International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-3, February 2020

Trust Based Secure Routing Mechanism in Mobile Adhoc Networks for Enhancing the Routing Performances

K. Mani, S. Prasath Sivasubramanian

Abstract: ***Mobile Adhoc Networks enforces certain level of challenges for the researchers since they operate without a fixed infrastructure. Moreover the constant movement of nodes gives additional challenges while implementing any type of solutions. Similarly enforcing secure mode of routing in mobile adhoc networks creates lot of hurdles for the implementers. This paper addresses these issues, by computing the trust of each node and updating the trust tables of the respective nodes and the cluster head. This paper focus in designing a trusted secure mechanism for routing. The objective of this work is to calculate the trust of nodes using various trust methods. Later the calculated trust is updated with the trust table of the cluster head by forming a web of trust. This will enable a secure channel of communication among the adhoc nodes. After incorporating the newly computed trust, the routing performance of well known routing protocol say AODV, is evaluated for various routing parameters and it is compared with the performance of Trusted AODV(TODV).***

Keywords **: *Direct Trust, Indirect Trust, Web of Trust, Clusters, throughput, packet delivery ratio***

I. INTRODUCTION

Adhoc Networks are decentralized networks that bye-passes the centralized router. Unlike the wired counterpart, this network does not depend on the existing infrastructure for their operations. As the word 'adhoc' means 'for this purpose', this network finds its application where fixed networks cannot be configured. Since this network, functions in a decentralized manner, here, each node acts as a router while forwarding a packet to the destination. Hence this networks operates as a multihop network. Moreover, the nodes in the adhoc network are inherently mobile which makes frequent disconnections in the links. So, when a node wants to route a packet to the destination, the routing protocol's functioning is highly challenging[1]. Inorder to handle these challenges, researchers strive to find lot of solutions. One such solution to handle the mobility of nodes is that, they tried to build some hierarchy among nodes, by forming clusters. Clusters enable the division of entire network into small and manageable groups and these small groups of clusters will operate on a whole for various operations like routing, secure communication and service discovery process. Mostly in any network infrastructure, communication among the nodes is achieved through the routing protocols specifically designed for that network. Similarly in adhoc networks, various routing protocols have been designed for the purpose of node communication and data transmission. But, all the different categories of protocols that are designed for adhoc network does not enforce secure communication. Hence, in this paper, it is proposed to bring in a security mechanism for routing, using the concept of trust. The trust value of each node is calculated and the trust table of the cluster head is updated. The cluster head uses this table to decide which node can actively participate in the routing process based on the trust values by eliminating the malicious nodes. The trust tables of all cluster heads will be used for node communication by forming a web of trust.

The remaining part of this paper is formulated as stated herewith. Basic aspects of trust is detailed in Section 2. A survey of the existing literature of trust calculation process is done and the findings are listed in section 3. The mathematical background for calculating the direct and indirect trust is presented in section 4. The proposed methodology for calculating the trust and updation of the trust table is given in section 5. Experimental evaluation of the trusted routing with untrusted routing protocol is simulated and the outcome are discussed in section 6, and section 7 ends with conclusion.

II. BASIC ASPECTS OF TRUST

Trust is a characteristics of a node based on its behavior of both positive and negative experiences it imparts to its neighboring node during a data transmission[2-3]. Trust metrics can be used to quantify the level of trust. It can be either continuous and discrete. If it is a continuous measure the values can be $[0,1]$ and if it is discrete then it can have values in the range of $[-1,1]$. Trust metrics can be modeled as fuzzy model, probability model, similarity model, mobility models, context based models like energy, signal, measure of hops etc. In MANET, there is no central authority to monitor the network infrastructure. Moreover, they are highly dynamic nature of the network, does not allow pre-computed fixed secure routes. This type of open network cannot follow any security policy defined by the owner of the information.

Revised Manuscript Received on February 05, 2020.
* Correspondence Author
Dr. K. Mani*, Associate Professor of Computer Science, Nehru Memorial College, Puthanampatti, Trichirapalli, India
nitishmanik@gmail.com
S.Prasath Sivasubramanian, Research Scholar,, Nehru Memorial College, Puthanampatti, Trichirapalli, India, mail2prasath@gmail.com

Cryptographic security mechanisms for providing confidentiality of communication and authentication of nodes will not help against packet dropping and delayed packet attack or rushing attack nor it can help in rating the services[4]. Hence, trust systems are emerging as important decision support tools for selecting a node for routing to enhance the performance.

III. RELATED WORK

B. Nandhini,Praveena [5], in their research paper detects the selfish nodes using the concepts of honeypot interaction techniques and non cooperative game theory. Their entire approach uses Direct Trust for their implementation. Gohil Bhumika, Mukesh A. Zaveri, and Hemant Kumar Rath[6], proposed an approach using trust model for a service discovery process that was done efficiently within the network with reduced packet overhead and. K.Gomathi et.al[7], proposes an integrated approach of fuzzy trust based clustering (FTBC) using group key management by distributing them in hierarchical manner. They applied fuzzy logic based rules for identifying and eliminating the misbehaving nodes. J. Manoranjini, A. Chandrasekar , S. Jothi [8], in their research formulation, observes the behavior sensor nodes by creating a relationship using trust metrics thereby identifying the communication and mobility pattern of the nodes. This method enables a graceful elimination of blackhole attacks.. M. Ashwin, et.al,[9], proposed a weight based clustering model for trust calculation and evaluated the influence of malicious node on cluster head selection process. Zhengwang Ye,Tao Wen, Zhenyu Liu, Xiaoying Song, Chongguo Fu [10], proposed an proficient trust evaluation model in a dynamic fashion for WSNs. It includes the direct trust model with multiple trust factors. They took communication trust, data consistency, and energy trust into account for their implementation.

IV. MATHEMATICAL BACKGROUND OF TRUST CALCULATION

A. Trust Evaluation

Trust of a particular node in MANETs is evaluated based on three entities. They are Experience, Recommendation and Knowledge. The Experience component collects the trust of a particular node using direct trust calculation by sensing the node behavior periodically and the trust table is updated in a dynamic way. This entity takes the responsibility of maintaining the trust details up-to-date by dynamically updating the trust table. The Recommendation entity takes the responsibility of distributing the trust table details to all the neighboring nodes thereby recommending the updated trust details to the remaining nodes present in the network. The knowledge entity utilizes the updated trust details recommended by the Recommendation entity in the current trust calculation[11-12].

B. Direct Trust Calculation

Direct trust of a node is computed with all its one hop neighbors with their positive or negative experiences gained over a recent transactions. It is a measure of the ratio of the complete set of received packets over the number of packets sent at a particular instance of time. It is computed using the equation 1:

$$T^{d}_{m,n}(t) = \frac{w_1 * S_1{}^{m,n}_{rec}(t) + w_2 * S_2{}^{m,n}_{rec}(t)}{S^{m,n}_{sen}(t)} \quad (1)$$

Where $T^{d}_{m,n}(t)$ is a measure of direct trust at a particular instance of time t and $S_1{}^{m,n}_{rec}(t)$, and $S_2{}^{m,n}_{rec}$ is the number of data packets and control packets that are received by the receiving node at that time instance t and $S^{m,n}_{rec}(t)$ is the number of data and control packets sent by the sending node and w_1, w_2 are the weights and $w_1, w_2 \geq 0$ and $w_1 + w_2 = 1$.

C. Indirect Trust Calculation

Indirect trust is measured using the recommendation value a node received from the direct nodes of the target node using their positive or negative experiences. It is computed using the equation 2:

$$T^{i}_{m,n}(t) = \frac{1}{k}\sum_{g=1}^{k} T^{d}_{g,n}(t) \quad (2)$$

where $T^{i}_{m,n}(t)$ represents the indirect trust that is calculated at a time instance t and k denotes the total number of nodes that contribute for indirect trust of the target node n and $T^{d}_{g,n}(t)$ specifies the direct trust of the n and its neighbours who contributes for the indirect trust calculation. The value of g is ranges from $1 \leq g \leq k$.

D. Recent Trust

$$T^{r}_{m,n}(t) = \alpha * T^{d}_{m,n}(t) + (1 - \boldsymbol{\alpha}) * T^{i}_{m,n}(t) \quad (3)$$

where $T^{r}_{m,n}(t)$ specifies the computed recent trust at a time instance t and $\alpha = 0.7$ which specifies the direct trust weight. Direct trust is given higher weight since it gives more contribution for calculating the trust of a node.

v. PROPOSED WORK

It is proposed to evaluate the performance of a well known routing protocol after taking the trust computations of each node. The computed trust value of each node of the cluster is tabulated and ranked. Later the trust values that are computed for the nodes are propagated to the cluster head. This propagated values enables the cluster head, to decide which nodes can be an active member of the routing process based on the rank of the nodes. Similarly the trust values are propagated to each cluster head and the computed trust tables on each cluster head will form a web of trust, which enables each cluster head to function in cooperative manner[13].

The proposed work carries the following modules for implementation:

- Trust calculation
- Cluster head trust table updation
- Trusted Protocol Evaluation (TAODV)
- Result Analysis

A. Trust Calculation

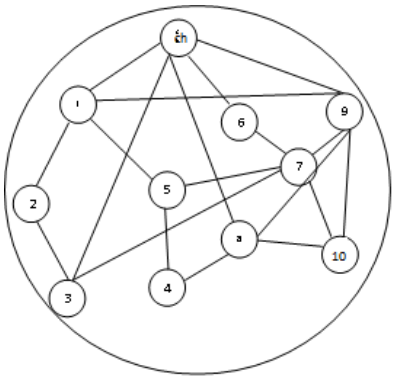

Figure. 1. Cluster formed with 10 nodes

In figure 1, there are 10 nodes in the cluster with a cluster head and while computing the trust values of each nodes, both the direct and indirect trust calculation process is performed and the trust table of the corresponding node is updated.

In figure 1, to update the trust table of node 1, the trust values are computed for the nodes that are connected directly and indirectly to node 1. The following steps shows the trust table updation process of node 1:

Node 1 has the following nodes as its direct neighbours, say $N1 \rightarrow N2, N5, N9\ and\ CH$, and its indirect neighbours are $N1 \rightarrow N3, N4, N6, N7, N8\ and\ N10$. After conducting a simulation run for the cluster shown in figure 1, and analyzing the data and control packets transmitted by node 1 to its neighbours, it was found that for a unit time of transmission, the data packets and the control packets contribute approximately 70% and 30% respectively, of the total transmission. Using the equation 1, direct trust is computed for the neighbouring nodes of Node 1 and it is shown in the table I.

Table I: Direct Trust Values of nodes connected to Node 1 directly

V and W	Packets Sent	Packets Received	Trust value
$N1 \rightarrow N2$	121	120	0.99
$N1 \rightarrow N5$	115	112	0.97
$N1 \rightarrow N9$	115	10	0.08
$N1 \rightarrow CH$	100	100	1

Similarly the indirect trust of node 1 with its indirect neighbours are calculated by getting the trust values from that node's direct neighbours using the equation 2 and is shown in table II to table VII.

$N1 \rightarrow N3$ (COLLECT INFORMATION FROM ITS NEIGHBOURS SAY N2, N7, CH

Table II: Indirect Trust Values of nodes connected to Node 1 (N3)

V and W	Packets Sent	Packets Received	Trust value
$N2 \rightarrow N3$	110	105	0.95
$N7 \rightarrow N3$	105	99	0.94
$CH \rightarrow N3$	105	103	0.96
			1/3 * 2.85 = 0.95

$N1 \rightarrow N4$ (COLLECT INFORMATION FROM ITS NEIGHBORS SAY N5 AND N8)

Table III: Indirect Trust Values of nodes connected to Node 1 (N4)

V and W	Packets Sent	Packets Received	Trust value
$N5 \rightarrow N4$	110	10	0.08
$N8 \rightarrow N4$	112	20	0.17
		1/2 * 0.25 = 0.12	

$N1 \rightarrow N6$ (COLLECT INFORMATION FROM ITS NEIGHBORS SAY N7 AND CH)

Table IV: Indirect Trust Values of nodes connected to Node1 (N6)

V and W	Packets Sent	Packets Received	Trust value
$N7 \rightarrow N6$	112	100	0.82
$CH \rightarrow N6$	100	85	0.85
		1/2* 1.67 = 0.83	

$N1 \rightarrow N7$ (COLLECT INFORMATION FROM ITS NEIGHBORS SAY N3, N5,N6,N9 AND N10)

Table V: Indirect Trust Values of nodes connected to Node 1 (N7)

V and W	Packets Sent	Packets Received	Trust value
$N3 \rightarrow N7$	113	110	.97
$N5 \rightarrow N7$	100	100	1
$N6 \rightarrow N7$	115	98	0.85
$N9 \rightarrow N7$	10	10	1
$N10 \rightarrow N7$	115	112	.97
		1/5* 4.7 = 0.94	

$N1 \rightarrow N8$ (COLLECT INFORMATION FROM ITS NEIGHBORS SAY CH,N4,N9 AND N10)

Table VI: Indirect Trust Values of nodes connected to Node 1 (N8)

V and W	Packets Sent	Packets Received	Trust value
$CH \rightarrow N8$	110	105	0.96
$N4 \rightarrow N8$	5	5	1
$N9 \rightarrow N8$	5	5	1
$N10 \rightarrow N8$	112	98	0.80
		1/4 * 3.75= 0.93	

$N1 \rightarrow N10$ (COLLECT INFORMATION FROM ITS NEIGHBORS SAY N7,N8, AND N9)

Table VII: Indirect Trust Values of nodes connected to Node 1 (N8)

V and W	Packets Sent	Packets Received	Trust value
$N7 \rightarrow N10$	115	112	0.95
$N8 \rightarrow N10$	100	85	0.97
$N9 \rightarrow N10$	5	5	1
		1/3 * 2.82 = 0.93	

After computing the trust values of all the nodes, Node 1's trust table is updated by assigning ranks to the nodes in the higher order of trust and is shown in table VIII.

Table VIII: Updated Trust Table Of Node 1 After Trust Calculation

Other Nodes	Trust Values	Trust Rank
N2 (Direct)	**0.99**	**1**
N3(Indirect)	**0.95**	**3**
N4(Indirect)	**0.12**	**Untrusted Node**
N5(Direct)	**0.97**	**2**
N6(Indirect)	**0.94**	**5**
N7(Indirect)	**0.94**	**3**
N8(Indirect)	**0.93**	**4**
N9 (Direct)	**0.08**	**Untrusted Node**
N10(Indirect)	**0.9**	**4**

From the table VIII, Node 1 can identify the untrusted nodes whose trust values are lower that 0.30, and hence, it can efficiently eliminate those untrusted nodes from participating in routing process.

Recent Trust of Node 1 is computed using the equation 3 at a particular instance. Here α is assigned a value of 0.7 since direct trust contribute more for a trust computation and, for a particular instance of time the percentage of data packets transmitted is approximately 70%. The recent trust of node 1 is calculated using equation 3 as:

$$(0.7 * 2.04) + ((1- 0.7) * 4.69) = 1.428 +1.407$$
$$= \mathbf{2.835}$$

B. Cluster Head Table Updation:

Since Cluster Head(CH) plays a crucial role in deciding the routing decisions, it is more significant to compute the trust values of the nodes attached to the CH. Similarly, the direct and indirect trust of CH is also calculated and it is shown table IX:

Table IX: Trust Table Of Cluster Head(CH) After Trust Calculation

Other Nodes	Trust Values	Trust Rank	Recent Trust
N1 (direct)	**0.99**	**1**	**2.83**
N2 (Indirect)	**0.9**		**2.75**
N3(direct)	**0.97**	**2**	**2.8**
N4(Indirect)	**0.1**	**Untrusted Node**	
N5(Indirect)	**0.93**		**2.76**
N6(direct)	**0.95**	**4**	**2.77**
N7(Indirect)	**0.8**		**2.6**
N8(direct)	**0.96**	**3**	**2.79**
N9 (direct)	**0.08**	**Untrusted Node**	
N10(Indirect)	**0.9**		**2.75**

C. Trusted Protocol Evaluation (TAODV)

Once the trust values are updated for each node and also of the CH, the well known routing algorithm of adhoc networks is simulated to verify its performance. The following algorithm shows the process of evaluating the Trusted AODV evaluation:

Algorithm 1: Trusted AODV evaluation process
Input: Set of trusted nodes, RREQ
Output: RREP, trusted route

Step 1: Prior to initiate the transmission of data, the source node n_s scan its local routing table for an appropriate path to the destination node n_d.

Step 2: If such a desired entry exists, it starts its transmission through that trusted next hop n_d.. Go to Step 8.

Step 3: If the source node n_s, fails in finding the entry to destination in the routing table, then it will initiate the process of finding the route to n_d by flooding the RREQ.

Step 4: Any intermediate node say n_k will accept a route reply it receives from its neighbour say n_j, only when n_k ensures that n_j is a trusted node by checking the computed trust values of n_j (should be less than the allowed range)

Step 5: When multiple route replies are received by n_s, then the node giving a route with highest trust value in the Next hop route to n_d is identified and an entry is made in the routing table of n_s.
Step 6: When the route discovery process fails, it will be reinitiated from Step 3.
Step 7: A successful route discovery initiates Node n_s to starts data transmission to n_d.
Step 8: When an intermediate node n_k finds a next hop n_m is not a trusted node either by computing the direct or indirect trust, to reach node n_p, then it discards the corresponding routing table entry and will initiate a fresh route discovery process to update its routing table.

VI. EXPERIMENTAL EVALUATION

In order to check the validity of the proposed methodology, the experimental evaluation of Trusted AODV (TAODV) with normal AODV protocol is carried out using NS2 tool. The simulation is carried out for 150 nodes and the performance is evaluated by plotting the values received using XGRAPH tool.

A, Parameters taken for evaluation

- Delay: This can be calculated by subtracting time at which first packet was transmitted from source minus the time at which first packet arrived to the destination[14].

- Packet Delivery Ratio : It is defined as the ratio of data packets received by the destination to those generated by the sources.
- Throughput : Throughput is measured as a total number of successful packets received by the destination nodes of the network, at a particular instance of time[15].
- Routing Overhead: It is measure of how much packets a node sent, received and forwarded.

B. Simulation Environment and Parameters

The simulation of the proposed work in NS2 takes the following steps of fixing a rectangular area where the nodes are randomly placed. Mobility of nodes follows a random waypoint model, wherein the nodes navigates at a uniform speed to a random location. The uniformity in the speed of navigation is fixed from a value of 0 to a higher value. Later the node is made to wait for a stipulated time, before it selects another random location, and the process is repeated. Simulation parameters that are taken for implementation is shown in Table.9.

Table. 9: Simulation Parameters

PARAMETER	VALUES
Number of Nodes	150
Transmission Range	30m
Mobility model	Random waypoint
Idle Degree	10s
Maximum speed of nodes	2 – 10m/s
Maximum Displacement	1 – 10m

C. Results Analysis

After the simulation of the protocol's performance evaluation with the above simulation parameters for various routing parameters like PDR, DELAY, THROUGHPUT and Routing Overhead, the following graphs are drawn:

Figure 2a. Packet Delivery Ratio

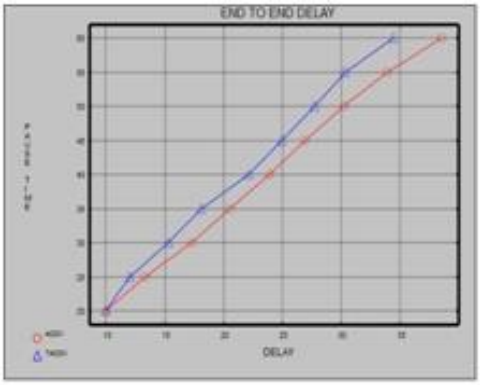

Figure 2b. End to End Delay

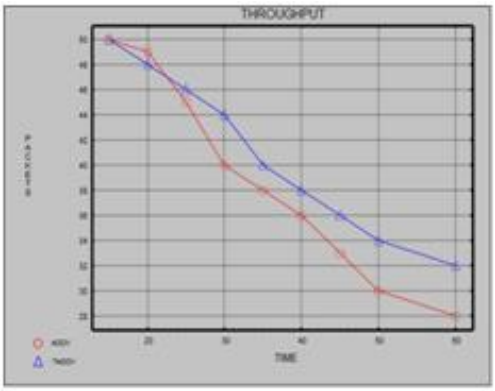

Figure 2c. Throughput

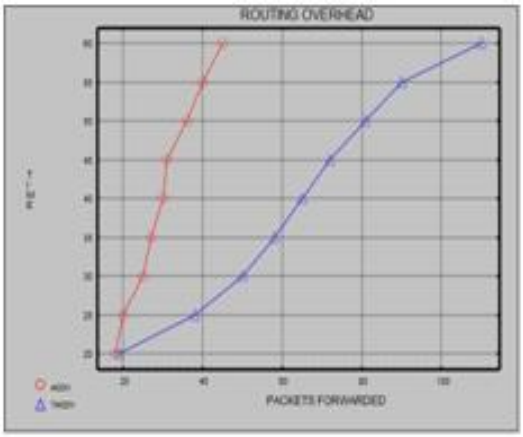

Figure 2d. Routing Overhead

The evaluation of various parameters like Packet Delivery ratio, Delay.

Throughput and Routing Overhead shows that the TAODV has a better performance measure over its normal counterpart. This is because, the trust value computed by each node enables a better way of identifying malicious and also selfish nodes. This is achieved by varying the weight values of data and control packets. As Quality of Service (QOS) is determined more by the data packets, higher importance is given for such packets in trust computation while varying the weights. Packet Delivery Ratio and Throughput computations of TAODV has significantly increased since, the cluster head refrains the untrusted nodes to participate in the routing decision process.

This can be visually seen from figure 2a, that the ratio of packets successfully transmitted and successfully received is 6% more for TAODV and in figure 2c, TAODV has more number of packets delivered per unit time when compared to AODV. In adhoc networks, the malicious nodes present in the clusters enforces more delay in delivery of packets. The delay of TAODV has reduced to 4.1 unit time as shown in figure 2b. when compared to the delay encountered in AODV. This change in delay is due to the fact that in TAODV, the identification of malicious node is carried out efficiently using both direct and indirect trust computation and it is removed from taking part in the routing process. Since all the CH trust table has been used to form a web of trust, over all routing overhead of TAODV has a better performance than the normal AODV.

VII. CONCLUSION

In this paper a novel approach for computing the trust values of nodes has been proposed and the performance of AODV and TAODV is measured. Based on the performance exhibited by the protocols after the evaluation of routing parameters, it is concluded that the performance of TAODV shows good results over conventional AODV. The trust values computed by each node is updated with the trust table of Cluster head which inturn forms a web of trust with the neighboring cluster heads. This enables all the cluster head to take a routing decision in a cooperative manner and due this web of trust, routing performance has enhanced considerably. By giving varying weights for data and control packets during trust calculation, malicious nodes are identified efficiently in TAODV, and they are eliminated from participating in routing process. This elimination of malicious nodes has a marked performance improvement in avoiding the delay This improvement in the performance of routing enables betters the quality of service.

REFERENCES

1. V. Jayalakshmi, T. Abdul Razak "Trust Based Power Aware Secure Source Routing Protocol using Fuzzy Logic for Mobile Adhoc Networks "IAENG International Journal of Computer Science, 43:1, IJCS_43_1_12, Advance online publication: 29 February 2016
2. Ramireddy Kondaiah, Bachala Sathyanarayana, "Trust Factor And Fuzzy-Firefly Integrated Particle Swarm Optimization Based Intrusion Detection And Prevention System For Secure Routing Of Manet" International Journal of Computer Networks & Communications (IJCNC) Vol.10, No.1, January 2018.
3. KE Xuemeng, ZHOU Guofu, DU Zhoumin " Trust Evaluation Model for P2P Networks based on Time and Interaction" MATEC Web of Conferences 208, 05005.https://doi.org/10.1051/matecconf/201820805005, ICMIE 2018.
4. Shaik Sahil Babu, Arnab Raha, Mrinal Kanti Naskar "Trust Evaluation Based on Node's Characteristics and Neighbouring Nodes' Recommendations for WSN "Wireless Sensor Network, 6, 157-172, 2014.
5. B. Nandhini , Praveena , "Dual Trust Based Service Allocation Protocol For Service Oriented Manet" , International Journal of Mechanical Engineering and Technology (IJMET) Scopus Indexed, Volume 8, Issue 12, pp. 608–616, December 2017.
6. Gohil Bhumika, Mukesh A. Zaveri, and Hemant Kumar Rath "Trust Based Service Discovery in Mobile Ad-Hoc Networks" Lecture Notes on Software Engineering, DOI: 10.7763/LNSE.2015.V3.210. Vol. 3, No. 4, November 2015.
7. K. Gomathi, B. Parvathavarthini, C. Saravanakumar "AnEfficient Secure Group Communication in MANET Using Fuzzy Trust Based Clustering and Hierarchical Distributed Group Key Management", Springer Science Business Media New York, Wireless Pers Communication 94:2149–2162, DOI 10.1007/s11277-016-3366-x, , 2017.
8. J.Manoranjini, A. Chandrasekar & S. Jothi, "Improved QoS and avoidance of black hole attacks in MANET using trust detection framework", Journal for Control, Measurement, Electronics, Computing and Communications, Volume 60 - Issue 3, 2019.
9. M. Ashwin, S. Kamalraj, Mubarakali Azath,"Weighted Clustering Trust Model for Mobile Ad Hoc Networks", Wireless Pers Commun 94:2203–2212, DOI 10.1007/s11277-016-3371-0, Springer Science Business Media New York, 2017.
10. Zhengwang Ye,Tao Wen, Zhenyu Liu, Xiaoying Song, and Chongguo Fu, "An Efficient Dynamic Trust Evaluation Model for Wireless Sensor Networks" Hindawi, Journal of Sensors, Article ID 7864671, 2017.
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:197, DOI 10.1186/s13638-016-0691-4, 2016
12. Muhammad Salman Pathan, Nafei Zhu, Jingsha He, Zulfiqar Ali Zardari, Muhammad Qasim Memon and Muhammad Iftikhar Hussain "An Efficient Trust-Based Scheme for Secure and Quality of Service Routing in MANETs" Future Internet; doi:10.3390/fi10020016,www.mdpi.com/journal/futureinternet, 2016
13. Turki Ali Alghamdi , "Convolutional technique for enhancing security in wireless sensor networks against malicious nodes" , Human-centric Computing and Information Sciences volume 9, Article number: 38 , 2019
14. Dr. K. Mani, Prasath Sivasubramanian, "Cluster Enabled Performance Evaluation of MANET Routing Protocols Using Mobility Patterns" International Journal of Electronics Engineering (ISSN: 0973-7383) Volume 11 , Issue 1 pp. 738-750 June 2019
15. J. Sebastina Queen Rose, S. Sumithra, "A Cluster Based Walk for Peer To Peer Streaming In Wireless Sensor Networks". International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 5, May 2015

AUTHORS PROFILE

Dr. K. Mani, has 30 + experience in teaching and nearly 15 years experience in research.
He has completed M.C.A., M.Tech Computer Science and Engineering, M.Phil and PH,D from Bharathidasan University Trichirapalli. He has published more than 50 research papers in reputed Journals and International conferences. He has proposed innovative mathematical models for Cryptographic Algorithms that has gained him reputation in leading Journals. He is a external examiner for conducting the public viva-voce examination for Ph.D scholars of various universities. He is nominated as Doctoral Committee member by Bharathidasan Univeristy for many Research scholars. He is an active Member of academic bodies for framing course curriculum for Masters in Computer Science courses of Bharathidasan University. He has successfully guided 8 Ph.D and more than 30 M.Phil Research scholars. Presently he is working as Associate Professor in the Department of Computer Science and Research of Nehru Memorial College (Autonomous), Puthanampatti. Trichirapplli. His broad area of Research includes Mathematical Cryptography, Networks, Information Security

S. Prasath Sivasubramanian,, is working as Assistant Professor in Tagore Government Arts and Science College, Puducherry, India and pursuing research in Nehru Memorial College, Puthanampatti, Trichirapalli under the guidance of **Dr. K.Mani**. He has completed M.Sc Computer Science from Bharathidasan University,Trichirapalli, M.Tech Computer Science and Engineering from Pondicherry University, M.Phil from Manonmaniam Sundaranar University, Tirunelveli,
He has more than 20+ years of teaching and 5 years of research experience. Published 6 research papers in leading journals. He has guided 2 M.Phil Scholars. He is member of academic body of Pondicherry University and has involved in the framing the Undergraduate syllabus.
His area of research includes, Adhoc Networks, Service Oriented Architecture.