International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume 5, Issue 2 (April '2019)

A LITERATURE REVIEW ON SECURE ROUTING MECHANISM IN MANET USING TRUST MODEL

K.Ranjithsingh,
Research Scholar,
Sri Vijay Vidyalaya College of Arts & Science,
Dharmapuri, Tamilnadu, India.

Dr. D.Maruthanayagam,
Head/Professor,
PG and Research Department of Computer Science,
Sri Vijay Vidyalaya College of Arts & Science,
Dharmapuri, Tamilnadu, India.

Abstract: A MANET is a kind of wireless mobile network that can be easily established with the help of few infrastructure less connections. In such networks, every node is independent of its own and therefore can act as a router and execute the job of routing as well. In a public channel, the main reason of use the MANET is to propel the data protect between source and the destination. Trust mechanism is being used as substitute to the cryptographic technique. Trust mechanism protected the data forwarding by separating the nodes with malevolent intention using the trust value on corresponding nodes. It is an infrastructure-less network where the one mobile device link with other device wirelessly. Every device in MANET changes its movement and links in any direction often. Routing in MANET is the method of transfer the information from start node to destination node. For the period of the routing process, load balancing and energy consumption are the challenging issue to get better the network lifetime. In addition, security plays main part during the data transmission from source node to destination. *This paper focuses routing performance* in the Mobile Adhoc Networks (MANETs) relies on the support of the individual nodes that form the network. Secured routing is process of preserving the information from unauthorized users during data transmission in MANET. *In this paper reviews for various researchers have carried out their previous work related to routing mechanism in MANET by using trade model.*

Keywords: Mobile Ad Hoc networks, Routing mechanism, Trust model, trust, Trust computation, Mobile networks and Attacks.

I.INTRODUCTION

Mobile adhoc networks **(MANETs)** are a ***group of mobile nodes*** which establish the communication with each other via multihope wireless links. Each node in the MANETs proceeds as router and host at the identical time. MANETs routing protocols are classify into two types, on demand (reactive) and table-driven (proactive). On-demand routing protocols which are well thought-out in this paper perform ***enhanced with significantly lower overheads*** than table-driven routing protocols in most situations. Several adhoc on-demand routing protocols contain projected, for example, dynamic source routing, temporally ordered routing algorithm **(TORA)** and adhoc ondemand distance vector. In common, both form of routing protocols for the MANETs are intended basis on the assumption that all contributing nodes are completely cooperative. Due to the MANETs distinctiveness such as dynamic topology, protocol weaknesses, openness and mobility these might be targeted by the attackers in some of ways.

Several ***"secure" routing protocols are improved*** for MANETs. The majority of them presume trusted third-parties or centralized units which actually demolish the self-organization nature of MANETs. These protocols are effectual to fight against external attacks, but are not able to put off selfishness like malicious. Limited resources like power, bandwidth, processing capability, and storage space, it is an essential one to minimize the routing overhead in MANETs and guarantees the high rate of packet delivery. Security in MANET routing protocol is method to transfer the data packet securely. The routing protocol is depending on security connection, key distribution, authentication, cryptography scheme, etc. MANET is the prospect network as it is versatile, easy to employ, inexpensive and immediately update as well as reconfigure.

A Mobile ad Hoc Network consists of highly dynamic adaptive nodes, ***also called as routers*** which can be easily established without the help of any predefined infrastructure. All the nodes are independent of each other and perform the task of routing as well few management functions. There will not be any centralized coordinator and hence any node is free to join and leave the network as and when needed easily. All the ***nodes in a MANET work together*** with each other and perform the task of routing; hence it can be treated as a multi hop cooperative network.

MANET Challenges

A MANET environment has to defeat certain subject of limitation and inefficiency. It includes:

Frequent breakages in transmission links due to various interferences like co channel interference, noise, ***fading of signal strength*** add many difficulties in the receiver side. As the nodes in this type of network are wireless, ***there is very limited transmission range*** because of which the transmission cannot be through a single hop. Due to the wireless physical channel in MANET's, the probability of occurrence of errors is very high, which invites trouble in a MANET. Because of the ***mobility feature of the nodes***, topology of the network changes very frequently and hence problem of routing the packets through intermediate nodes becomes difficult. Because of being a ***highly dynamic in nature*** and no centralized coordinator nodes are free to join

and leave the network easily which creates a path for malicious nodes to enter easily into the network. As data is being transmitted ***through a wireless medium***, the possibility of occurrence of different types of attacks is very much more in MANET's. In this paper is structured as follows. ***Section 2 describes the literature review of various routing*** mechanism in MANET based on trust model and ***section 3 describes the conclusion***.

Properties of Trust in MANET

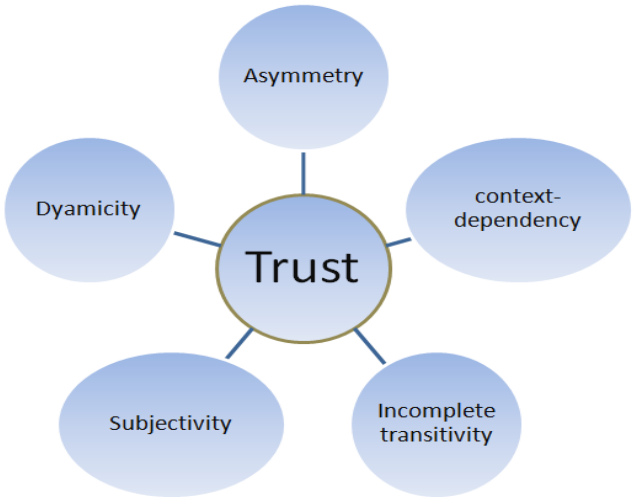

Figure 1: Trust Properties in MANET

Dynamics: Due to the dynamic character of topology in MANET, it is confront to keep the trust because of changed or incomplete information. So, the dynamical character of trust can be imprisoned in representing the certainty by binary or even distinct value entity.

Subjective: ***Trust is measured as subjective in MANET***. With various experience with node and the dynamic topographical version, the trust will be maintain at various levels by trustor node against the same trustee node.

Incomplete Transitivity: Transitive relation of the two entities with the third entity is not essential. Trustor maintains two category of trust. First, trust in trustee and trustee advice to the third party.

Context-Dependency: The trust is preferred by ***based upon the task***.

Asymmetry: Asymmetry means high potential nodes are ***trusted by low potential nodes*** but vice-versa is not essential.

Composability: Trust information from all the path should be combined to obtain the ***single opinion value.***

II. LITERATURE REVIEW

A lot of researchers have carried out their work in this section we are discuss about previous work related to routing mechanism in MANET by using trade model. This paper presents here a couple of such techniques and enlists the major research work in this area.

[2017] Darren Hurley-Smith, *et al.* [1] Proposed to address the secure communication in MANETs, network access controls and node authentication. The main focus is to protected access to a virtually closed network **(VCN)** that permits the expedient, reliable communication with integrity, authenticity and confidentiality services. SUPERMAN joined the routing and communication security at network layer to preserve the network. To attend to the problem of unified MANET communication security and structured a Virtual Closed Network architecture to protect both application data and network. Authentication provides a means by which a node may be identified as trustworthy. By using a certificate to prove that they share a trusted authority, two nodes may validate one-another based on their shared Trusted Authority (TA).

[2017] Nadav Schweitzer, *et al.* [16] proposed method for decreasing the gray-hole DoS attack. The designed solution failed to assume explicit node collaboration with node internal knowledge gained through routine routing information. In contrast, proposed method to great extent minimizing the gray-hole attack efficiency.

[2015] David Airehrour, *et al.* [14] proposed method for Grade Trust secure routing based up on the trust levels. It improves packet delivery ratio by using trust to segregate ***black hole attack*** and offer secure routing for data traffic as well as the improved packet delivery ratio. The ratio of effective packet interchange between the neighbor nodes is computed in the network. Based on the ratio nodes in the network under grade trust protocol will be classified on the basis of the importance of the trust level of the node. The first node will be classified as trusted Friend which is the most secured node, the next node as Friends which is moderately secure and the last node which is not secure is possible Friends. Each one will be assigned with a priority number based on the trust level. This will continue till the packet reaches the destination. Preliminary simulation results have exposed that the trust compromise and the packet delivery ratio is improved in Grade Trust ***compare to traditional routing protocols, such as FSR and AODV***.

[2014] Harris Simaremare, *et al.* [2] proposed trust AODV, a trust mechanism to secure the AODV protocol. In adhoc network, black hole attack and active attack like DOS tin can easily occur. These attacks could reduce the performance of routing protocol. The performance of this protocol is improved by using ant algorithm. When node is trusted the ant agent put positive pheromone. Path communication is based on the value of the pheromone. The performance improves in stipulations of throughput ratio and packet delivery.

[2014] Akshai Aggarwal, *et al.* [15] proposed a method for Trust Based Secure OnDemand Routing Protocol also known as **TSDRP.** Adhoc on demand Distance vector **(AODV)** is ***modified to propose* TSDRP *t***o secure it from different attacks such as Black hole attack, Denial of service attack (DOS) etc. This protocol provides security against denial of service attack and black hole attack. AODV was

modified to **TSDRP** by establish the Node trust table and Packet buffer. Node trust table stores information about each node and the misbehaving node. Each node has node ID and trust computation is performed to calculate the value of trust based on packet observation. Packet buffer uses three different PB, such as PB_RREQ**,** PB_DATA and PB_RREP to store control and data packets. Therefore, DoS attack and Blackhole attack TSDRP has performed extremely well in approximately all parameters: PDF, NRL and AT as compared to AODV.

[2013] Dilli Ravilla, *et al.* [3] proposed the Secure Zone of routing protocol to identify misbehaving nodes and prevent network from destroying. Earlier, Zone routing Protocol [4] which is hybrid routing protocol which is prone to various security attacks. Misbehaving nodes deliberately drop the packets all along the route to disrupt the process of routing protocol. This is overcome by proposed scheme. To evaluate Packet Delivery Ratio using SZRP is comparable with **ZRP,** while there is minimal adverse impact of SZRP on End-to-End Delay and Routing Overhead. To ensure confidentiality we used public key cryptography and to ensure authenticity, integrity and nonrepudiation we use digital signature. It uses key generation which generates private and public key pair for digital signature. In MANET, Neighbor Discovery Protocol **(NDP)** is used to discover the neighboring nodes in the wireless channel considering its location and round trip information. To give the packet integrity in the Secure Intra Zone Routing Protocol ***(SIERP) by uses digital signature and RSA.***

[2013] D.Santhosh Kumar, *et al.* [4] proposes Efficient Trust based routing using confront to establish security. This takes the scheme from the real world network of friends. It works by sending sharing friends list and challenges of the trusted nodes to source node so that data transmission can be done successfully. The rating of the nodes will done on the basis successful transmission and friendship with other nodes in the list. Friendship account can be obtained by sharing your friend's process which will be done periodically in the network. This will completely isolate the misbehavior nodes which are missing with no role play. The limitation of the scheme is as it does not rely on any scheme that will spread information about the malicious node so the chances of colliding takes place are very low. The special challenge is in authenticating the nodes unique characteristics. ETAR algorithm is separated into four stages, Rate friends, Route through friends, Challenge your neighbor and Share Friends. Provides an intrinsic security to network and malicious nodes are easily exposed.

[2013] Mazda Salmanian and Ming Li, *et al.* [5] in this proposal, the perception of dispersity routing with maintaining and managing of an obtainable modular security Architecture is influenced and integrated. so the dispersity routing is achieved by adopting the Adhoc On-level Demand Multipath**(AOMDV).** To enlarge modular security architecture, have Trust improved Routing Table module to contain the reliability metric. Therefore that route, among the multiple accessible routes to a destination, may be selected and tracked with policy-set parameters. Under the proposal, secure route is the one that will be mapped throughout the trusted (authenticated) nodes with the established SAs, where trustworthy route is the one that will have a high Mean Time among Failure. Reliability and trust as parameters are used with the multiple routes provide the graded routing service − the ability of providing a number of potential routes to destination in a MANET, each of which may be selected because its security and reliability metrics match those of the policy. The four potential grades of service are provided in fraded service like Secure and stable grade of service, Stable graded service, Secure and unstable graded service, Unstable graded service to ***combine routes from both OLSR and AOMDV.***

[2012] S.Neelavathy Pari, *et al.* [6] proposed the colluding nodes detection and defense mechanism by using both ***cluster-based approach and trust-based route discovery*** through every node in a MANET and a scheme to identify the colliding nodes that cause internal effect. The new trust based on cluster oriented method is used. The route redundancy and message redundancy will be reduced by broadcasting the packets. An algorithm for calculation of the trust and to get the route to identify the colliding nodes with no redundancy in route and message for the duration of discovery of route by use of Requisite trust based on secure routing **(RTSR).** Computation of trust will be complete in the local forwarding nodes where it is used in the route discovery. The ***cluster head*** can store the ***trust information*** and route discovery information. The piggy backing bit would have decrease the broadcast storm problem. This reduces the mobility overhead which will avoid dynamic cluster head election.

[2011] Jing-Wei Huang, *et al.* [7] proposed a message security scheme to the MANET. By use of trust-based on multipath AOMDV routing collective with the soft-encryption, yielding the so it is called as T-AOMDV scheme. If malicious nodes are present in the network then it is the serious message security concern. For providing authenticity the message is sectioned at the source node and then encrypted before being routed through different path to the destination. Generate original message by using the decryption approach, it will take place at recipient end. Various issues happen when malicious networks node is present in the network it causes serious security message concern. However, scheme yields the ***minimal route selection*** time and the T-AOMDV, is more secure ***than traditional multipath algorithms*** and the T-DSR scheme.

[2010] Raihana Ferdous, *et al.* [8] in this proposed method to formalized trust mechanism in MANET. It have a key management scheme to utilize trust the same as a foundation and establish the key between nodes in a MANET and use metrics as a trust to establish secure ***distributed controls in the MANET***. DSR protocol will be used as it gives a complete path between source and destination to be discovered before communication is initiated between them. To provide route maintenance and route discovery used path rater and watch dog. The design issues are pair wise keys will be used to establish, manage trust values and to make decisions. For establish the trust in MANET, authentication, certification , auto-configuration are needed.

[2010] Pedro B. Velloso, *et al.* [9] proposed a method for flexible trust model based up on the ***idea of human trust***,

which give nodes with a mechanism to calculate the trust level of its neighbors. The basic ideas consist of using previous recommendations and experiences of other neighbors to evaluate the trust level of the other nodes. Initiate the conception of relationship maturity, which permit nodes to attribute more relevance to the recommendations issued by nodes that know the appraised neighbor for a long time and also propose the Recommendation Exchange Protocol **(REP)** which enable nodes to send recommendations and receive recommendations. Interactions among nodes are confined to neighbors. Such approach implies lower resource consumption and a lower vulnerability to false recommendations attack. Another important quality is the flexibility due to the possibility of operating in three different modes, depending on the node resource restrictions. Thus, the model is suitable for heterogeneous network, where nodes present distinct constraints. Besides, the presence of nodes that do not implement at all our trust system do not disturb the other nodes that are using the system, since nodes are capable of evaluating the trust level even in the occurrence of a few cooperating neighbors. This does not need disseminating the trust over the complete network as an alternative, nodes will only keep on exchanging the information about the nodes within the range. There is no global information required. This scales well for large networks as well while reducing the number of exchanges. It also mitigates the result of colluding attacks which are collected of liars in network. The main aim they introduce is the relationship maturity, which will allow the nodes to improve the efficiency of the model in case object is mobile in nature.

[2010] Islam Tharwat A. Halim, *et al.* [10] proposed a model to overcome the existence of misbehavior node while routing operation is carried out. Reliability of the network nodes must be considered in the route selection process combine with the hop count. The Reliability is achieved by measure the trust value for every node in the network. Self monitoring agent is based on dynamic source routing presented. So the protocol called as Agent-Based on Trusted Dynamic Source Routing Protocols **(ATDSR)** for the MANETs. The objective is to control trust information nearby with time delay and minimal overhead messages. This is achieved by installing each contributed node in network to multi-agent systems. MAS consist of two kinds of agents: routing agent **(ROA)** and monitoring agent **(MOA).** The further realistic objective model of computing the trust value is initiated which is weighted by the both size and number of routed packets to imitate the ***"selective forwarding" behavior of a node***. The performance simulation via evaluation shows that proposed protocol is enhanced trusted than and standard DSR.

[2010]R. S. Mangrulkar, *et al.* [11] propose method is focused on routing algorithm (trust based AODV), which adds an extra field in the request packet which stores trust value representing node trust on neighbor. On the ***basis of level of the trust factor***, routing information will transmit according to the highest trust value amongst all the nodes. This trust value is updated on every successful communication. Node power can be saved by avoiding unnecessary transmission of control information but ***bandwidth or channel utilization*** which is ***more important in MANET***. The misbehaving node can attack on control packets and leads to misbehavior in the network. The malicious node may be trusted or may not be trusted. Irrespective of shortest and longest path we use the trusted path for a communication in the network. Route trust values are computed on receiving the completed reply path which is utilized by the source node for approaching communication in the network. The trust based on routing protocol improves the security level and also prevent malicious node attack in the network.

[2009]A.Menaka Pushpa, *et al.* [12] Introduced trust based ***model based on node trust and route trust*** in AODV protocol. With this minimum overhead, we can easily eliminate the malicious node as well as we can establish a best trusted route between source and destination. Also it creates a secure communication in this environment without any internal attackers. A new data structure Neighbor table is introduced which consist of trust value and neighbor id which must be maintained by each node to maintain track of the dynamically changing list and its corresponding node trust values. Trust is calculated by the common opinion of the nodes. The ***major challenge*** is that the network ***must provide its services*** without any problem by trust based protocols. Supports modified extended routing protocol. T his will give communication in secure manner with no any internal attackers.

[2007] Mohamad Y. Alsaadi and Yi Qian, *et al.* [13] proposed a method for secured MANET routing protocol, and particularly on the improvement of the security for Dynamic Source Routing Protocol (DSR). Improve the security of routing for the obtainable DSR protocol by ***enhance the conception of trust value***, the chosen of a secure route will be based on these trust values. NS-2 simulations are perform to assess the impact of apply the trust value based on the route selection to the DSR protocol. Improves the trust based routes selection that is apply to the DSR protocol which will develop the security of routing protocol. They select the best and the secure route. Previously, DSR protocol involves in choosing shortest route to the destination nodes but they are choosing the secure and route most reliable to the destination based on trust value. This provides the trust based routing solution when there are exists high number of malicious nodes. The best route selection will be based on two criteria: 1) it will return the average of the trust values of all the nodes in the network. 2) Evaluates the node on basis of average of past experience. They are implementing a separate acknowledgement module to monitor the received acknowledgement and adjust the trust values on the node of the route. It shows that, trust based on DSR can achieve higher throughput and packet deliver ratio than the existing DSR when misbehavior nodes are there in the network.

[2007] Sesha Bhargavi, *et al.* [17] In this proposal, ***focus on new hybrid secure routing protocol that establish secure communication*** path transversely the nodes in network which can get better the throughput and ratio of packet delivery etc. This protocol helps in selecting the finest path for secure file transmission based on the trust information from neighboring nodes. The proposed protocol

have implement on NS-2 .This protocol accomplished better reduced delay and ratio of the packet delivery while compare with protocols like AOMDV, AODV, etc. In hybrid secure routing protocol, the file is transmitted based on the information of trust receives from different nodes. It reduces the service based attacks and it also reduces the recommendation based attacks if there are not more than 50% malicious nodes in the network. It uses three types of metrics, service, and reputation and path trust metrics to create a secured path in the network's proximity. This work also ***implements the load balancing mechanism*** to utilize the network resources effectively. Hence, the time required for a node to find the path can also be reduced. Performance Evaluation was done for various scenarios and found that the no. of packet losses is increasing drastically with the malicious nodes. This new Secure S-DSR protocol was implemented to reduce packet loss and to improve ratio of packet delivery and reduce the end to end delay even in the presence of malicious nodes. It helps to reduce many problems encountered in the existence of attacks.

III.CONCLUSION

Mobile AdHoc Network (*MANET) is the special form of the wireless mobile network* where a group of mobile devices form a temporary network with no help of an established infrastructure and it is highly challenged environment of the network appropriate to its extraordinary characteristics such as dynamic topology, decentralization and neighbor based routing. Each node in this network relays its neighbors for routing and message forwarding. *The file is transmitted based upon the trust information* receives from different nodes. Analyzed and surveyed many schemes in MANET for providing the trust based secure routing to ensure the trust in multiple perspectives. Due to the open nature it is difficult to maintain the trust and resource constraints; hence the *trust is the desired challenge for best performance*. This literature survey reviewed all the achievable trust management for secure routing with required protocols as well as discussed the *merits and demerits* of those work effectively.

IV.REFERENCES

[1]. Darren Hurley-Smith, Jodie Wetherall and Andrew Adekunle, "SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad hoc Networks", IEEE Transactions on Mobile Computing, Volume 16, Issue 10, October 2017.

[2]. Harris Simaremare , abdelhafid abouissia, RIRI FITRI SARI,"performance analysis of optimized trust aodv using ant algorithm",IEEE ICC 2014 - Communications Software, Services and Multimedia Applications Symposium.

[3]. Dilli Ravilla, Dr Chandra Shekar Reddy Putta "Performance of Secured Zone Routing Protocol due to the Effect of Malicious Nodes in MANETs", 2013, IEEE.

[4]. D.Santhosh Kumar,Dr.K.Thirunadana Sikamani "Efficient And Secure Trust Based Ad Hoc Routing in MANET ", International Conference on Current Trends in Engineering and Technology, ICCTET'13 .

[5]. Mazda Salmanian and Ming Li "Enabling Secure and Reliable Policy-based Routing in MANETs", 2013 IEEE.

[6]. S.Neelavathy Pari1, B.Narmadhadevi2, Sridharan Duraisamy3, "Requisite Trust-Based Secure Routing Protocol for MANETs", 2012 IEEE.

[7]. Jing-Wei Huang "Multi-Path Trust-Based Secure AOMDV Routing in Ad Hoc Networks", 2011 IEEE.

[8]. Raihana Ferdous, "Trust Formalization in Mobile Ad-Hoc Networks", 2010, IEEE.

[9]. Pedro B. Velloso, Rafael P. Laufer, Daniel de O. Cunha, Otto Carlos M. B. Duarte, and Guy Pujolle, "Trust Management in Mobile Ad Hoc Networks Using a Scalable Maturity-Based Model", IEEE, september 2010.

[10]. Islam Tharwat A. Halim, Hossam M. A. Fahmy 2, Ayman M. Bahaa El-Din 3, Mohamed H. El-Shafey"Agent-based Trusted On-Demand Routing Protocol for Mobile Ad-hoc Networks", 2010 IEEE.

[11]. R. S. Mangrulkar, Dr. Mohammad Atique "Trust Based Secured Adhoc on Demand Distance Vector Routing Protocol for Mobile Adhoc Network" 2010, IEEE.

[12]. A.Menaka Pushpa M.E. "Trust Based Secure Routing in AODV Routing Protocol", 2009 IEEE.

[13]. Mohamad Y. Alsaadi, Yi Qian "Performance Study of a Secure Routing Protocol in Wireless Mobile Ad Hoc Networks", 2007 IEEE.

[14]. David Airehrour, Jairo Gutierrez, Sayan Kumar Ray " GradeTrust: A Secure Trust Based Routing Protocol For MANETs",2015, IEEE, International Telecommunication Networks And Application Conference(ITNAC).

[15]. Akshai Aggarwal "Trust Based Secure on Demand Routing Protocol (TSDRP) for MANETs", 2014 , IEEE, Fourth International Conference on Advanced Computing & Communication Technologies.

[16]. Nadav Schweitzer, Ariel Stulman, Asaf Shabtai and Roy David Margalit, "Contradiction Based Gray-Hole Attack Minimization for Ad-Hoc Networks", IEEE Transactions on Mobile Computing, Volume 16, Issue 8, August 2017.

[17]. V. Sesha Bhargavi , Dr. M.Seetha, S.Viswanadharaju "A Trust Based Secure Routing Scheme for MANETS", 2007, IEEE.

ABOUT THE AUTHORS

K.Ranjithsingh received his M.Phil Degree from Periyar University, Salem in the year 2008. He has received his M.Sc., Degree from Madurai Kamaraj University, Madurai in the year 2002.He is working as Assistant Professor at PGP College of Arts & Science, Namakkal. He has 16 years of experience in Academic Field. He is pursuing his Ph.D. (Part-Time) Degree at Sri Vijay Vidyalaya College of Arts & Science, Dharmapuri, Tamilnadu, India. His areas of

interest include Mobile Computing, Cryptography and Network Security.

Dr.D.Maruthanayagam received his Ph.D Degree from Manonmaniam Sundaranar University, Tirunelveli in the year 2014. He received his M.Phil Degree from Bharathidasan University, Trichy in the year 2005. He received his M.C.A Degree from Madras University, Chennai in the year 2000. He is working as HOD Cum Professor, PG and Research Department of Computer Science, Sri Vijay Vidyalaya College of Arts & Science, Dharmapuri, Tamilnadu, India. He has above 18 years of experience in academic field. He has published 5 books, more than 35 papers in International Journals and 30 papers in National & International Conferences so far. His areas of interest include Computer Networks, Grid Computing, Cloud Computing and Mobile Computing.