International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-5S3, July 2019

Vehicular Adhoc Network Based Location Routing Protocol for Secured Energy

A. Chinnasamy, P. Selvakumari, V. Pandimurugan

Abstract: ***ALERT chiefly uses irregular message routing copy to supply namelessness protection. The projected protocol provides the ALERT routing high namelessness protection, EALERT additionally dynamically partitions a network field into zones and haphazardly chooses nodes in zones as intermediate relay nodes, that Anon-traceable anonymous route. It then haphazardly chooses a node inside the choice zone as a result of subsequent relay node and uses the EGPSR formula as a variant of GPSR in awake to send the information to the relay node. Within the last step, the information is broadcasted to k nodes at intervals the destination zone, providing k-anonymity to the destination. In addition, the protocol contains a method to hide the information instigator among sort of initiators to strengthen the k-anonymity protection of the provision. The projected Energy aware ALERT detects the Sybil attack within the network, Routing protocol, geographical routing.***

Index Terms:: Vehicular ad hoc networks, anonymity, routing protocol, geographical routing.

I. INTRODUCTION

Wireless communication has proved its various blessings over wired communication thanks to the actual fact that electrical engineer properly transmitted indicators throughout the channel for the first time in 1898. thanks to the actual fact that then, oil-fired by means of digital and oftenness (RF) fabrication trends, movable cellular gadgets, in conjunction with cellular telephones, non-public virtual assistants (PDA) and laptops, have communication networks are evolved, consisting of cellular networks, wi-fi lans (WLAN), bluetooth networks, ultra-huge band (UWB) networks, transport advert hoc networks (VANETs), and WIMAX. amongst these, mobile networks, bluetooth networks, and WLANs ar the utmost extensively used. but, cellular networks and WLANs ar centralized networks, that mean that luxurious infrastructure and centralized management ar needed. mistreatment bluetooth generation, hosts will connect with every totally different in an advertisement hoc fashion, however this generation is just targeted at low power short-variety wire substitute. consequently, a wireless mobile advert hoc community may be adistributed, self-organized and multi-hop network that has obtained good attention in recent years. VANET may be a disbursed community that doesn't need centralized manage, and every host works not best as a supply and a sink but in addition as a router. this sort of dynamic community is specifically helpful for army communications or be supported. moreover, the simplicity of building an advertisement hoc community permits sharing statistics in a very meeting or in hospitable piece of land basically. Sanction multi-media programs beside video and audio conversation in vanets needs nice of service (QOS) guide. the usage of anonymous routing protocols ar vital in vanets to supply cozy communications by suggests that of concealment node identities and preventing web site guests analysis assaults from out of doors observers. obscurity in VANETs consists of identification and locality obscurity of information assets (i.e., senders) and locations (i.e., recipients), additionally to course obscurity. "identification and space obscurity of resources and destinations" approach it's miles tough if viable for various nodes to amass the important identities and precise places of the sources and locations. for course obscurity, adversaries, each route or out of the trail, cannot hint a packet flow back to its supply or resort area, and no node has records just about the particular identities and places of intermediate nodes route. alert offers route obscurity, identification and region obscurity of supply and destination. alert provides the unnamed routing to the packet. once that alert is resilience to intersection assaults and temporal order attacks. alert contains a approach to effectively counter intersection assaults, that have well-tried to be a {troublesome|a tricky} open trouble. the planned protocol offers high obscurity safety (for assets, destination, and direction) with low fee at the aspect of the elevated nodal time period within the community. the planned system considers the strength of the nodes involved inside the spoken communication.

A. Characteristics of VANET

VANET is associate degree application of Edouard Manet however it's its own distinct characteristics which might be summarized as:

1.High quality
2. speedily ever-changing constellation
3. infinite network size,
4.Frequent exchange of data

Manuscript published on 30 July 2019.
***** Correspondence Author (s)
Dr.A.Chinnasamy, Department of Computer Science Engineering, Sri Sairam Engineering College, Chennai
P.Selvakumari, Department of Computer Science Engineering, Tagore Engineering College, Chennai.
V.Pandimurugan, Department of IT. Hindustan Institute of Technology & Science,Chennai.

B. Applications Of VANET

Ad-hoc networking may change the military to want gain of common region community technology to hold academic degree statistics community between the soldiers, vehicles, and military info head zone. for a pair of business environments, the requirement for cooperative computing is probably any important out of doors point environments than internal and whereby of us do have to possess out of doors conferences to induce along and exchange records on a given mission. ad-hoc networks can autonomously link an on the spot and temporary multimedia network. the use of non-public pc systems to unfold and share information among contributors at a convention or magnificence space. the opposite applicable neighborhood stage code is probably in home networks whereby gadgets can communicate on to exchange records. VANET that embody bluetooth can amendment the repose articulation among varied cellular gadgets that embody a pc, and a cellular smartphone. ad-hoc is additionally employed in emergency operations for catastrophe relief efforts, e.g. in hearth, flood, orearth quake. emergency rescue operations should take space where by non-current or broken articulation infrastructure and speedy preparation of a account network is needed

II. RELATED WORK

SEAD on the DSDV-SQ version of the insecure DSDV impromptu network routing protocol. specifically, to avoid long routing loops in SEAD, it use destination sequence numbers, as in DSDV; we tend to conjointly use these destination sequence numbers to produce replay protection of routing update messages in SEAD. we tend to dissent from DSDV therein we don't use a edian weighted subsidence time in causing triggered updates. to cut back the quantity of redundant triggered updates, every node in DSDV tracks, for every destination, the typical time between once the node receives the primary update for a few new sequence variety for that destination, and once it receives the most effective update for that sequence variety for it (with the minimum metric among those received therewith sequence number); when deciding to send a triggered update, every DSDV node delays any triggered update for a destination for this average weighted subsidence time, within the hope of solely desperate to send one triggered update, with the most effective metric, for that sequence variety. SEAD doesn't use such a delay, so as to forestall attacks from nodes which may maliciously not use the delay. Since a node Xiaox in Wu and Bharat Bhargava et al(2005 planned the Privacy is required in accidental networks. an advert hoc on-demand solely the position of the destination is exposed within the network for route discovery position to a true node ID. this could be implemented by the employment of secure position service systems. Node quality enhancesDestination namelessness by creating the match of a node ID with an edge short. propose secure location aware services over conveyance accidental networks (VANET) with our geographical secure path routing protocol (GSPR). GSPR is associate infrastructure free geographic routing protocol, that is resilient to disruptions caused by malicious or faulty nodes. Results show that though the presence of malicious nodes will increase the routing path length, a knowledge delivery rate of larger than eightieth is sustained albeit four-hundredth of the nodes malicious Pathak et al (2008),.

proposed dueto the published nature of wireless transmissions, communications MANETs lot of subject to malicious traffic analysis. In spite of the secure routing protocols, traffic analysis attacks ar still not well addressed . Indeed, these protocols concentrate on security of route maintaining and defensive against modification of routing data, that cannot forestall traffic we tend to propose Associate in Nursing anonymous version of ARAN, that is one amongst the foremostsecure routing protocols, to produce obscurity and preserve security of nodes in MANETs ElaheSheklabadi, Mehdi Berenjkou et al (2011). Seryvuth Tan and Keecheon Kim et al(2013) ,proposed the MANET permit mobile hosts to initiate communications with one another over As are result, Ad-hoc On demand Distance Vector (AODV), that is one in all the quality VANET protocols may be attacked by malicious nodes.

III. PROBLEM DEFINE

The Sybil attack is one during which a malicious node on a network illegitimately claims to be many totally different nodes at the same time. A Sybil assaulter will either produce quite one identity on one physical device so as to launch a coordinated attack on the network or will switch identities so as to weaken the detection method, thereby promoting lack of answerableness within the network. Here the relay node might act because the assaulter so, the node produce the new identity and then act because the neighbor to the actual node ,it will send message to the relay node with the various identity , relay node route packet to the incorrect relay node that doesn't nearer to the destination. If it happens it'll drains energy of the nodes concerned within the network.

IV. PROBOSED WORK

A. PROPOSED SYSTEM

In order to produce high obscurity protection (for sources, destination, and route) with low price, this project proposes associate Anonymous Location-based and economical Routing protocol (ALERT). ALERT dynamically partitions a network field into zones and haphazardly chooses nodes in zones as intermediate relay nodes, that sort a non-traceable anonymous route. Specifically, in each routing step, a data sender or forwarder partitions the network field thus on separate itself and conjointly the destination into a pair of zones. It then hap hazardly chooses a node inside the various zone as a result of consequentrelay node and uses the GPSR formula to send the information to the relay node. inside the last step, the information is broadcasted to k nodes inside the destination zone, providing k-anonymity to the destination. in addition,

ALERT contains a technique to hide the information leader among style of initiators to strengthen the obscurity protection of the availability. ALERT is in addition resilient to intersection attacks and temporal arrangement attacks this project analyze ALERT in terms of obscurity and efficiency. It in addition conducted experiments to guage the performance of ALERT compared with totally different obscurity and geographic routing protocols. In Summary, the contribution of this work includes: initial one is Anonymous routing.. ALERT contains a technique to effectively counter intersection attacks, that have established to be a hard open issue. .The projected protocol provides high obscurity protection (for sources, destination, and route) with low price beside the improved nodal life inside the network. With this the inherent battery backup of the node is in addition thought-about throughout geographical forwarding. By this though the node is that the most effective forwarder by the house issue, it's elect for forwarding as long as it is the tight battery power to carry out the task of forwarding the information packets. inside the last step, the information is broadcasted to k nodes inside the destination zone, providing k-anonymity to the destination. in addition, the protocol contains a technique to hide the information leader among style of initiators to strengthen the obscurity protection of the availability. Second strategy embowered inside the protocol is towards the detection of the Sybil bad person nodes that aims at creating duplicate identities for themselves as completely{different|completely totally different} nodes at different locations thereby increasing the routing overhead and wasting the inherent battery power of the legitimate nodes by responding to those faulty identities.

4.2 Objective

- To detect the Sybil attack in the network,
- To avoid the Sybil attack in the network,

4.3 Architecture Diagram

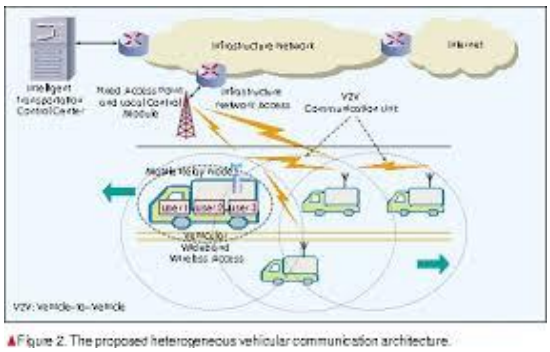


Figure 2. The proposed heterogeneous vehicular communication architecture.

Fig .1 Architecture diagram

4.4 Modules

1 Anonymous routing for VANET
2 Energy Aware
3 Against Attack
4 Performance Evaluation

1 Anonymous routing for VANET

B. Network Model

Network model contemplate model contemplate the random means purpose model and the cluster also the cluster quality model Network area unit classified into Zone. contemplate a message's sender is also unconcealed by just exposing the transmission direction. Therefore, associate anonymous communication protocol that may give un-traceability is required to strictly make sure the namelessness of the sender once the sender communicates with the opposite aspect of the sector. Moreover, a malicious observer could try and block the information packets by compromising variety of nodes, intercept the packets on variety of nodes, or maybe trace back to the sender by police investigation the information transmission direction. Therefore, the route ought to even be undetectable.

C. Zone Partition

ALERT the communication vary is divided into the Zones. If the supply and destination don't seem to be gift within the same zone, throughout the Zone partition the condition to be thought-about is, the forwarder and also the destination not gift within the same zone. until this condition happy it'll be portioned into horizontal and vertical zones. In this, Random forwarder is chosen arbitrarily within the zone. RF is chosen within the following manner. 1st the arbitrarily the situation is chosen from the actual Zone. The node nearest to the situation is elective because the Random Forwarder.

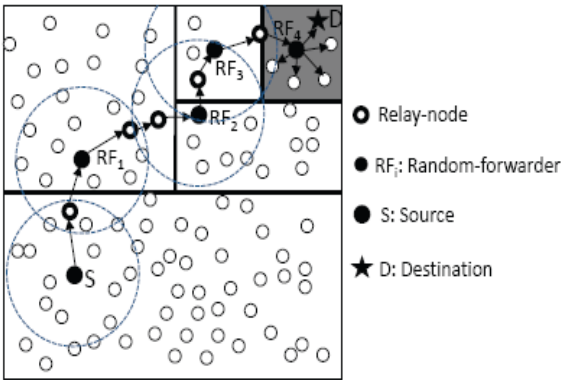
Input:Random Forwarder selection
Output: partitioned Network

Relay node selection:
Greedy forwarding based Relaynode
Input: NeighborTable, sender, destination;
Output: Greedy Relaynode;
ListN: Neighbor List
ListC: Candidate List, initialized as an empty list
ND: Destination Node
Base: Distance between current node and ND
Greedy forwarding based Relaynode
if find(ListN, ND) then
next hop ND
return
end if
fori 0 to length(ListN) do
ListN[i]:dist dist(ListN[i], ND)
end for
ListN: sort()
Relaynode→ListN[]
Assign weight w2 for the sorted list from high to low

D. ALERT routing

ALERT options a dynamic and unpredictable routing path, that consists of variety of dynamically determined intermediate relay nodes. every which way chooses a node within the divided zone in every step as an intermediate relay node

(i.e., information forwarder), so dynamically generating hit or miss routing path for a messag



Input: source send message
Output: Message received by Destination

E. Energy Aware

E-GPSR switches to perimeter forwarding. Compared to GPSR, with the employment of E-GPSR, the unfairness in node usage would comparatively scale back and therefore with this the inherent battery backup of the node is additionally thought of throughout geographical forwarding. By this even if the node is that the best forwarder by the space issue, it's designated for forwarding as long as it's the decent battery power to hold out the task of forwarding the info packets. With in the last step, the info is broadcasted to k nodes within the destination zone, providing k-anonymity to the destination. additionally, the protocol encompasses a strategy to cover the info leader among variety of initiators to strengthen the namelessness protection of the supply.

Input: while selection of Random Forwarder energy of the node considered
Output: energy aware routing

F. Against Attack

The proposed system detects the attacker using the received signal strength in the network. Relay node receives packets from the same node with different identity and transfer the packet to the destination. The Attack detection operation is performed in the following way. Relay Node calculates the Received signal strength of the nodes from those it gets the packets and it will detect the attacker nodes in the network. If nodes Rss value is low it will consider as the random node and it will allow that node to route the packet. Otherwise that node considers as the attacker and it will avoid the node to transfer the packet it will consider as the attacker. In ELAERT, the same operation performed for the ALERT.

A Sybil attacker node which aims at creating duplicate identities for themselves as different nodes at different locations thereby increasing the routing overhead and wasting the inherent battery power of the legitimate nodes by responding to these faulty identities. By this the battery draining of nodes due to unnecessary routing policies are avoided priory thereby increasing the overall lifetime of all the nodes in the network is possible. Thus the proposed EALERT has the efficient strategy towards increased nodal life time in the low cost anonymous routing protocol.

Input: Sybil attacker with different identity sent packet to relay node
Output: Energy drain of the nodes involved in the routing

The distinction between a new legitimate node and a new Sybil identity can be made based on their neighborhood joining behavior. While receiving the message from the same node with different identity, the RSS values for those neighbors are calculated. If the received RSS value is high it will be detected as attacker.

Input: RSS calculation
Output: detection of the attack presence

The proposed scheme utilizes the RSS (Received Signal Strength) in order to differentiate between the legitimate and Sybil identities. This scheme does not use localization technique for Sybil attack detection and hence does not need any directional antennae or any GPS equipment. The distinction between a new legitimate node and a new Sybil identity can be made based on their neighborhood joining behavior. The Received signal strength values are varied for the neighbors act as the Sybil attacker from that of the legitimate node.

Input: RSS calculation
Output: detection of presence of Sybil attack in network.

4 Performance Evaluation

The projected performance evaluated for the node's energy before the Sybil attack detection and once detection of Sybil attack within the network whereas exploitation EALERT routing.

V. SIMULATION RESULTS AND EVALUVATION

To measure our success in meeting the planning goals for GPSR AND EGPSR, we simulated the algorithmic rule on a spread of static and mobile network topologies. we tend to focus principally on the mobile simulation results in this paper, as that a part of the planning area is a lot of demanding of a routing protocol—link additions and removals much more frequent beneath quality.

A. Simulation Environment

Network simulation (NS) is one of the types of simulation, which is used to simulate the networks such as in MANETs, VANETs etc. It provides simulation for routing and multicast protocols for both wired and wireless networks. NS is licensed for use under version 2 of the GNU (General Public License) and is popularly known as **NS2**. such as TCP and UPD, traffic source behavior such as FTP, Telnet, Web, CBR and VBR, router queue management mechanism such as Drop Tail, RED and CBQ, routing algorithms and many more.

In ns2, C++ is used for detailed protocol implementation and Otcl is used for the setup. The compiled C++ objects are made available to the Otcl interpreter and in this way, the ready-made C++ objects can be controlled from the OTcl level.5.2 Simulation Model:

SIMULATOR	Network Simulator 3
NUMBER OF NODES	Random
TOPOLOGY	Random
FIXED SETUP	Source,destination,random forwarder
INTERFACE TYPE	Wireless
MAC TYPE	802.11P
QUEUE TYPE	Droptail/Priority Queue
QUEUE LENGTH	200 Packets
ANTENNA TYPE	Omni Antenna
PROPAGATION TYPE	Tworay Ground
ROUTING PROTOCOL	DSDV
TRANSPORT AGENT	UDP
APPLICATION AGENT	CBR
TRANSMISSION POWER	Vary at each Layer(0.2-1.0)
RECEPTION POWER	Vary at each Layer(0.2-1.0)

5.3 Implementation Results

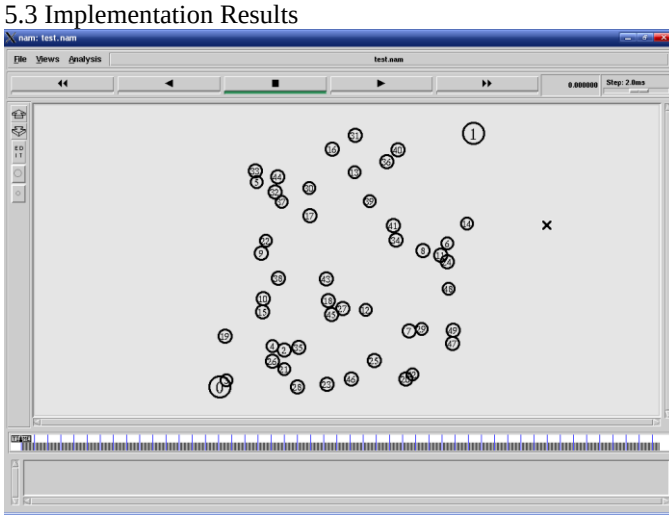


Fig 1 It is Network setup. The nodes are present in the random location.

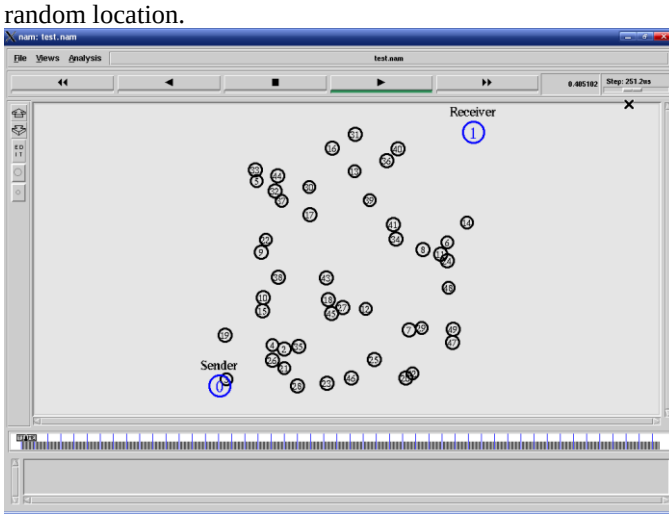


Fig 2 the node colored in blue is the sender of the communication. And also the receiver also showed in the blue color.

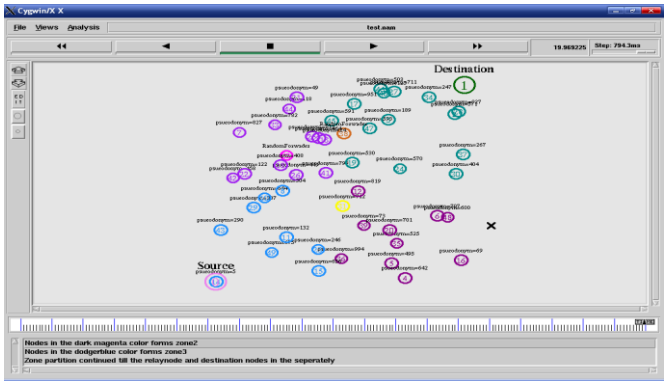


Fig 3 Energy aware

VI. CONCLUSION

ALERT additional strengthens the namelessness protection of supply and destination by concealment the information initiator/receiver among variety of knowledge initiators/receivers. it's the "notify and go" mechanism for supply namelessness, and uses native broadcasting for destination namelessness. This project contributes QoS in ALERT, The planned theme proposes the energy aware Anonymous Location primarily based routing; it thought-about the energy of the nodes concerned in network. except concealment details death of any node because of battery debilitating nodes isn't attainable or maybe very tough in such hostile environments.

REFERENCES

1. B. Karp and H. Kung,. "GPSR: Greedy Perimeter Stateless routingfor Wireless Networks" in: Proceedings of ACM MobiCom, 2000,pp. 243–254
2. yih-Chun Hu David B. Johnson, "Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," in Proc.IEEE Workshop on Mobile Computing Systems and Application, 2002.
3. Xiaoxin Wu and Bharat Bhargava "Ad HocOn-Demand Position-BasedPrivate Routing Protocol" in Proc. IEEE Transactionson Mobile Computing, 2005.
4. Zhou Zhi and Yow Kin Choong "Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy" in Proc IEEE Transactions.2005.
5. VivekPathak and Danfeng Yao "Securing Location Aware Services Over VANET UsingGeographical Secure Path Routing" IEEE Trans. Veh. Technol., 2008.
6. [6]LanjunDang andjixeu ,"Distributed Anonymous Secure Routing with Good Scalability for Mobile Ad Hoc Networks" in Proc.IEEE Transactions.2010.
7. ElaheSheklabadi, and Mehdi Berenjkou"An Anonymous Secure Routing Protocol for MobileAd Hoc Networks" in Proc. IEEEInternational Symposium on Computer Networks and Distributed Systems .2011
8. Tong Zhou, Romit Roy Choudhur "Sybil Attacks Detection in VehicularAd Hoc Networks" in Proc. IEEE Journal on Selected Areas In Communications, VOL. 29, NO. 3, 2011
9. Karim El Defrawy "ALARM: Anonymous Location-Aided
10. Routing in Suspicious MANETs" in proc IEEE Transactions On Mobile Computing, VOL. 10, NO. 9, 2011
11. Rui Jiang and Yuan Xing "Anonymous On-demand Routing and Secure Checking of Traffic Forwarding for Mobile Ad Hoc Networks"31st International Symposium on Reliable Distributed Systems 2012.
12. Haiying Shen and Lianyu Zhao"ALERT: An Anonymous Location-BasedEfficient Routing Protocol in MANETs" in Proc.

13. IEEE transactions on mobile computing, vol. 12, no. 6, 2013 SohailAbbas,MadjidMerabti"Lightweight Sybil Attack Detection in MANETs" in Proc. IEEE systems journal, vol. 7, no. 2, 2013.
14. Kuen-Han Li Jenq-ShiouLeu "Ant-based On-demand Clustering Routing Protocolfor Mobile Ad-hoc Networks,"Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing 2013.
15. Kim KyuSeok and NavratiSaxena "Analysis of a Novel Advanced Greedy Perimeter Stateless Routing Algorithm" in proc IEEE transaction 2013
16. Seryvuth Tan and Keecheon Kim "Secure Route Discovery for Preventing Black Hole Attacks on AODV-based MANETs " In procIEEE International Conference on Embedded and Ubiquitous Computing 2013
17. BehnamHassanabadi and ShahrokhValaee "Reliable Periodic Safety Message Broadcasting in VANETs Using Network Coding" In proc IEEE transactions on wireless communications, vol. 13, no. 3, 2014
18. Wei Liu and Ming Yu "AASR: Authenticated Anonymous Secure Routingfor MANETs in Adversarial Environments,"IEEE transactions on vehicular technology, vol. 63, no. 9, November 2014.
19. K.Vijayakumar·C,Arun,Continuous security assessment of cloud based applications using distributed hashing algorithm in SDLC,Cluster Computing DOI 10.1007/s10586-017-1176-x,Sept 2017
20. K.Vijayakumar·C,Arun, Analysis and selection of risk assessment frameworks for cloud based enterprise applications", Biomedical Research, ISSN: 0976-1683 (Electronic), January 2017
21. K. Vijayakumar,C.Arun,Automated risk identification using NLP in cloud based development environments,J Ambient Intell Human Computing,DOI 10.1007/s12652-017-0503-7,Springer May 2017.

AUTHORS PROFILE

Dr.A.Chinnasamy born on 26th Nov 1981 in Salem district, Tamilnadu, India. He obtained his Bachelors degree (B.E) in Computer Science and Engineering from Anna University in 2005, Master degree (M.E) in Computer Science and Engineering from Anna University in 2008 and Ph.D., Information and Communication Engineering, Anna University, Chennai, 2017. He is currently working as Associate Professor in the Department of Computer science and Engineering at Sri Sairam Engineering College affiliated to Anna University, Chennai, (INDIA). He research interest is Wireless Communication. He is a life member of the Computer Society of India (CSI), ISTE, IAENG. Reviewer in Measurement and control Journal and Wireless Personal Communication

P.Selvakumari born on 14th Mar 1983 in Salem district, Tamilnadu, India. She obtained her Bachelor degree B.Tech(IT) Anna University in 2005, Master degree (M.E) in Computer Science and Engineering from Anna University in 2009.She is currently working as Assistant Professor in the Computer Science and Engineering at Tagore Engineering College affiliated to Anna University, Chennai, (INDIA). She is a Research Scholar (Part-time) in the Anna University, Chennai-25. her research interest is Wireless Communication. She is a life member of the Computer Society of India (CSI).