the number of normal communication service offered by nodes in MANETs. Thus, the trust rateis defined as the differentiation between number of data packets forwarded and thenumber of data packets dropped to the total number of data packets broadcasted to neighboring mobile nodes in network. Here, the data packets forwarded is estimated as the percentages of data packets is initiated from the mobile node MN_i that was transmitted by mobile node MN_j over the total number of data packets distributed to mobile node MN_j. Therefore, the data packets forwarded is measured as,

$$\text{DPF} = \frac{DPF(MN_j)}{DP_i} \quad (4)$$

From the equation (4), $i, j = 1,2,..n.$ here, $DPF(MN_j)$indicates the number of data packets forwarded by the mobile node MN_jwhereas DP_irepresents the number of data packets received by the mobile node MN_j. Further, the data packets dropped measures percentages of the packets that were dropped over the total number of data packets transmitted to the mobile node MN_j. Therefore, the data packets dropped is determined as,

$$\text{DPD} = \frac{DPD(MN_j)}{DP_i} \quad (5)$$

From the equation (5), $i, j = 1,2,..n$ whereas $DPD(MN_j)$represents the number of data packets dropped by the mobile node MN_jandDP_i represents the number of data packets received by the mobile node MN_j. Thus, the trust rate of mobile nodes TR_{MN_i} is evaluated using below mathematical expression,

$$TR_{MN_i} = \frac{TDP_S - (DPF - DPD)}{TDP_S} \quad (6)$$

From the equation (6),TDP_S represents the total number of data packets send to particular mobile node. With help of measured node energy, mobility and trust rate, finally SAT-CKR technique calculates the trust value of mobile node TV_{MN_i}which is mathematically formulated as,

$$TV_{MN_i} = RE_{MN_i} + M_{MN_i}(t) + TR_{MN_i} \quad (7)$$

From the equation (7), trust value for each mobile node in network is measured.With the aid of determined trust value of the mobile nodes, then SAT-CKR technique efficiently discovers the malicious attack nodes and also choose optimal mobile nodefortransmitting the data packets from the source to the destination nodes in network.This in turn helps for improving the security of data packet transmissions with higher attack detection rate.

The algorithmic process of service authentic trust based malicious node detection is shown in below.

// Service Authentic Trust Based Malicious Node Detection Algorithm
Input: Mobile Nodes '$MN_i = MN_1, MN_2, \ldots, MN_n$', Source Node SN, Destination Node DN, Data Packets '$DP_i = DP_1, DP_2, \ldots, DP_n$'
Output: ImprovesAttack Detection Rate And Reduces Energy Consumption for Data Transmission
Step 1:Begin
Step 2:For each Mobile Node 'MN_i'
Step 3:If (MN_i is neighbour to MN_j node)
Step 4: Evaluate energy value of node using (1)
Step 5: Compute mobility of node using (2)
Step 6: Determinedata packet forwarding rate using (4)
Step 7: Computedata packet drop rate using (5)

Step 8: Estimatetrust rate of node using (6)
Step 9: Calculate trust value using (7)
Step 10:If ($TV_{MN_i} > TV_{Th}$) then
Step 11: MN_i isanormal node
Step 12:Else
Step 13: MN_i isamalicious node
Step 14:End if
Step 15: End if
Step 16: End for
Step 17: End

Algorithm 1Service Authentic Trust Based Malicious Node DetectionforSecured Routing in MANETs

The above Algorithm 1 describes the process of service authentic trust for detectingthe malicious attack nodeand achieving secured routing in MANETs.The Service Authentic Trust Based Malicious Node Detection algorithm initially calculates thenode energy, mobility, trustrate with the objective of measuring the trust value for each mobile node in network. Subsequently, this Service Authentic Trust Based Malicious Node Detection algorithm evaluates the trust value for all mobile nodes in MANETs with aiming at detecting the malicious attacks. Finally, Service Authentic Trust Based Malicious Node Detection algorithm compares the trust value of each mobile node with predefined threshold in order to find out the malicious attacks in network. If the trust value of mobile nodes is greater than the TV_{Th}, then the mobile node is marked as normal. Otherwise the mobilenode is marked as malicious attack. Therefore, SAT-CKR technique enhances the attack detection rate of MANETs in an efficient manner. This also helps for SAT-CKR technique to select the optimal mobile node with higher trust value for performing reliable data packet transmission in MANETs with minimum energy consumption.

After choosing the optimal mobile node for transmitting the data packets to destination from the source, SAT-CKR technique creates coherence key in order to attain secure the communication between the mobile nodes and to minimize the routing overhead in MANETs. The detailed explanation about coherence key generation process is described in next section.

2.2 Coherence Key Based Node Authentication

TheSAT-CKR techniqueconstructs the coherence key for each mobile node in MANETs with aiming at improving the communication security.The coherence key is a general key which is created for authenticating all mobile node in MANETs while a performing the data transmission. With help of formulated coherence key, SAT-CKR technique authenticates the each mobile nodes in network for transmitting the data.The process involvedin coherence key based node authenticationis demonstrated in below Figure 3.

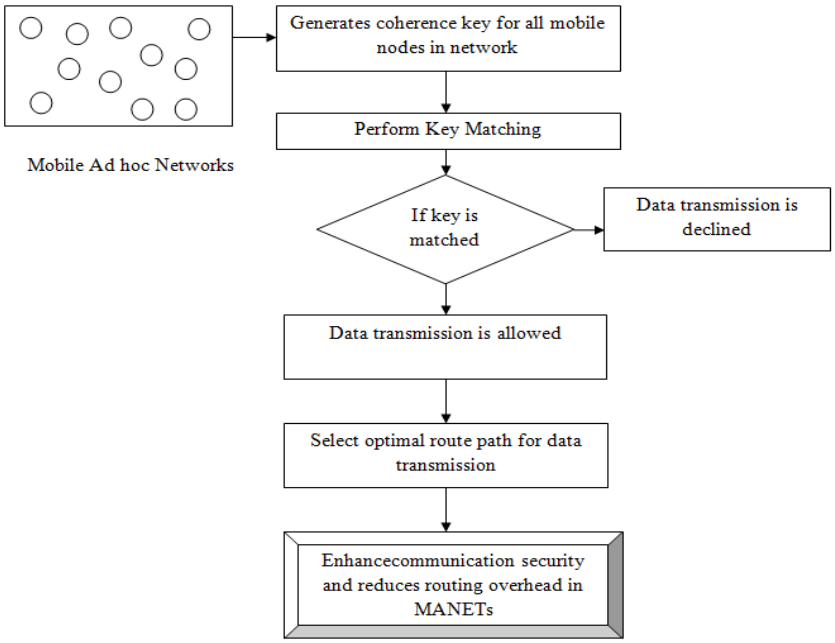

Figure 3 Process of Coherence Key Based Node Authentication for Secured Communication in MANETs

As illustrated in Figure 3, at first SAT-CKR technique makes coherence key for all mobile nodes in network with objective of improvingthe communication security. Next, SAT-CKR technique authenticates the every mobile node in route path throughperforming key matching. If the coherence key of both nodes is matched, then the data transmission through neighbouring node is allowed. Otherwise, the data transmission through neighbouring node isdeclined.

TheSAT-CKR technique generates coherence key for every mobile node in network using below mathematical expression,

$$Coherence\ Key = \sum_{i=0}^{n} CohK_i\ (MN_i) \quad (8)$$

From the equation (8), coherence key $CohK_i$ is constructed for mobile nodesMN_i. Before transmitting the data, the source nodes authenticates neighbouring mobile node in route path in order to achieve higher communication security by matching coherence key which is mathematically formulated as below,

$$CohK_i(MN_i) == CohK_i(MN_j) \quad (9)$$

From the equation (9), $CohK_i(MN_i)$ indicates the coherence key of source node whereas $CohK_i(MN_j)$ represents the coherence key of neighbouring node in network. If $CohK_i$ of both mobile nodes is identical, then the SAT-CKR technique performs the data transmission via neighbouring node. Otherwise, the data transmission process via neighbouring node is declined.The Coherence Key Based Node Authentication Algorithm is shown in below.

//Coherence Key Based Node Authentication Algorithm
Input: Mobile nodes'$MN_i = MN_1, MN_2, MN_3 \ldots MN_n$', Source Node SN_i, Destination Node $DN_i$and Coherence Key $CohK_i$, '$DP_i = DP_1, DP_2, \ldots`, DP_n$'
Output: Improves communication security level and reduce routing overhead
Step 1: Begin
Step 2: For each mobile node MN_i
Step 3: create Coherence key CK_i
Step 4: **If** (MN_j is neighbour to the MN_i th node) then carry out key matching
Step 5: **If** ($CohK_i(MN_i)$ ==$CohK_i(MN_j)$) then
Step 6: allow data transmission through neighboring node MN_j
Step 7:Else
Step 8: data transmission through neighboring node MN_j is declined
Step 9:End if
Step 10: Authenticates all neighboring mobile nodes in route until data packets reaches its destination node
Step 11:End if
Step 12: Endfor
Step 13:End

Algorithm 2 Coherence Key Based Node Authentication

By using the above algorithmic process, SAT-CKR technique efficiently improves the security level of communication by authenticating the each mobile node in MANETs using coherence key. This alsohelps for SAT-CKR technique to reduce the routing overhead in an effective manner.

III. Simulation Settings

In order to analyze the performance of proposed method, Service Authentic Trust and Coherence key based Routing (SAT-CKR) techniqueis implemented in NS-2 simulator with the network area of 1000*1000 m. In SAT-CKR technique, number of mobile nodes taken for conducting the experimental works is 500. Besides,SAT-CKRtechnique is used Destination Sequence Based Distance Vector (DSDV) as routing protocol for simulation work. The simulation parameters employed for experimental work is exposed in below Table 1.

Table 1 Simulation Parameters

Parameter	Value
Network simulator	NS 2.34
Protocols	DSDV
Network range	1000 m * 1000 m
Simulation time	45 ms
Number of mobile nodes	50, 100, 150,200,250,300,350,400,450,500
Number of Packets	10,20,30,40,50,60,70,80,90,100
Mobility speed	0-20 m/s
Pause time	15 ms
Mobility model	Random Way Point Model
Transmission range	300m
Packet Size	100-1000 bytes

Theperformance of proposed SAT-CKRTechnique is determined with different sizes of data along with multiple malicious adversaries for attaining higher communication security in MANETs. The effectiveness ofSAT-CKRTechnique is compared against with the existing Trust-based Source Routing (TSR) protocol [1] and Fuzzy Petri NeT based Optimized Link State Routing (FPNT-OLSR) protocol [2]. The performance of SAT-CKRTechnique is measured in terms of energy consumption, attack detection rate, routing overhead and communication security level.

IV. Results And Discussions

The performance result of SAT-CKR techniqueis compared against with the existing two methods namelya Trust-based Source Routing (TSR) protocol [1] and Fuzzy Petri NeT based Optimized Link State Routing (FPNT-OLSR) protocol [2] respectively. The efficiency of SAT-CKR techniqueis determined along with the following metrics with the assist of tables and graphs.

4.1 Measurement of Attack Detection Rate

In SAT-CKR technique, the attack detection rate measures the ratio of differentiation between the total number of nodes and the number of nodes identified as malicious in the network to the total number of mobile node. The Attack Detection Rate (ADR) is mathematically represented as follows,

$$\text{ADR} = \frac{\text{total number of nodes} - \text{number of nodes identifed as malicious}}{\text{total number of nodes}} * 100 \quad (10)$$

From the equation (10), the attack detection rate is measured. The attack detection rate is measured in terms of percentages (%). While the attack detection rate is more, the method is said to be more effectual.

Table 2 Tabulation for Attack Detection Rate

Number of Mobile Nodes	Attack Detection Rate (%)		
	TSR protocol	FPNT-OLSR protocol	SAT-CKR technique
50	71.24	79.15	90.25
100	73.62	81.35	91.92
150	74.98	83.65	92.65
200	77.16	85.19	93.05
250	79.26	86.36	93.85
300	81.22	88.16	94.58
350	83.45	90.05	95.12
400	86.74	91.15	96.62
450	88.18	92.88	97.53
500	90.14	93.65	98.75

Table 2 depicts the result analysis of attack detection rate based on the different number of mobile nodes in the range of 50-500 using three methods. While considering the 300 number of mobile nodes in the network, proposed SAT-CKR techniqueattains94 % attack detection rate whereas the existing TSR protocol [1] and FPNT-OLSR protocol [2] attains 81% and 88 % respectively. Hence, the attack detection rate using SAT-CKR techniqueis higher when compared to other existing works.

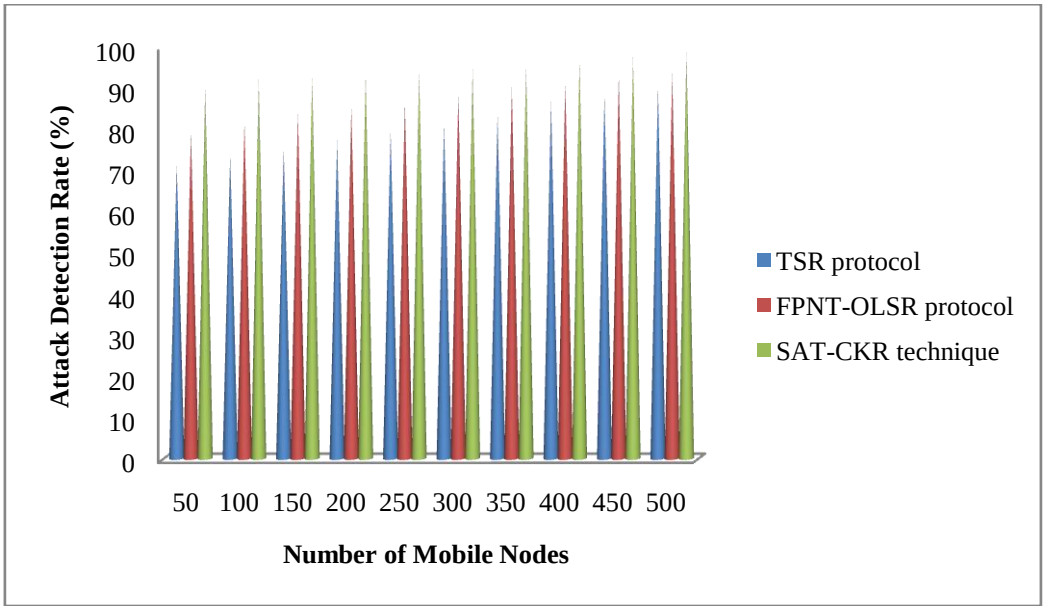

Figure 4 Measurement of Attack Detection Rate versus Number of Mobile Nodes

Figure 4 shows the impact of attack detection ratewith respect to dissimilar numbers of mobile nodes in the range of 50-500. As illustrated in figure, the proposed SAT-CKR techniqueprovides higherattack detection ratewhen compared to existingTSR protocol [1] and FPNT-OLSR protocol [2] respectively. Further, while increasing the number of mobile nodes for performing data transmission, the attack detection rateis also gets increased using all the three methods. But comparatively, the attack detection rateusing proposed SAT-CKR techniqueis higher when compared to other existing works. This is because of the application of service authentic trust based malicious node detection algorithm in SAT-CKR technique where it determines the trust values for each mobile node based on its energy, mobility and trust rate.With aid of measured trust value, then service authentic trust based malicious node detection algorithm significantlyidentifies the malicious attack node presence in MANETs. This in turn helps for enhancing the attack detection rate in an effective manner. Therefore, SAT-CKR technique increase the attack detection rate in MANETs by 18 % when compared to TSR protocol [1] and 9 % when compared to FPNT-OLSR protocol [2] respectively.

4.2 Measurement of Energy Consumption

In SAT-CKR technique, Energy Consumption (EC) determines the amount of energy utilized for successfully broadcasting the data packets to destination node from the source. Hence, energy consumption is measured as the product of number of mobile nodes, power used in terms of watts and time consumed in terms of seconds. The energy consumption is mathematically expressed as,

$$EC = Number\ of\ mobile\ nodes * Power * Time \quad (11)$$

From the equation (11), the energy utilization for reliable data transmission is evaluated. The energy consumption is measured in terms of Joules (J).When the energy consumption is lower, the method is said to be more efficient.

Table 3 Tabulation for Energy Consumption

Number of Mobile Nodes	Energy Consumption (J)		
	TSR protocol	FPNT-OLSR protocol	SAT-CKR technique
50	31.5	25.3	10. 2
100	36.3	27.6	13.5
150	41.5	31.2	15.8
200	48.2	35.7	19.4
250	57.6	43.5	22.3
300	64.1	51.2	25.6
350	68.5	55.4	31.1
400	71.4	59.3	38.6
450	73.2	65.9	42.5
500	76.7	71.8	49.4

Table 3 portrays the result analysis of energy consumption for achieving reliable data transmission with respect to the diverse number of mobile nodes in the range of 50-500 using three methods. While considering the 400 number of mobile nodes for performing simulation, proposed SAT-CKR techniqueutilizes38.6Jenergy for reliable data transmission whereas the existingTSR protocol [1] and FPNT-OLSR protocol [2] utilizes 71J and 59J respectively. Thus, the energy consumption using SAT-CKR technique is lower when compared to other existing works.

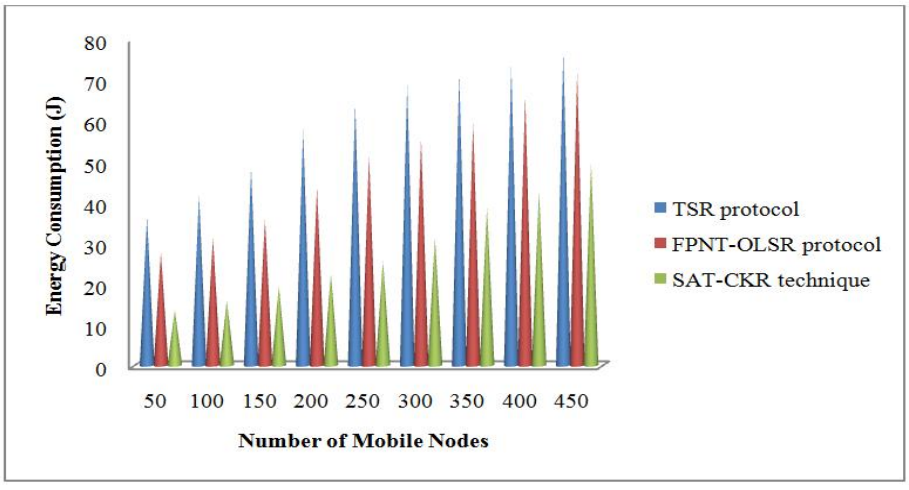

Figure 5 Measurement of Energy Consumption versus Number of Mobile Nodes

Figure 5describes the impact of the energy utilization forachieving secure data transmission based on thediverse numbers of mobile nodes in the range of 50-500. As demonstrated in figure, the proposed SAT-CKR techniqueprovides better energy consumption for the reliable data transmission in MANETs when compared to existingTSR protocol [1] and FPNT-OLSR protocol [2] respectively. In addition, while increasing the number of mobile nodes for data packet transmission, the energy consumptionis also gets increased using all the three methods. But comparatively, the energy consumptionusing proposed SAT-CKR techniqueis lower when compared to other existing works. This is owing to the application of service authentic trust based malicious node detection algorithm in SAT-CKR technique in which it find outs the trust values for each mobile node based on its energy, mobility and trust rate. This in turn helps for SAT-CKR technique to choose the higher residual energy mobile node for data transmission. The discovery of higher residual energy mobile node assists for reducing the energy utilization in a significant manner. As a result,proposed SAT-CKR technique minimizes the energy consumption of data transfer in MANETs by 55 % when compared to TSR protocol [1] and 45 % when compared to FPNT-OLSR protocol [2] respectively.

4.3 Measurement of Routing Overhead

In SAT-CKR technique, the routing overhead measures the amount of time taken to broadcast data packets from the source to destination node in network. The routing overhead is evaluated in milliseconds (ms) and it is formalized as below,

$$Routing\ Overhead = \sum_{i=1}^{n} MN_i * Time(data\ packet\ transmission) \quad (12)$$

From the equation (12), the routing overhead of SAT-CKR technique is measured where MN_irepresents number of mobile node, $Time(data\ packet\ transmission)$ represents the amount of time taken for single node to broadcasts the data packet. While the routing overhead is lower, the method is said to be more effectual.

Table 4 Tabulation for Routing Overhead

Number of Mobile Nodes	Routing Overhead (ms)		
	TSR protocol	FPNT-OLSR protocol	SAT-CKR technique
50	36	31	18
100	40	36	25
150	47	41	33
200	50	47	39
250	59	55	45
300	65	61	53
350	72	69	61
400	79	76	68
450	87	84	75
500	94	90	88

Table 4 reveals the result analysis of routing overhead with respect to the variousnumbers of mobile nodes in the range of 50-500 using three methods. While taking the 350 mobile nodes for conducting the simulation, proposed SAT-CKR techniqueobtains61msrouting overhead whereas the existing TSR protocol [1] and FPNT-OLSR protocol [2] obtains 79 ms and 76 msrespectively. As a result, the routing overhead using SAT-CKR technique is lower when compared to other existing works.

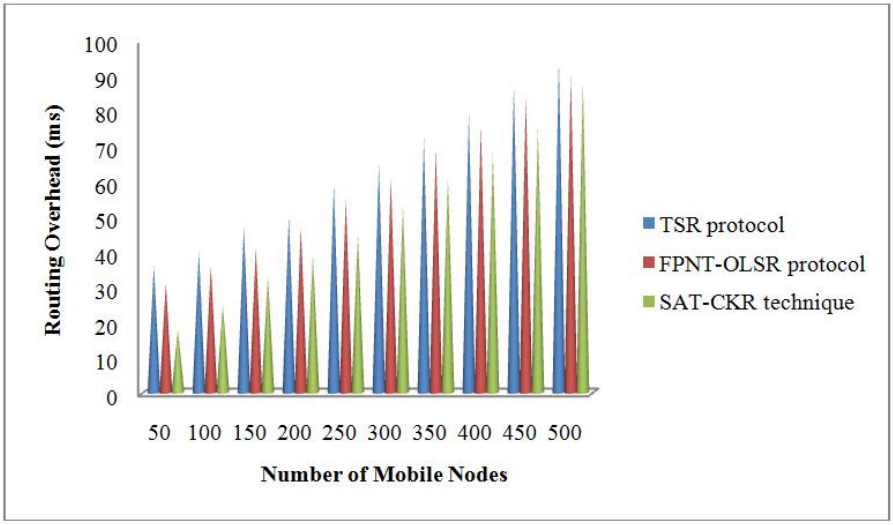

Figure 6 Measurement of Routing Overhead versus Number of Mobile Nodes

Figure 6demonstrates the impact of routing overhead based ondiverse numbers of mobile nodes in the range of 50-500. As exposed in figure, the proposed SAT-CKR techniqueprovides minimum routing overhead when compared to existingTSR protocol [1] and FPNT-OLSR protocol [2]. Furthermore, while increasing the number of mobile nodes for carried outing the simulation, the routing overhead is also gets increased using all the three methods. But comparatively, the routing overhead using proposed SAT-CKR techniqueis lower as compared to other existing work. This is due to the application ofCoherence Key Based Node Authentication Algorithm in SAT-CKR technique.With the support of this algorithmic process, proposed SAT-CKR technique authenticates every mobile node in network in order to securing the communication between the mobile nodes during the data transmission. Thus, the SAT-CKR technique selects the secured node in network for transmitting the data packets to destination node from the source. This assists for reducing the routing overhead in MANETs. As a result, proposed SAT-CKR technique minimizes the routing overhead by 23 % when compared to TSR protocol [1] and 18 % when compared to FPNT-OLSR protocol [2] respectively.

4.4 Measurement ofCommunicationSecurity Level

In SAT-CKR technique,communication security level (CSL) is evaluated in terms of packet loss rate. Thus, communication security level is measured as the ratio of number of data packet dropped to the total number data packets broadcasted. The mathematical formula for communication security level isshown in below,

$$CSL = \frac{number\ \ packets\ \ dropped}{total\ \ number\ \ of\ packet\ s\ transmitted} * 100 \quad (13)$$

From the equation (13), security level of communication is determined. When the data packet loss rate is lower, the proposedSAT-CKR technique attains higher communication security level. When the security level of communication is more, the method is said to be more effective.

Table 5 Tabulation for CommunicationSecurity Level

Number of data Packets	CommunicationSecurity Level (%)		
	TSR protocol	FPNT-OLSR protocol	SAT-CKR technique
10	42.35	29.25	10.22
20	45.87	31.05	11.56
30	46.91	32.81	13.45
40	48.62	34.61	15.36
50	51.36	37.59	18.17
60	52.14	40.12	20.14
70	55.78	41.94	21.86
80	56.87	43.14	23.54
90	58.19	45.96	26.98
100	61.05	48.16	30.11

Table 5explains the result analysis of communication security level with respect to the different numbers of data packets using three methods.While considering the 50data packets for transmission, proposed SAT-CKR techniqueacquires 18.17 %packet loss rate whereas the existing TSR protocol [1] and FPNT-OLSR protocol [2] acquires 52.14 % and 37.59 % respectively. Therefore, the security level of communication usingSAT-CKR technique is higher when compared to other existing works.

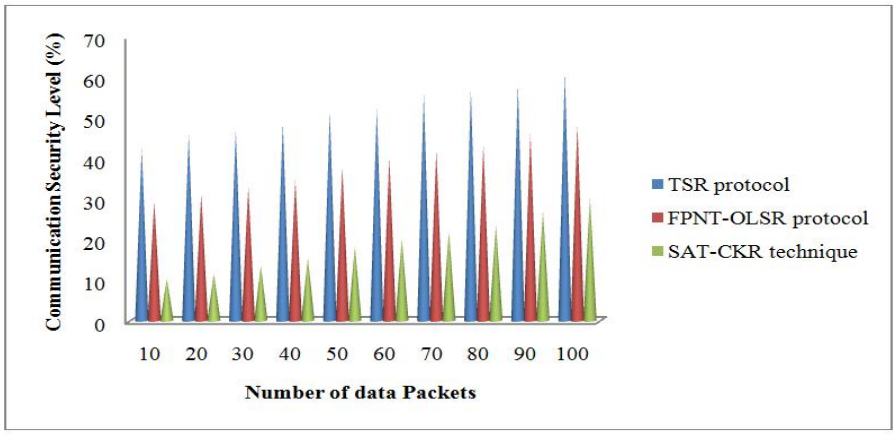

Figure 7 Measurement of communication security level versus Number of Data Packets

Figure 7 exhibits the impact of communication security levelbased on different number of data packets using three different methods. As revealed in figure, the proposed SAT-CKR technique provides highercommunication security levelwhen compared to existing TSR protocol [1] and FPNT-OLSR protocol [2]respectively. As well, while increasing the number of data packets for conducting the simulation, the communication security levelis also gets increased using all the three methods. But comparatively, the communication security levelusing proposed SAT-CKR techniqueis higherwhen compared to other existing work. This is because of the usage of Coherence Key Based Node Authentication Algorithm in SAT-CKR technique. By using this algorithmic process, proposed SAT-CKR technique certifieseach mobile node in network with objective of achieving higher communication security between the mobile nodes while performing the data transmission. This helps for minimizing the data loss rate in MANETs. The reduction of data loss rate considerably increases the security level of communication in an effectual manner. Therefore, proposed SAT-CKR technique enhance the security level of communication in MANETs by 64 % when compared to TSR protocol [1] and 52 % when compared to FPNT-OLSR protocol [2] respectively.

V. Related Works

A multi-attribute trust framework was designed in [11] for enhancing the security of routing in MANETsby means ofremoving malicious attack nodes in the routing paths.However, attack detection rate was not sufficient which lacks security level.A Friendship-based AODV routing protocol was intended in [12] for performing the secured data transmissionin MANETs. But, the routing overhead increased in this routing protocol. A Trust based Certificate Revocation for Secure Routing (TCRSR) protocol was presented in [13] in order tominimize the vulnerabilitiesof attack nodes and to enhance the security of MANETs using trust value. However, the routing overhead was more which increases the energy utilization of data transmission. An authenticated anonymous secure routing (AASR) was used in [14] to reduce thepossible active attacks in route pathusing a group signature. However, the different adversary attack in MANETs was not efficiently detected which reduces the attack detection rate.

Unified trust management scheme was designed in [15] to improve the security of MANETs in which reasoning theory is used to estimate the trust of nodes.But, communication security was remained unaddressed. An ID based Secure AODV routing protocol was intended in [16] for improving the security of routing and route maintenance process against the attacks. Though, establishing secure communication was remained unsolved.A trusted routing protocol was presented in [17] to avoid malicious nodes while performing the route discovery and to improve the MANETs security. But, the energy utilizationwas remained unsolved. A secure for BeeAdHoc framework was designed in [18] based on fuzzy set theory to remove the diverse types of attacks and to accomplish secure routing in MANETs. However, this framework takes more energy consumption for transmitting the data.A Secure Trust Based Dynamic Source Routing was intended in [19] tochooseabest route path and to lessen the packet loss caused through malicious nodes in MANETs. However, the data loss rate was higher. The survey of diverse routing protocols developed for discovering the malicious activities and the secured data transmission in MANETs was analyzed in [20].

VI. Conclusion

An efficient Service Authentic Trust and Coherence key based Routing (SAT-CKR) technique is developed with objective of improving security in MANETs during communication. At first, The SAT-CKR technique evaluates the trust values for all mobile nodes in network depends on the energy, mobility, and trust rate. Subsequently, SAT-CKR technique discovers the malicious attacks node in MANETs using determined trust value which resulting in improved attack detection rate and reduced the energy consumption. After that, SAT-CKR technique makes coherence key for each mobile node in network. Finally, SAT-CKR technique chooses the optimal path by means of authenticating the mobile nodes using generated coherence key. Therefore, SAT-CKR technique increases the communication security of MANETs with low routing overhead. The effectiveness of SAT-CKR technique is test with the parameter such asattack detection rate, energy consumption, routing overhead and communication security level. With the simulations carried out for SAT-CKR technique, it is observed that the attack detection rateaffords more precise results for discovering the malicious adversaries in MANETs when compared to state-of-the-art works. The simulation results illustrates that SAT-CKR technique is offers better performance with an enhancement of attack detection rate and reduction of energy utilizationwhen compared to the state-of-the-art works.

References

[1] Hui Xia, Zhiping Jia, 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

[2] 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

[3] Suyash Bhardwaj, Swati Aggarwal and Shikha Goel, "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

[4] Erman Ayday, Faramarz Fekri, "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

[5] Jan Papaj and Lubomir Dobos, "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

[6] 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

[7] 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

[8] Ahmad Alomari, "Security Authentication of AODV Protocols in MANETs",Network and System Security, Springer, Pages 621-627, 2013

[9] Keyvan RahimiZadeh and Peyman Kabiri, "Trust-based routing method using a mobility-based clustering approach in mobile ad hoc networks",Security and Communication Networks, WilleyPublications, Volume7, Issue11, Pages 1746–1763, November2014

[10] Jian Wang, Yanheng Liu, YuJiao, "Building a trusted route in a mobile ad hoc network considering communication reliability and path length",Journal of Network and Computer Applications, Elsevier,Volume 34, Issue 4, Pages 1138-1149, July 2011

[11] Muhammad Saleem Khan, Majid Iqbal Khan, Saif-Ur-Rehman Malik, Osman Khalid, Mukhtar Azim and Nadeem Javaid, "MATF: a multi-attribute trust framework for MANETs",EURASIP Journal on Wireless Communications and Networking, Pages 1-17, 2016,

[12] Tameem Eissa, Shukor Abdul Razak, Rashid Hafeez Khokhar, Normalia Samian, "Trust-Based Routing Mechanism in MANET: Design and Implementation",Mobile Networks and Applications, Volume 18, Issue 5, Pages 666–677, October 2013

[13] Banoth Rajkumar, G. Narsimha, "Trust Based Certificate Revocation for Secure Routing in MANET",Procedia Computer Science, Elsevier, Volume 92, Pages 431–441, 2016

[14] Wei Liu and Ming Yu, "AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments", IEEE transactions on vehicular technology, Volume 63, Issue 9, Pages: 4585 – 4593, 2014

[15] Zhexiong Wei, Helen Tang, F. Richard Yu, Maoyu Wang, Peter Mason, "Security Enhancements for Mobile Ad Hoc Networks with Trust Management Using Uncertain Reasoning",IEEE Transactions on Vehicular Technology,Volume 63, Issue 9, Pages 4647 – 4658, 2014

[16] Waleed S. Alnumay and Uttam Ghos, "Secure Routing and Data Transmission in Mobile Ad Hoc Networks", International Journal of Computer Networks & Communications (IJCNC) Volume 6, Issue 1, Pages 111-127, January 2014

[17] Renjian Feng, Shenyun Che, XiaoWang and Ning Yu, "A Credible Routing Based on a Novel Trust Mechanism in Ad Hoc Networks",Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks, Volume 9, Issue 4, Article ID 652051, Pages 1-12, 2013

[18] Marjan Kuchaki Rafsanjani, Hamideh Fatemidokht, "FBeeAdHoc: A secure routing protocol for BeeAdHoc based on fuzzy logic in MANETs", International Journal of Electronics and Communications, Elsevier, Volume 69, Issue 11, Pages 1613-1621, 2015

[19] Yogendra Kumar Jain, Nikesh Kumar Sharma, "Secure Trust Based Dynamic Source Routing in MANETs",International Journal of Scientific & Engineering Research Volume 3, Issue 8, Pages 1-7, August-2012

[20] Ratul Dey, Himadri Nath Saha, "Secure Routing Protocols for Mobile Ad-Hoc Network (MANETs) –A Review", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 5, Issue 1, Pages 74- 78, 2016

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

P.Gowthamarayathirumal. "Service Authentic Trust and Coherence Key Based Secured Routing For Mobile Ad Hoc Networks." IOSR Journal of Computer Engineering (IOSR-JCE) 19.4 (2017): 40-51.