Journal of Green Engineering (JGE)

Volume-10, Issue-3, March 2020

Reliable Wormhole Detection System Based Secure Routing and Authentication for Environmental Monitoring

[1]G.Mani, [2]V.Nivedhitha, [3]N.S.Pradeep,[4]T.Jayasankar, [5]K.Vinoth Kumar

[1]Assistant Professor (Sr.Gr), Department of Computer Science and Engineering, University College of Engineering, Arni, Tamilnadu, India.
E-mail: gmani1879@gmail.com
[2]Assistant Professor, Department of Computer Science and Engineering, SSM Institute of Engineering and Technology, Dindigul, Tamilnadu, India.
E-mail: nivedhitha.it@gmail.com
[3] Assistant Professor (Sr.Gr), Department of Electronics and Communication Engineering, University College of Engineering, BIT Campus, Anna University, Tiruchirappalli, Tamilnadu, India. E-mail:pine_deep@yahoo.com
[4]Assistant Professor (Sr.Gr), Department of Electronics and Communication Engineering, University College of Engineering, BIT Campus, Anna University, Tiruchirappalli, Tamilnadu, India. E-mail:jayasankar27681@gmail.com
[5]Associate Professor, Department of ECE, SSM Institute of Engineering and Technology, Dindigul, Tamilnadu, India. E-mail:vinodkumaran87@gmail.com.

Abstract

Ad hoc sensor network is a new kind of wireless networks where the sensor node or mobile sensor node can be communicated randomly. In the absence of access point, attackers are entered easily without the knowledge of source or neighbour node. Worm hole attack in the network records the packet in one route and drops it in another route which may cause congestion in the network. In this research work, Reliable Wormhole Detection System (RWDS) is proposed to provide secure routing and authentication for environmental monitoring. The system consists of three phases. In first phase, reliable routes are discovered from source to sink node. In second phase, extended coverage approach is introduced to estimate the energy during route maintenance phase. In third phase, worm hole detection

Journal of Green Engineering, Vol. 10_3, 734–749.

algorithm is proposed to detect the attackers in the network and balanced the energy in the network.

Keywords: Wormhole Attack, Ad hoc Sensor Networks, Extended Coverage Approach, Energy, Detection and Isolation of Attacks

1 Introduction

Ad hoc sensor networks play a vital role in wireless networks. It's a combination of both ad hoc and sensor networks. Vulnerability of attackers in the network is difficult to find. The network performance may get degraded due to the presence of the active and passive attackers. Ad hoc sensor networks contain no access points where it can be used for emergency and real time applications in the network. Wormhole attacks in ad hoc sensor networks affect the network Performance. Due to that, network performance may get affected. Detection and prevention of worm hole attack is of great importance. In this research, it is required to isolate the attack permanently in the network.Figure.1 shows the wireless sensor networks architecture.

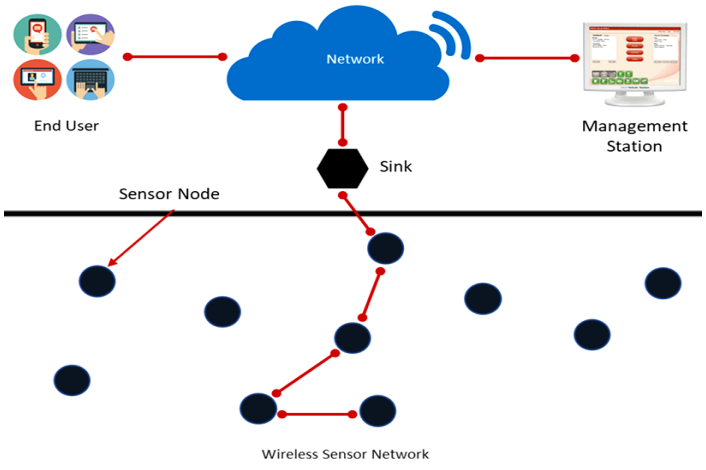

Figure 1. WSN Architecture

2 Related Works

A secure clustering routing scheme based on hybrid topology in MANET. The various types of intrusions were detected and eliminated using the new security algorithm. Meanwhile malicious nodes were identified using secure routing algorithm. In a cluster, mobile nodes may join or leave the network with the knowledge of cluster head. In existing schemes, it was found that security lapses in the network which may affect the performance of the network [1]. Based on neighbour nodes and sink node, recommendations are collected to provide the trust of each node.

The authors surveyed the various approaches, schemes, protocols and methods for the security of network. Since the MANET is a decentralized network, the vulnerability of attackers is getting increased. Sometimes it is difficult to obtain the location of attackers in the network [2]. From this analysis, it is concluded that decentralized crypto mechanism is of great importance and need.

Trust factor and Fuzzy Firefly integrated intrusion detection system. Here instead of choosing shortest path, mechanism prefers only the secure path for protecting the data from the attackers. Various trusts are calculated to provide the feasible paths from source to sink node. From the feasible paths, optimal path was found based on particle swarm optimization technique [3]. The path with high trust value was taken as best secure path for the routing. The routes are discovered and protect the data packets from misbehaving nodes thereby improving detection rate, end to end delay and packets received in periodical time.

New multilevel intrusion detection system is for identifying attackers using virtual machine level. The isolated features of data center were collected at the cloud [4]. The knowledge base center was used to store the record of internal and external attackers to enhance the future research. The central hub node was chosen in the clustered topology. The consistency between the nodes was also maintained during the detection phase. Different various tools were analysed with maximum attacks to attain the maximum reliability. The intrusion detection rate, positive alarm rate and delay were simulated for the performance analysis.

A new model for detecting packet dropping attacks in ad hoc networks. The misbehaving nodes are isolated from the network based on promiscuous nodes. The internal dropping attacks in the network increase the overhead and delay. It will lead to network degradation [5]. To avoid this, the trust threshold vector and monitoring nodes were maintained to reduce the packet dropping attacks successfully in the network.

The light weight authentication scheme is to discover security in the network. The two processes were combined i.e. alarm based reply and authenticated request procedure [6]. The safety schemes were integrated to provide node detection and secure authentication at any manner the message routing was formalized with the guaranteed security services. The solution was provided with authentication to provide data integrity and non-repudiation.

An intrusion detection system using cross layer approach [7]. The anomaly detection scheme was integrated with machine leaning approach to detect the misbehaving nodes. This approach was established based on feature selection model and generic algorithm to detect the misbehaving nodes. The classification features were extracted using the cross layer approach. The control overhead and detection efficiency was satisfied using this model. Meanwhile, the IDS efficiency was summarized under various routing attacks.

The black hole attack detection and isolation modelis a novel strategy was deployed to recognize and withdraw the malicious node from the network [8]. The novel routing mechanism was integrated based on cluster method and blacklist routing scheme. The comparative results revealed the proposed technique outperforms than existing schemes. The network efficiency was improved based on the metric of throughput.

The research on wormhole attack in ad hoc networks, the evidences and common activity procedures were formalized to sketch overview of wormhole attack [9]. The remote framework model was formalized based on wormhole strike arrangement concept. The attack model was executed to secure ambush. Various formulated technologies like reference integrated modelling, time synchronization and bundle code technology were adopted to detect the worm hole attacks in the network.

The concept of cluster based data replication algorithm was defined [10]. A set of ad hoc nodes formed the individual group and data items

were created to reduce the packet redundancy. If any path contains worm hole attack, the alternative stable path will be immediately identified and path will be isolated in future transmission.

The hybridized immune system to avoid the worm hole attacks in ad hoc network. The fuzzy decision parameters were used to reduce end to end delay, overhead and route delay in the network [11]. These parameters were converted into crisp values in order to provide secure route to avoid worm hole attack. From these parameters, the fuzzy path priority was set to determine the high stable path. If any path contains worm hole attack, the alternative stable path will be immediately identified and path will be isolated in future transmission.

A localization based load balanced routing protocol the geographical position of neighbour nodes was included during route discovery procedure. The set of disjoint routes was chosen by the sink node based on route request and route reply packets. A data lookup and aggregation scheme was focused on the issues of data availability and data collection procedure [12-14]. The fuzzy decision parameters were used to reduce end to end delay, overhead and route delay in the network. These parameters were converted into crisp values in order to provide secure route to avoid worm hole attack.

3. Reliable Wormhole Detection System (RWDS)

In this section, each node in the ad hoc environment has the limited power to broadcast the packets during route maintenance phase. Misbehaving nodes in the network creates high traffic by sending hello messages continuously. Hence the malicious nodes have to be prevented in the network. The Intrusion detection system consists of intrusion detection scheme to detect the misbehaving nodes. The extended coverage approach is implemented to cover the maximum range of network. The main objective of the intrusion detection is to reduce the traffic overload and overhead during data transmission phase.

Reliable Wormhole Detection Scheme (RWDS) is proposed to divide the network region into small groups with small set cluster members in the network. If a node with sufficient energy is considered as genuine node. If it does not have, the node will be added into blacklisted table.

The following assumptions are made in the proposed system.

i. Two set of nodes are maintained i.e. reliable and unreliable node.
ii. Trust is maintained and vector is calculated from the neighbour recommendations.
iii. In the sub-network, if the message is blocked in the route, attack may be present.
iv. Routes are bidirectional.

Figure.2 shows the wormhole attack model of security intrusion system to detect the misbehaving nodes.

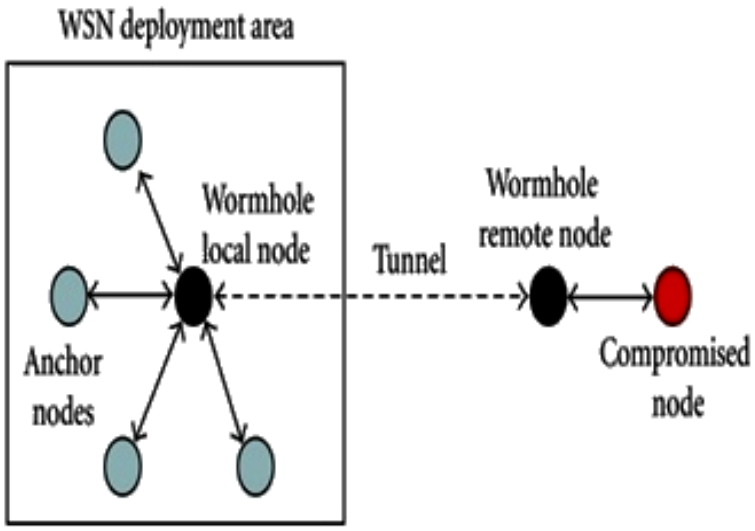

Figure 2 Wormhole Attack Mod**el**

3.1 Extended Coverage Approach (ECA)

In this phase, the node in the coverage area has the sufficient energy for future communication. All the nodes under extended coverage area are genuine nodes. The reliability and energy of a node determines the good network. Each node with trust factor is considered as reliable node.

Based on initial energy of node (IE), present energy of node (PE), Waste Energy (WE) and total energy of node (TE), the threshold factor of trust score is determined as,

$$\left(1-\frac{PE+WE}{IE}\right)\times 100 > \Gamma_T \qquad (1)$$

OR

$$\left(\frac{PE}{TE}\right)\times 100 < \Delta \qquad (2)$$

Γ_T and Δ are based on average power of the nodes in the network.

The following security model is developed against the wormhole attacks in MANET. Figure.3 shows the model of security intrusion system to detect the misbehaving nodes.

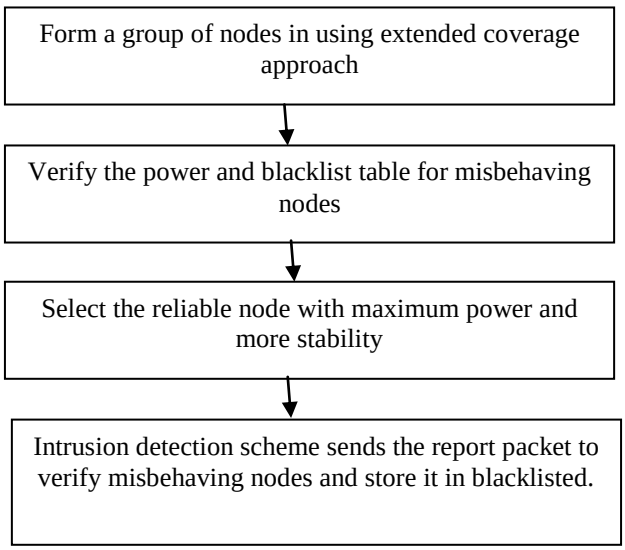

Figure 3 Security Intrusion System

3.2 Wormhole Detection Algorithm

This algorithm aims to detect the wormhole attacks in the network. The attacks are detected based on trust vector routing. The following steps are used to detect the attacks.

Step 1: Set the network by choosing the reliable node with sufficient energy to send the report packets in the network.
Step 2: Intrusion detection scheme predicts the nodes in the route and if any misbehaving nodes are present, it will be added in the black list.
Step 3: Source node sends the packets to sink node via intermediate node with no misbehaving nodes to improve the throughput.
Step 4: The received packets from sink node towards source node without any uncertainty.
Step 5: Each node maintains the trust vector. If any falls below the threshold vector of source node, it will be considered as misbehaving node.

Step 6: Source node chooses the alternative path to route the packets via trust vector routing.
Step 7: Source node identifies the wormhole attack where it can observe the packets at one end or drop the packets at another end.

4 Results and Discussions

The simulation results of RWDS are simulated using network simulator tool version 2.35. Here the number of nodes used for simulation is 150 nodes. The coverage area size is 1100 x 1100 sq.m. The MAC id used here is 802.15.4 is shown in Table1.Ad hoc on demand multipath vector routing protocol (AOMDV) is used as basic routing protocol.

Table 1 Simulation Metrics of RWDS

No. of Nodes	150
Area Size	1100 X 1100 sq.m
Mac	802.15.4
Radio Range	100 meter
Simulation Time	100 sec
Traffic Source	Poisson
Packet Size	80 bytes
Mobility Model	Random Walk
Protocol	AOMDV

4.1 Performance Metrics

The following metrics are evaluated using network simulator tool.

Wormhole Detection Ratio: It is the ratio of detected worm hole attacks to the total number of nodes in the routing.
Packet Delivery Ratio: It is the ratio of packets received to toe number of packets sent.

Path Reliability Rate: Number of reliable and secure paths to the total number of paths available.
Network Lifetime: It is the total number of energy allocated for packet transmission in the nodes.
Non Repudiation Rate: It is the number of nodes denying the sent packets towards the sink node.

Figure.4 shows the performance of RWDS in terms of packet delivery ratio while varying the number of nodes in x axis. From the

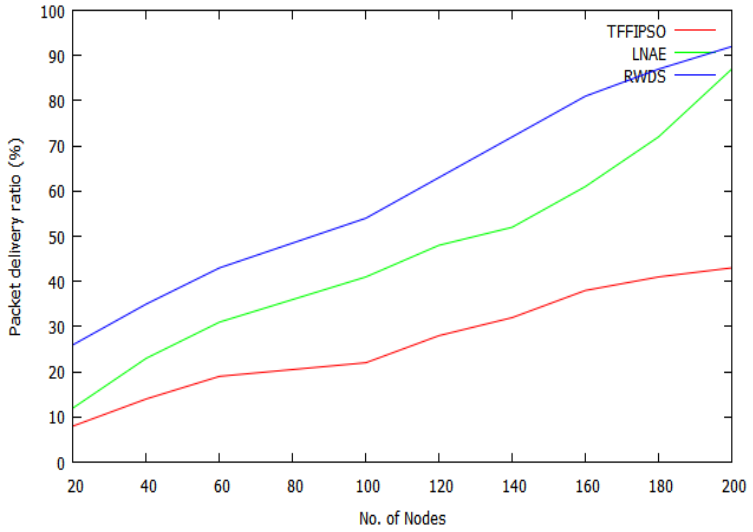

Figure 4 Packet delivery ratio Vs No. of Nodes

results, it is seen that the proposed system achieves high packet delivery ratio than existing schemes. In the proposed system, the attackers are detected and prevented from the network permanently. Due to that, the proposed system achieves high rate than existing schemes.

Figure.5 shows the results of non-repudiation rate for proposed and existing schemes. The number of nodes is not denied the sent packets to sink node. It is because of channelization of routes.

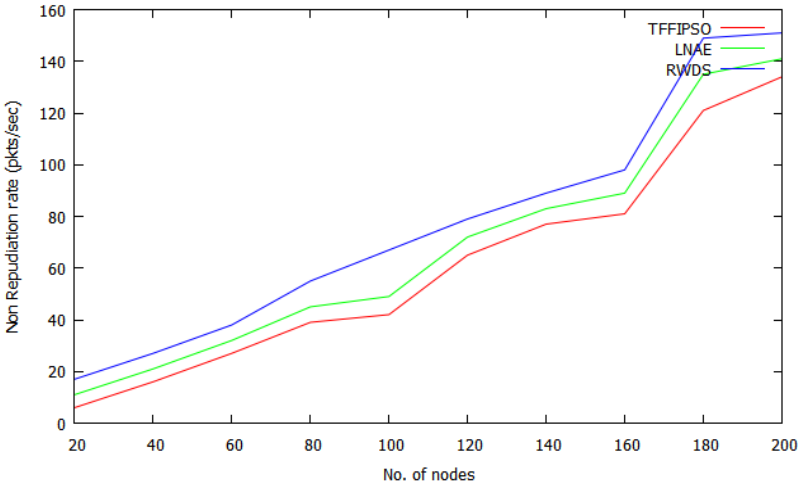

Figure 5 NonRepudiation Rate Vs No. of Nodes

Figure.6 shows the performance of path reliability rate while varying number of paths in x axis. From the results, it is seen that proposed system achieves high path reliability rate than existing schemes.

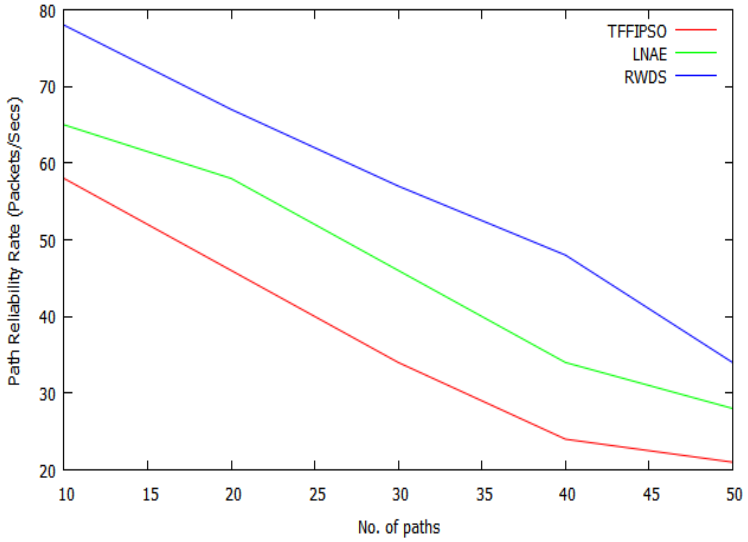

Figure 6 Path Reliability Rate Vs No. of Paths

Figure.7 illustrates the analysis of control overhead for proposed system and existing schemes. From the results, it is seen that RWDS produces less overhead than existing schemes due to wormhole detection.

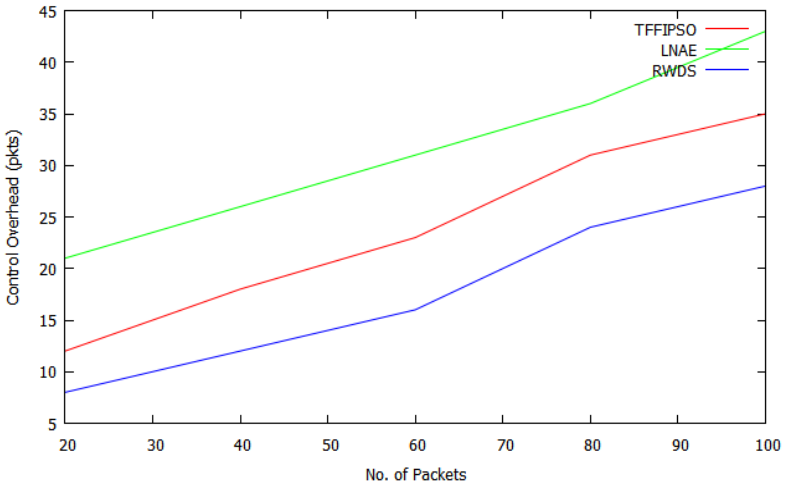

Figure 7 Control Overhead Vs No. of Packets

Figure.8 illustrates the performance of network lifetime for proposed system and existing schemes. It is concluded from results, RWDS achieves more network lifetime than existing schemes.

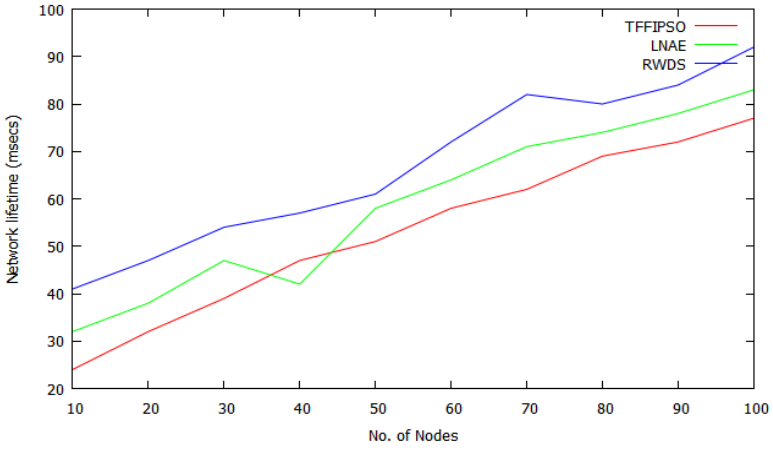

Figure 8 Network Lifetime Vs No. of Nodes

5 Conclusion

Attacks in the Ad hoc sensor networks are easy to impersonate the nodes. It is difficult to find the attacks in the network. In this research work, reliable worm hole detection system is introduced to detect the attacks and prevent from the network for environmental monitoring. The concept of extended coverage approach and worm hole attack detection are implemented in the routing. Extensive simulation results are performed in the network using NS2. The proposed system RWDS achieves less overhead, high path reliability rate, high network lifetime, high packet delivery ratio and non-repudiation rate than existing schemes. In future, it is planned to detect gray hole and black hole attacks while balancing theenergy in the network.

References

[1]K.VinothKumar, T.Jayasankar, M.Prabhakaran and V.Srinivasan, "Fuzzy Logic based Efficient Multipath Routing for Mobile Adhoc Networks", Appl. Math. Inf. Sci.,vol.11, no.2, pp.449–455, 2017.

[2]K.Vinoth Kumar, V.Eswaramoorthy, S.Nagakumararaj and J.Wilson, "Fuzzy Clustering Enchanced Multipath Routing to Enhance the Network Lifetime in Wireless Sensor Networks", International Journal.of Scientific & Technology Research, vol.8, no.11, pp.3415-3420, 2019.

[3]Ramireddy Kondaiah and 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 Advanced Computer Science and Applications, vol. 9, no. 3, pp.13-33,2018.

[4]S.Pramela Devi, V.Eswaramoorthy, K.Vinoth Kumar and T. Jayasankar, "Likelihood based Node Fitness Evaluation Method for Data Authentication in MANET", International Journal of Advanced Science and Technology, vol. 29, no.3, pp. 5835 – 5842, 2020.

[5]C.Tabassum Begum, Atheeq, Syed Raziuddin, Arshad Ahmed Khan Mohammed, "Eliminating Intentional Packet Dropping Attacks in MANETs Using Promiscuous Mode", International Journal for Research in Applied Science & Engineering Technology, vol. 6, no.3, pp. 2591-2598, 2018.

[6]K.Vinoth Kumar,S.Bhavani, "An Effective Localization based Optimized Energy Routing for MANET" Journal of Theoretical and Applied Information Technology (JATIT), vol.77,no.2, pp.291-299, 2015.

[7]Shalu Malik and Anil Kumar Sharma, "Detection And Isolation Technique For Blackhole Attack In Wireless Sensor Network", International Journal of Computer Engineering & Technology, vol.9, no.1, pp.66-73, 2018.

[8]S.Pramela Devi, V.Eswaramoorthy, K.Vinoth Kumar , T.Jaya Sankar, "Likelihood based Node Fitness Evaluation Method for Data Authentication in MANET ", International Journal of Advanced Science and Technology, vol.29, no.3, pp.5835~5842,2020.

[9]K Spurthi, T.N.Shankar, "A Research on Wormhole Attack in Mobile Ad-Hoc Networks",International Journal of Recent Technology and Engineering, vol.8, no.1S4, pp.1136-1141, 2018.

[10]S.Gopinath, K.Vinoth Kumar and T.Jaya Sankar, "Secure Location Aware Routing Protocol With Authentication For Data Integrity", Cluster Comput , vol.22, pp.13609–13618, 2019.

[11]M.Sujatha, N,.B.Prakash, G.R.Hemalakshmi, T.Jayasankar "High Performance Grouping With Load Balancing Scheme for Wireless Sensor Networks" International Journal of Advanced Science and Technology, vol.28, no.12, pp. 441-449,2019.

[12]K.Vinoth Kumar, S.Bhavani, "Trust Based Multipath Authentication Protocol for Mobile Ad Hoc Network" , Journal of Computational and Theoretical Nanoscience (CTN), vol.12, no.12, pp. 5479-5485, 2015.

[13]K. B. Gurumoorthy, S. Gopinath, K. Vinoth Kumar, "Ant Colony Optimization and Genetic Algorithm Integrated Load Balancing Approach for MANET", International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol.8, no.5, pp.399-405, 2019.

[14]E.Vishnupriya, T. Jayasankar and P.Maheswara Venkatesh,"SDAOR: Secure Data Transmission of Optimum Routing Protocol in Wireless Sensor Networks For Surveillance Applications", ARPN Journal of Engineering and Applied Sciences, vol. 10, no.16, pp.6917- 6931,2015.

Biographies

G.MANI has finished his B.Tech in Information Technology from Madras University, Chennai,Tamil nadu in 2002 and M.E in Computer Science and Engineering from Anna University, Chennai,Tamil nadu in 2008. From 2009 to 2014 he has an Assistant Professor in the Department of Computer Science and Engineering of Anna University ,BIT Campus,Tiruchirappalli,Tamilnadu, India. Since 2014 he has been an Assistant Professor(Sr.Gr) in the University College of Engineering Arni, Anna University, Chennai, Tamilnadu, India. He is a member of CSI.He has published 1 paper in the reputed international Journal and 6 papers in the international Conferences. His research activities are focused on Data Mining, Mobile Ad hoc networks and Sensor network.

V.NIVEDHITHA is working as an Assistant Professor in the department of Computer Science and Engineering at SSM Institute of Engineering and Technology. She has a teaching experience of 7 years in reputed Engineering Colleges. She is currently pursuing her Ph.D. degree in the Faculty of Information and Communication Engineering, Anna University, Chennai. She is a life member of Indian Society for Technical Education (MISTE). She has published 1 paper in International Journal, presented 6 papers in International Conferences, 2 papers in National Conferences published several books. Her

field of Interest includes Wireless Sensor Networks and Internet of Things. She has attended several FDPs,workshops and seminars.

N.S.PRADEEP, Assistant Professor in the Department of Electronics and Communication Engineering, Anna University-BIT Campus, Tiruchirappalli, Tamil Nadu. He obtained his Ph.D degree in Wireless Communication from Anna University, Chennai in 2019, M.E in Applied Electronics from Kongu Engineering College, Erode, Tamilnadu and B.E in Electronics and Communication Engineering from Anna University, Chennai. He has published 9 papers in international journals, 2 papers in national level conferences and 11 papers in international conferences. His areas of interests are Advanced DigitalCommunication, MIMO-OFDM and 4G.

T.JAYASANKAR working as an Assistant Professor in the Electronics and Communication Engineering Department, University College of Engineering, Anna University, Bharathidasan Institute of Technology Campus, Tiruchirappalli, Tamilnadu, India. He received the B.E. Degree in Electronics and Communication Engineering from Bharathiyar University, Coimbatore in 2001 and M.E. Degree at Madurai Kamaraj University, Madurai in 2003 and Ph.D. in Speech Processing at Anna University Chennai 2017. He is a Member of IEI, ISTE. He has been a Lecturer at graduate and post-graduate level and has participated in a number of international and national level conferences and workshops. He has published more than 35 papers in the reputed international journals including science indexed journals and Scopus indexed journals, 20 papers in the international and national conferences. His main interest is currently speech synthesis, speech and image processing and wireless networks.

K. VINOTH KUMAR working as Assistant Professor in SSM Institute of Engineering and Technology, Dindigul ,Tamil Nadu, India. He received the Bachelor's Degree in Electronics and Communication Engineering from the Kurinji College of Engineering and Technology, Manapparai, Tamilnadu, India, in 2009. He received the Master's Degree in Applied Electronics from the J.J. College of Engineering and Technology, Tiruchirappalli, Tamil Nadu, India, in 2011. He received the Ph.D. in Karpagam University Coimbatore, Tamil Nadu, India in 2017. He is a Member in Universal Association of Computer and Electronics Engineer (UACEE) and Member in International Association of Engineer (IAENG). He published more than 35 international journals including science indexed journals and Scopus indexed journals. His research interests include wireless communication, mobile ad hoc networks, wireless sensor networks and communication networks.