International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-4, February 2020

Fuzzy based Combined Trust Scheme for Secure Routing in MANET (FCTRS)

T. Arul Mozhidevan, K. Mohan Kumar

Abstract: ***Mobile Ad Hoc network (MANET) is a self-configuring network consisting of mobile nodes without any fixed infrastructure. However due to the nodes has not any fixed infrastructure in MANET, it is susceptible to various security attacks like data modification, information sniff, due to low energy, computing ability and bandwidth. In MANET Black hole is also an attack and it is difficult to detect and prevent. The lack of quality in security aspects of ad-hoc routing protocols won't provide reliability in the data packets movement between source and destination nodes. Implementing the routing decision with trust is an important one in the MANNET security. Hence, this research work propose an enhanced Fuzzy based combined trust scheme (FCTRS) based on public trust and Quality of Service (QoS) trust to detect black hole attack. It provides secure routing based on certificate authority (CA) to improve the performance of Ad-hoc On-demand Distance Vector (AODV). The results will show the performance improvement of proposed protocol over Enhanced Trusted Routing Scheme with Pattern Discovery (ETRS-PD) and the protocol AODV. The metrics in the performance of network examined with different conditions of mobility and the presence of black hole node positions.***

Keywords: ***Mobile ad-hoc networks, Packet-forwarding misbehavior, Secure routing, Fuzzy logic, combined trust model.***

I. INTRODUCTION

A mobile ad-hoc network is infrastructure less, self configuring and self maintained network. In this network, mobile nodes are communicated with each other directly if they are in the same network coverage area. If they are, out of the coverage range, the communication will require the formation with the help of cooperatives. Consequently, each node operates as a host and router as well. Due to these features they are used in many critical applications such as emergency operations, disaster relief, vehicular computing, mobile offices and many more. In MANETs, one of the most complicated tasks is the security. Due to the Open medium, dynamic topology, distributed cooperation, and constrained capability; MANETs are liable to suffer from security attacks. Hence, various attacks on different node positions may affect the security aspects in network.

The present routing protocols for ad-hoc networks are not adequate to manage the different routing attacks.

At present the existing cryptographic security schemes are used to prevent the network from external attacks. However these schemes are inefficient to resist the attacks created by the internal malicious nodes. Such nodes affect the security by doing misbehavior in packet-forwarding. In this scenario the term 'Trust' is introduced to measure the behavior of adjacent nodes [1].

The notion of trust would confirm to be useful for dynamic environments where the nodes have to depend on each other to attain their goals [2].

In recent times, trust management systems have been considered as a possible security solution to improve the routing decisions in MANETs by identifying and isolating distrusted nodes [3].

Moreover, one of the most prominent attacks in MANETs is the Black hole attack, which can be easily instigated on reactive routing protocols like AODV or Dynamic Source Routing (DSR). In this attack, a malicious node can magnetize all data packets by falsely claiming a fresh route or shortest route to the destination, without having any active route to the particular destination, and then attracts them without forwarding it to the destination node. Therefore, this paper propose an enhanced Fuzzy based combined trust scheme (FCTRS) with public trust and QoS trust to detect black hole attack and provide secure routing based on certificate authority to improve the performance of AODV.

This work is carried out with the following two stages. (1) Fuzzy based combined trust scheme is used to evaluate the trust value of neighbors while using AODV protocol. (2) The performance on black hole attack of FCTRS is compared with the protocols ETRS-PD and AODV through network simulator.

II. LITERATURE REVIEW

In recent times, several research works are going to tackle the security necessities of routing protocols using trust management. Xia et al. [4] developed a trust-based source routing (TSR) scheme to determine shortest route for data transmission in a secured manner. In this, current trust value of node is calculated using fuzzy logic. Nevertheless, the system gain maximized computational overhead in route's trust computation. Airehrour et al. [5] presented Grade Trust protocol to separate black hole opponents by selecting a secure path, as well as minimization of communication overhead and elimination of excessive routing computations.

Revised Manuscript Received on February 28, 2020.
***** Correspondence Author
T. Arul Mozhidevan*, Research Scholar, PG and Research Department of Computer Science, Rajah Serfoji Government College, Thanjavur, Affiliated to Bharathidasan University, Trichirappalli, Tamil Nadu, India. Email: arulmd@gmail.com
Dr. K. Mohan Kumar, Head, PG and Research Department of Computer Science, Rajah Serfoji Government College, Thanjavur, Affiliated to Bharathidasan University, Trichirappalli, Tamil Nadu, India. Email: tnjmohankumar@gmail.com

However, this protocol does not provide efficient simulation results compared with the conventional protocols.

From the literature review, it is clears that a combined trust metric with public and QoS trust components perform tasks effectively to provide performance as well as trust requirements [6],[7].

Especially, Cho et al. [6] used social (public) trust components namely intimacy and honesty, whereas Kohlas et al. [7] used honesty, reliability, maliciousness and competency to specify trust relationships.

Additionally, this scheme realized another significant QoS trust component, namely, consumption of energy for increasing the performance of the network [7],[8]. From these aspects, this research work proposed an enhanced and efficient trust based scheme called FCTRS.

Rutvij et al. [9] presented a model named ETRS-PD (Enhanced trust routing scheme with attack-pattern discovery), to reduce the opponents carry out various kinds of packet-forwarding misbehaviors. But it cannot handle problems with inaccurate and incomplete data.

Therefore, this paper propose an enhanced Fuzzy based combined trust model(FCTRS) to detect black hole attack and provide secure routing based on certificate authority to improve the performance of AODV.

III. METHODOLOGY

The following assumptions are taken in the proposed trust model of FCTRS (i). Links in the wireless network are bidirectional (ii). Every mobile node has identical physical characteristics; (iii). In order to observe the neighbor nodes, all the nodes are operating in promiscuous mode. (iv). Finally, the source (initiate) node and the destination (final) node are generous nodes.

The proposed FCTRS is used to improve the performance of the routing through trust derivation and trust computation in a different way.

A. Trust derivation

The proposed FCTRS obtain neighbor nodes trust value using direct observations by examining *Control packets reducing ratio, Data packets reducing ratio, channel ratio* and *consumption of energy* of neighbor nodes. This work also considers suggestions of trusted neighbors, in favor of providing efficient routing decisions.

B. Trust calculation

In the routing procedure, the sender computes neighbor node's trust by examining the activities carried out by that neighbor. Particularly, the node n_i will decrease the trust score of its neighbor n_j, if the neighbor does not forward the packet to the destination.

(i) *Control Packets Reducing Ratio (CPRR)*

It specifies the number of control packets reduced to the number of packets intended to forward. The computed *CPRR*, at time (t),

$$CPRR(t) = NCP_d(t) / NCP_a(t) \quad (1)$$

$NCP_d(t)$ - count of reduced control packets
$NCP_a(t)$ - total count of sent control packets

(ii) *Data Packets Reducing Ratio (DPRR)*

It specifies the number of data packets reduced to the number of packets intended to forward. The computed *DPRR*, at time (t),

$$DPRR(t) = NDP_d(t) / NDP_a(t) \quad (2)$$

$NDP_d(t)$ - count of reduced data packets
$NDP_a(t)$ - total count of sent data packets

(iii) *Consumption of Energy(CE)*

It specifies node's energy consumption to the initial energy of it. The computed *CE*, at time (t),

$$CE(t) = (IE - RE(t)) / IE \quad (3)$$

IE - initial energy
RE(t) – node's residual energy at time *t*.

(iv) *Channel Ratio (CTR)*

It is the ratio of neighbor node's trusted count during packets sent to the total count of received packets from that neighbor node. The computed *CTR(t)*,at time (t),

$$CTR(t) = NTH_d(t) / NTH_a(t) \quad (4)$$

$NTH_d(t)$ - neighbor node's trusted count
$NTH_a(t)$- total count of received packets from that neighbor node.

C. Final Trust Manager

The final trust manager (FTM) calculates the final trust values (*FTV*). The *FTV* of neighbor node n_j, is the computation of *Control packets reducing ratio(CPRR), Data packets reducing ratio(DPRR), consumption of energy(CE)* and *channel ratio(CTR)*. The final trust value of neighbor node n_j estimated by sender node n_i, indicated as FTV_{ij} is,

$$FTV_{ij}(t) = wg1 \times CPRR_{ij}(t) + wg2 \times DPRR_{ij}(t) + wg3 \times CE_{ij}(t) + wg4 \times CTR_{ij}(t) \quad (5)$$

wg1, wg2, wg3 & *wg4* - weights allocated to *CPRR*, *DPRR*, *CE*, and *CTR*.

Each node allocates these values and create trust table. The trust table contains ID of the node, Trust value, Trust type and its timeout. The centralized authority node demand the *FTM* to again calculate the node's trust value by fuzzy logic, existing node's trust value expired. Consistently trust table of node will be updated and altered whenever *FTM* calculating fuzzy trust value.

D. Fuzzy based analyzer

Fuzzy logic is used to predict the misbehaving nodes in the neighborhood accurately. Fuzzy logic contains trust values between 0 and 1. The trust value of node is computed using *CPRR, DPRR, CE,* and *CTR* values. These computed values are used as the fuzzy input value, nodes are marked as trusted or distrusted (malicious) node derived from fuzzy logic algorithm (FLA).

Fuzzy Logic System used to find trusted and cooperative node is shown in Fig.1. FLA will be called instantly, whenever sender node starts message to share data packet. If the fuzzy values are less than the critical threshold value, after that, node will be specified as malicious node. During communication, source node calls certified authority to confirm the trust value of node, at this time fuzzy analyzer (FA) is called upon. FA validates source node's trust level and execute fuzzy table depends upon fuzzy logic analyzer procedure. Using trust value, certified authority specifies that the node is trusted or distrusted. Moreover, certified authority discover that the asking node as insupportable, it send ALARM message to the entire trusted node. Certificate authority creates certificate using fuzzy based analyzer and pass it to the requested node.

The nodes classification is accomplished using fuzzy bias shown in Table 1. If the fuzzy trust value falls with low and very low, then the node marked as malicious, certified authority rejects certificate for intolerable node in the network and eliminated from routing. If fuzzy trust value falls with medium, high and very high, then the nodes are utilized in routing actions. When node certificate expired, then trust node asks for regeneration of credential before it initiates communication. Experimental results show effectiveness of FCTRS against black hole attacks.

Table-I: Fuzzy table for node behavior

Trust value of Node	Fuzzy Levels	Behaviour of Node
0-0.2	Very low	Malicious node
0.2-0.4	Low	Selfish Node
0.4-0.6	Medium	Normal Node
0.6-0.8	High	Co-operative node
0.8-1	Very High	Trustworthy and co-operative node

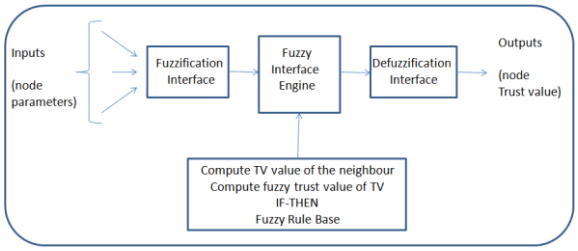

Fig. 1.Fuzzy Logic System used to find trusted and cooperative node

E. Certificate Authority

The maximum trust value node is certificate authority node. Certificate authority gets each node's trust value using final trust table. Based on authority, the malicious nodes are discarded and secure transmission is enabled in the network. The trusted node only will get authority, otherwise node will be changed. When centralized authority node exits beyond the range, then the successor utmost trust value node designated as a node of centralized authority. Centralized authority node certifies sending and receiving nodes for transmission of packets. The sending packets are encrypted by public key, the destination node only decrypt and read the message by private key.

F. Fuzzy composite trust-based on-demand routing strategy

The above said concepts are implemented through the modified routing strategy is described in Algorithm 1.

Algorithm 1:

Step 1: The source node (n_s) seem in its local routing table for the destination node (n_d) before starting data transmission.

Step 2: If the route exists, it starts sending data via the trusted next hop to destination node. Go to *Step 8*.

Step 3: If the entry does not exists, source node initiates a route discovery process by means of flooding route request (RREQ) packets to discover a route to destination node.

Step 4: When an intermediate node (n_k) receives a route reply (RREP) from its neighbor node (n_j), it receives the route reply only if neighbor node is not a distrusted node and *recommended as a trusted node*.

Step 5: If multiple route replies are arrived after the route discovery process, a route entry for the route with the fuzzy trust value and trusted next hop is created for *destination node and* inserted into the routing table of *source node*.

Step 6: If no such route is found, go to *Step 3*.

Step 7: *Source node* starts data transmission to *destination node*.

Step 8: If an intermediate node finds a next hop (*nm*) distrusted by direct observation or direct recommendation in its routing table for a destination n_p, the entry is discarded, during the fuzzy trust update procedure (*shown in Algorithm 2*). A local route discovery procedure is initiated by n_k to find an alternate route to n_p.

Step 9: Even though an intermediate node discovers a distrusted neighbor (*nm*) attempting to regain its trust by improving the trust value, *it is still not considered as a trusted node*.

The following Algorithm 2 should be incorporated at step 8 of above Algorithm 1. This is the detailed steps of Fuzzy Trust value procedure developed for this research work.

Algorithm 2:

```
For (Each neighbor table entry)
Do
        Verify the existence of attack pattern of the neighbor
        Compute TV value of the neighbor
        Compute fuzzy trust value of TV
                If (neighbor has TV as very low) then
                        Mark the node as a malicious node
                Else If (neighbor has TV as low) then
                        Mark the node as a selfish node
                Else If (neighbor has TV as medium) then
                        Mark the node as a normal node
                Else If (neighbor has TV as high) then
                        Mark the node as a cooperative node
                Else If (neighbor has TV as very high) then
                        Mark the node as a trusted and cooperative node
                End if
Done

For(Each routing table Entry)
Do
        Find the entry of the next hop from the entry table
                If(The next hop is found to be malicious in the neighbor table) then
                        Discard the route
                        Initiate a local route discovery procedure  to find an alternate route to the
                        destination
                End if
Done
```

IV. PERFORMANCE EVALUATION

NS-2 simulator is used to evaluate the performance efficacy of proposed protocol FCTRS with the existing protocols ETRS-PD and AODV. The major simulation parameters are shown in Table II.

Table-II: Parameters used in Simulation

Parameter	Value
Coverage area	1000 × 1000 m
MAC layer protocol	IEEE 802.11
Simulation time	240 s
Communication range of each node	250 m
Traffic type	CBR-UDP
Channel bandwidth	2 Mbps
Packet size	512 bytes
Mobility model	Random way point
Number of nodes	50
Number of connections	15
Maximum mobility (varying)	4–20 m/s
Pause time	5 s
Percentage of malicious nodes (varying)	0–40%
Routing protocols	AODV, ETRS-PD, FCTRS
Initial energy	1000 J
Transmit power	1.65 W
Receive power	1.4 W
Idle power	1.15 W
Sleep power	0.045 W
Transition power	2.3 W
Transition time	800 µs

The performance metrics used for the evaluation of FCTRS are

(i) *Packet delivery ratio*
(ii) Normalized routing overhead
(iii) *Average energy consumption*

The network parameters evaluated while implementing FCTRS are

1. *Node mobility speed* and
2. *Percentage of malicious nodes.*

4.1. Experiment 1: Node Mobility Speed

Protocols (AODV, ETRS-PD, and FCTRS) efficiency is evaluated by changing nodes mobility from 4 to 20 m/s and additional parameters are being unchanged.

(i) Packet Delivery Ratio

As exposed in Fig. 2, the packet delivery ratio of AODV almost drops from 46 to 39% while the mobility rises from 4 to 20 m/s. The increased number of link breakages makes increased packet loss at higher mobility higher node speeds. Alternatively, ETRS-PD gives packet delivery ratio from almost 80 to 65%. Meanwhile, when FCTRS is employed, the packet delivery ratio declines from almost 84 to 68% respectively.

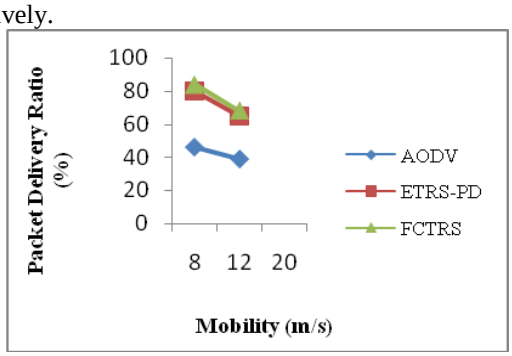

Fig. 2.Packet delivery ratio with varying node mobility

(ii) Normalized Routing Overhead

As revealed in Fig. 3, when the speed of the node is increased, the normalized routing overhead of AODV rises from almost 5.7 to 10.4. On the other hand, ETRS-PD improves normalized routing overhead by 3.8-6.5. Meanwhile, the FCTRS gives high performance by giving normalized routing overhead from almost 2.5 to 5.4.

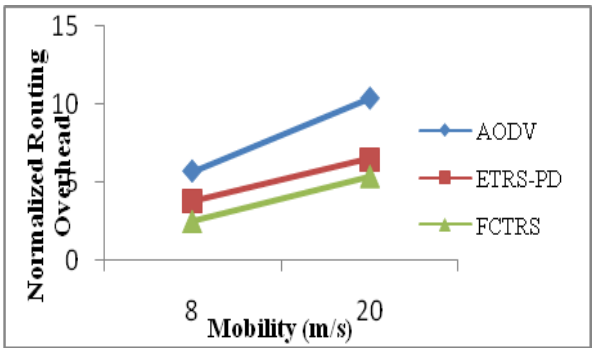

Fig. 3.Normalized routing overhead with varying node mobility

(iii) Average energy consumption

As shown in Fig. 4, the average energy consumption of AODV changes from 315.46 to 316.15 J. On the other hand ETRS-PD varies between 313.06 and 313.25 J. Meanwhile, FCTRS improves the average energy consumption between 310.23 and 311.42 J.

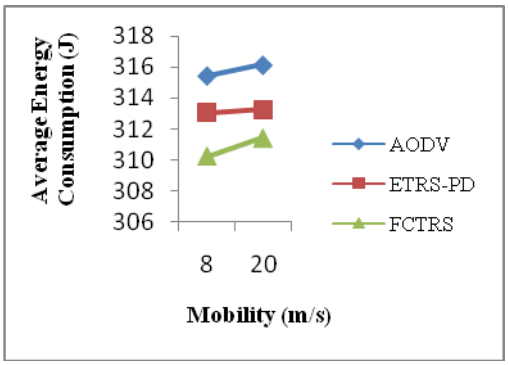

Fig. 4.Average energy consumption with varying node mobility

The following Table III shows the consolidated performance of the three protocols

Table-III: Performance of Node Mobility Speed

Test 1: Node Mobility Speed	AODV	ETRS -PD	FCTRS
PDR	46 to 39%	80 to 65%	84 to 68%
NRO	5.7 to 10.4	3.8 to 6.5	2.5 to 5.4
AEC	315.46 and 316.15 J	313.06 and 313.25 J	310.23 and 311.42 J

4.2. Experiment 2: Percentage of Malicious Nodes

Protocols (AODV, ETRS-PD, and FCTRS) performance efficiency is evaluated by changing of malicious nodes percentage from 0 - 40% and supplementary parameters are being changed. The parameter of percentage is set to 20 m/s.

(i) Packet Delivery Ratio

As exposed in Fig. 5, on account of the increased packets dropping intensity with increased malicious nodes ratio, the packet delivery ratio of AODV almost drops from 79 to 32%. Conversely, ETRS-PD offers packet delivery ratio from almost 80 to 55%. Meanwhile, FCTRS provide improvement in packet delivery ratio from almost 85 to 60%.

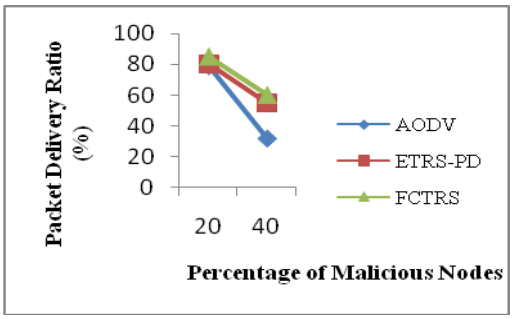

Fig. 5.Packet delivery ratio with varying malicious nodes percentage

(ii) Normalized Routing Overhead

As revealed in Fig. 6, the normalized routing overhead of AODV changes from almost 4.8 to 12.1. Meanwhile, ETRS-PD gives better normalized routing by the range of 4.8-8.5. Conversely, FCTRS improves normalized routing overhead by 4.8-6.2.

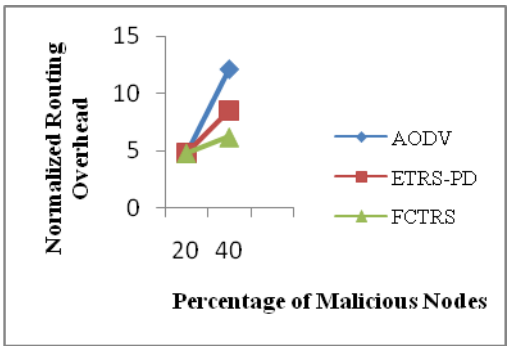

Fig. 6.Normalized routing overhead with varying malicious nodes percentage

(iii) Average energy consumption

As exposed in Fig. 7, the average energy consumption for the MANET employing AODV varies between 315.08 and 316.01. On the other hand ETRS-PD changes from 312.08 to 312.25 J. In the meantime, FCTRS gives improved average energy consumption by 310.21-310.53 J in the presence of adversaries.

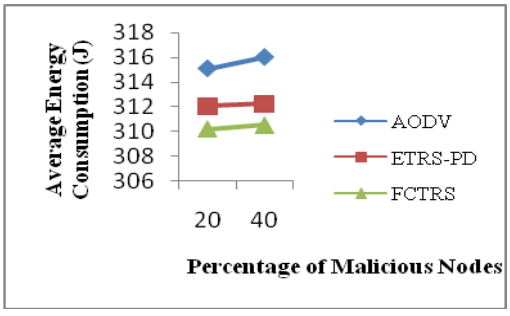

Fig. 7.Average energy consumption with varying malicious nodes percentage

The following Table IV shows the consolidated performance of the three protocols

Table-IV: Performance of Percentage of Malicious Nodes of Protocols

Test 2: Percentage of Malicious Nodes	AODV	ETRS-PD	FCTRS
PDR	79 to 32%	80 to 55%	85 to 60%
NRO	4.8 to 12.1	4.8 to 8.5	4.8 to 6.2
AEC	315.08 and 316.01 J	312.08 and 312.25 J	310.21 and 310.53 J

V. CONCLUSION

In MANET, the proposed Fuzzy trusts based approach detects black hole attack and provide secure routing in an efficient manner. The performance comparison of FCTRS with AODV and ETRS-PD proved that FCTRS achieves remarkable improvement in packet delivery ratio due to the enhanced routing process and inclusion of Fuzzy based combined trust components. Moreover, FCTRS reduced the generation of number of control packets using route handoff methods. Accordingly, FCTRS gives improved normalized routing overhead and energy consumption as compared to AODV and ETRS-PD under different network scenarios.

REFERENCES

1. H. Xia, Z. Jia., L. Ju, X. Li, and E. H. M. Sha, "Impact of trust model on on-demand multi-path routing in mobile ad hoc networks," *Computer Communications*, 2013, pp. 1078–1093.
2. H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A survey of trust and reputation management systems in wireless communications," *Proceedings of the IEEE*, 2010, pp. 1755–1772.
3. N. Marchang, and R. Datta, "Light-weight trust-based routing protocol for mobile ad hoc networks," IET Information Security, 2012, pp. 77–83.
4. H. Xia, Z. Jia., L. Ju, X. Li, and E. H. M. Sha, "Trust prediction and trust-based source routing in mobile ad hoc network," *Ad Hoc Networks*, 2013, pp. 2096–2114.
5. D. Airehrour, J. Gutierrez, and S. K. Ray, "Gradetrust: a secure trust based routing protocol for MANETs," *In: International Telecommunication Networks and Applications Conference*. IEEE, 2015, pp. 65–70.
6. J. H. Cho, A. Swami, and R. Chen, "Modeling and analysis of trust management for cognitive mission-driven group communication systems in mobile ad hoc networks," *In: International Conference on Computational Science and Engineering*. IEEE, 2009, pp. 641– 650.
7. R. Kohlas, J. Jonczy, and R. Haenni, "A trust evaluation method based on logic and probability theory," *In: IFIP International Conference on Trust Management*. Springer, 2008, pp. 17–32.
8. S. Reidt, S. D. Wolthusen, and S. Balfe, "Robust and efficient communication overlays for trust authority computations," *In: Sarnoff Symposium*. IEEE, 2009, pp. 1–5.
9. H. J. Rutvij, M. P. Narendra, and C. J. Devesh, "A composite trust model for secure routing in mobile ad-hoc networks. Available: http://dx.doi.org/10.5772/66519, 2017.

AUTHORS PROFILE

T. Arul Mozhidevan, pursed Master of Information Technology from Bharathidasan University, Thiruchirappailli and M.Phil from Alagappa University, Karaikudi. Currently doing Ph.D as a part time research scholar in PG and Research Department of Computer Science, Rajah Serfoji Government College, Thanjavur, Affiliated to Bharathidasan University, T.N, India. He is having 15 years of teaching experience. His main research work focuses on Computer Networks.

Dr. K. Mohan Kumar, received Master of Computer Science, Ph.D in Computer Science from Bharathidasan University, Tiruchirappalli, and M.Phil computer science from Manonmaniam Sundaranar University, Thirunelveli, India, currently working as Head in PG and Research Department of Computer Science, Rajah Serfoji Government College, Thanjavur, T.N, India. His main research work focuses on Network Security, Machine Learning and IoT, published more than 50 research papers in reputed International journals. He has 25 years of teaching experience and 20 years of Research Experience.