IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

Misbehaving Node Identification using I-GTA in MANET

A. Sushma[1], T. Manjula, M.E [2]

M.E Scholar, Hindustan College of Engineering, Coimbatore, India[1]

Professor, Department of E&I., Hindustan College of Engineering, Coimbatore, India[2]

Abstract: Mobile Ad hoc network is a secure data transmission model for the data. The nodes that present in the network was mobile nodes. It means they can design as the static node as well as the mobile nodes. The mobile nodes are the data transmission paradigm that is the emerging technology. This is based on the simple notation of data packet transmission. The drawback that most commonly occur during the data transmission was data forwarding attack. The attack mostly done by the malicious node. In which the nodes are used to avoid the transmission by without sending the data to the neighboring node. This should be avoided and overcome in the proposed mechanism. The proposed model consist of a secure protocol design for packet forwarding in MANET. Here the nodes are flexible by they can fix as a static node, otherwise the mobile nodes. The nodes are grouped into clustering by applying strong and robust improvised clustering algorithm. In which the data securely transmitted beyond the network of which it determined. The most upcoming strategies of applying this paradigm is mainly focused on the security data transmission in the network. This can be finally focused with the simple mobile data transmission. The proposed model introduced a novel scheme for data transmission. They are the punishment and bonus point credit for the data transmission. The bonus point for the true node is credited by applying the I-GTA mechanism. This mechanism is applied by introducing the Supervising agent. The Agent node is placed in each cluster for the data transmission. Thus the proposed technique is simple and efficient model for processing the data.

Index Terms: MANET, SA, AODV, Data Transmission, I-GTA

1 INTRODUCTION

Mobile Ad Hoc Network is a simple and efficient mechanism through which the data is transmitted from the source to destination. The main use of the WSN is to maintain the security of the data packet while it travels from one hop to another. Hop will easily misbehaved through the energy wastage. [1] Thus WSN process is a complexity network to transmit the data onto one source to another. Mobile Ad Hoc Network is mostly constructed with the help of set of nodes. And the process of performing the data transmission is based upon simple and efficient scheme. The nodes are interconnected with the help of links and routers.
The main use of the processing ability is to transmit the data from one to another in a single and multi- node.

W. Mao the research scholar who expands the Modern theory of cryptography that will increase the security of the passage through which the data can be safely protected in a unique format. This should be further added to the network to transmit the data with integrity constraints. [2] Adi Shamir express the idea of threshold scheme that can be very helpful in the cryptographic keys. We can encrypt the data to protect it. Threshold scheme is highly untrustworthy since a single misfortune can make the information inaccessible.

The previous model focus on reducing the packet dropping attack by implementing several process step activities. The systematic development of the model is used to develop the execution of the auto correlation process. A simple mathematical representation is used in above process. The node activities can be easily changed by performing the simple and efficient process. This should be easily processed by checking the packet dropping framework of the system. A diagrammatic representation of the model is shown below.

Lamport says “A method of user password authentication is described which is secure even if an intruder can read the system's data”, and can change by monitoring the communication between the user and the system [3]. This method is implemented with a microcomputer in the user's terminal and assumes a secure encryption method. Thus more or less every user needs to perform some other performance related activities to protect their own data. [4]Vanstone told that the pass breakers are more or less it can be used to produce the possible declaration of the system though the concept of simple and elegant format. Most of the methods focused to avoid the packet dropping attack for the simple data transmission. As shown in the above diagram the data that is stored in simple and efficient model. User is responsible to maintain the system and transmit the data from the unsecured network. The packets are transmitted in the network

and the packet dropping attack is easily solved by the mechanism is overcome by the system representation. The previous RIP and AODV protocol is not useful for processing data in the complex network.

A mobile ad hoc network is formed by wireless hosts which may be mobiles that are capable of communicating with each other and infrastructure less network. MANET is particularly vulnerable due to its fundamental characteristics, such as open medium, dynamic topology, distributed cooperation, and constrained capability. [5] MANET problems are not easy to solve. The routing security issues of MANETs, and the "black hole" problem-analyze that can easily. [6] The main routing security issues of "black hole" problem that means "node can be received data but it does not send data with its neighbor". Another problem "sinkhole" problem that means "user assign unique information which node has present that information that node its trustworthy node". We also propose a solution for the black hole problem for ad hoc on-demand distance vector routing protocol. There are two types of networks. a. Flat based network and b. cluster based network. Flat based network each nodes are interconnected with its neighbor nodes. But the cluster based network is simple and it's used to easy. When compared with the flat based network. Here the cluster based network is more efficient than the flat based system. Thus the node equality is commonly grouped into the system. The proposed model is suitable for both flat based and the cluster based concept.

Another type of network is called as VANET, [7] B.Ramakrishnan, R.S Rajesh, R.S Shaji describe speed and time in which the messages send and received in the intelligent transfer system. For this purpose VANET is used for this purpose a simple highway vehicular model in which a new clustering concept is introduced among the MANET node.[8] B.Ramakrishnan., M. selvi., R. Bhagavanth Nishanth proposed, the main purpose of the mobility model is to reproduce the movement features of vehicle in VANET. Mahattan mobility model is used by many researchers. To move packet among the vehicles a competent routing protocol is used.

[9].Dr.B. Ramakrishnan. Proposed a cluster based simple highway mobility model with routing AODV. The VANET MAC layer is used to measure packet receiving time and packet delivery ratio. This paper also describes analyzation of services discovery procedure. [10] M. Milton Joe. Dr.B. Ramakrishnan., Dr. R.S Shaji describe a comprehensive characteristics of vehicular network and also design a new GSM based mobile network communication in vehicular network. It establishes communication between vehicle and mobile phones. It proves its efficiency by the metrics of the GSM based mobile network communication.

2. RELATED WORK

[11] Tao Shuand Marwant Krunz proposed and elaborates the idea about Mobile Data Offloading in an offload infrastructure. User forwarding the packets using hand held devices through access points. Each data packet should reach the destination correctly is one of a challenging task. Customers willing to forward the data packets across the network, it may depend on the others and traffic may occur. This model proposed how the data packets successfully reach the destination with "tightness" concept. This system promotes to reduce the network resource utilization and cooperative behavior among other nodes.

[12]B. Awerbuch, R. Curtmola, D. Holmer proposed Airborne network is an evolving field in the wireless networks. Airborne network is an efficient routing protocol and it is suitable for larger size network. It is based on performance, routing model, network structure, methodology. Performance of routing protocol is test by a simulator. Performance like packet delivery ratio and time is varied depend on the other nodes in the network. These parameters are considered for evaluating routing protocol. Method used in the AeroRP similar to the discovery of neighbors is varied for different protocol.

[13]K. Balakrishnan, J. Dengand P. K Varshiny proposed routing protocol in mobile ad-hoc networks. Network is a collection of nodes which are connected dynamically without using any infrastructure. There are various types of routing protocols have been implemented such as OLSR, DSR, YMO, AODV, DSDV, BATMAN etc. The comparison is based on relative DYMO, OLSR and DSR protocols. These protocols are implemented in a different simulation environment. The proposed work has been selecting a suitable routing protocol. These three protocols are simulated in a sample network using set of parameters.

[14]E. Gerhards Padilla, N. Aschenbruck, P. Martini, M. Jahnke and J. Tolle proposed a mobile ad hoc network (MANET) has no centralized administration. In MANET the collection of mobile ad hoc node are act as self-organized nodes with dynamic topology. It has no pre-existing infrastructure. MANET nodes act like both host and the router. It transfer the data using multi-hop way to each other by forwarding packets. The fundamental characteristics are open medium, dynamic network topology, management are deficient in network are particularly affected by various type of attacks. Many other secure and robust routing protocols have been designed and many security schemes have been

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

recommended to tackle these issues in the security. In MANET, routing attacks are particularly severe due to presence of malicious nodes.

[15]Abubakar Karabade; Gurkan Tuna the layers of OSI model are targeted by many security issue. There are different types of attacks such as Distributed Denial of service, Man-In-Middle and IP Spoofing attack .This paper tries to overcome these attacks

[16]W. Yu, Y. Sun and K. R. Liu proposed how to prevent the vampire attacks in many popular protocols. This model provides methods to reduce the attack in a Cluster Head. Cluster Head employs in vampire attack and distributes the packet to destination without dropping the packet. This gives a successful and reliable message delivery even in case of Vampire attack. In worst case, Network-wide energy increased by single Vampire usage.

The previous paper mention is not simple and cost effective. To overcome this model the data processing is substitute with simple and efficient way through which it can be designed and perform for a previous day process in an elegant way. Thus the proposed model is implemented to design a perfect format for performing a simple transaction processing for the system. The different way of processing issues can be maintained the network as a simple and efficient way for processing the input.

[17] Dr. B. Ramakrishnan., S.R Sri Dhivya., M. Selvi proposed a design of adaptive routing protocol based on cuckoo search algorithm. This protocol combines topology and geography routing protocol and provide the secure transmission of data with less delay and high packet delivery ratio. To find the route this algorithm use a local stochastic broadcasting.

[18]A. Anuba Merlyn and A. Anuja Merlyn proposed an energy efficient routing approach and a new algorithm called descriptive delay function .In that algorithm RTS/CTS message handshaking mechanism used for data forwarding.

[19] MuhammetBaykara., Resul Das proposed honeypot system combine with IDS/IPS. Honeypots are used to analyse real time malicious attack. This system reduced the falls positive alarm level. IDS combine with honeypot are able to detect new attack.

[20] R.S Shaji., B.Ramakrishnan. R.S Rajesh describe a routing scheme called SFUSP used for finding best path in heterogeneous environment. This scheme works with efficient broadcasting technique and cluster based message passing method is used to find the weaker nodes.

3. PROBLEM IDENTIFICATION

The problem identified in the previous scheme was very vulnerable. The data that is transmitted over the network with efficient methodology is not appropriate. In previous model pairwise linking model is used. In this model the nodes are grouped together and they form the cluster with simple admiring properties. These properties are maintained by the sequence of which it could be maintained by the simple scheme for data forwarding. First the node are properly linked and merged into a simple scheme of which it could be grouped together. The grouped model is named as the cluster forming sequence. The cluster forming model is then popularized into the simple data transmission strategy model. The simple model is used for the secure data transmission. The nodes may behave through their identity in which each node get transmitted into the path of which the routing specified by the source user. Such like that the main credential of the source node is used to select the simple data transmission of which it could be used. The main use of the simplest form of the data uploading model is maintained in a continuous sequence of execution strategy. The malicious node get involved when the data packet get transmitted.

At this point the auditing node which is used to monitor the sequence of application will be used to maintain under the sequence of which it could be used. The auditing node can be followed by the sequence of operation of which it should be used. Then the auditing node eliminate the node from the network. Thus the malicious node send out. But the drawback behind in this situation is still it used to behave the node inside the network. In which the data can be easily processed with the additional data package transmission. Using this model it is still a major drawback in the network. Thus the energy of the node is still remain present in the node. This can be further not avoided by the node of which it should be used. Thus the model can be maintained with the simple could be used for the further data transmission of which it should be used. The energy stamina is still retain in the network. It may misbehave the other packet during the data transmission. This can be modified and overcome in the proposed model of application of which it could be used. Thus the data transmission of the malicious node is overcome by punishing the node with certain other sequencing model of which it should be used.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

DISADVANTAGE

- The data packet transmission is spoiled by the Malicious node
- The next sequence of the data transmission is not simple and efficient
- This can be maintained under the sequence of data transmission of which it could be used.
- The malicious node can be maintained under the sequence of which it could be used for the data transmission can be used.

Architectureof Cluster Formation

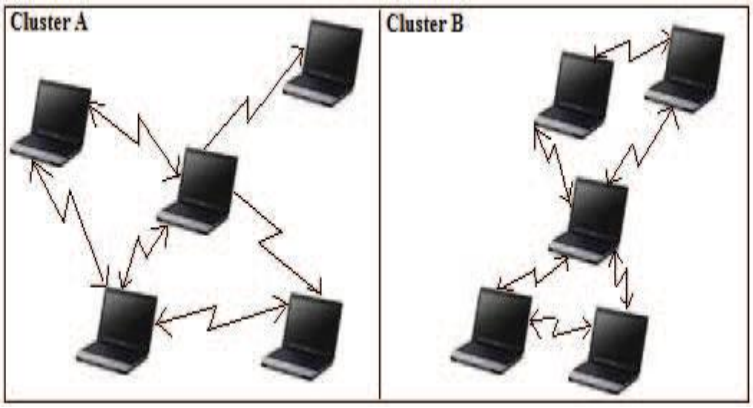


Figure 1: Cluster formation

The cluster forming ability is introduced in this project. Here the group of nodes are located in various location. The location based data transmission is based upon the simple and efficient data processing of which it can be used to transmit the data. The data transmission taken place without clustering is a time consuming process. And this can be maintained with the simple routing process. Then the data which is transmitted along the cluster formation is then placed to maintain in a simple and efficient scheme for maintaining the simple priority of the data to be get transmitted. This could be further imagined by the scheme of which it should be played in a simple Hello packet transmission methodology. The main use of the data transmission is used to get along with the packet transmission scenario of which it could be used. This can be further improved by the sequence of which it could be maintained by the additional working sequence. The data transmission can be maintained by avoiding the time consuming paradigm of which it should be used for further data classification. The data can be maintain under the sequence of which it could be played and monitor by the simple routing sequence of which it could get transmitted along the path. Then the sequence of data transmission is fully admired by the previous scheme of which it could be run under the previous concept of which it could be used. The drawback is concern and analyzed then overcome in the proposed scheme of application of which it could get transmitted. The main use of the scheme of which it could be maintained ion a simple set of process of which it maintained in the simplest form of usage of which it can be performed.

4. PROPOSED MODELING

MANET which contains both legitimate nodes and selfish or considered. Nodes are operated with battery power supply and can move within the limited network range called *clusters* without any restrictions. Nodes can either join or leave a cluster at any time. Reactive routing protocol DSR is proposed. To find the simplest route for transmission.

I-GTA is used to find the malicious node inside the cluster. In this process the nodes are transmitted with the simple hello packet transmission. Thus when the data is transmitted the nodes are identified by the auditing node. Before that routing task assignment is proposed. The packets are transmitted with the I-GTA concept. Malicious node detection taken place at the next process.

I-GTA referred as **I**ntegrated **G**ame **T**heoretical **A**pproach. The main use of I-GTA is used to identify the malicious node by sending a simple Hello Packet Transmission. Malicious node is also available inside the cluster. The identification of the malicious node inside the cluster is complex. This can be done by proposed novel algorithm. The I-GTA transmit the Hello packet throughout the cluster.

The node with proper ID will decrypt the packet and the node without any proper information may not respond. During this process the neighbouring node automatically identifies the misbehaving node. Finally the particular node is eliminated from the cluster. This should be done with the help of I-GTA model. Then the original packet is send through the destination. The proposed architecture design is implemented in the next section.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

4.1 PROPOSEDARCHITECTUREMODELING

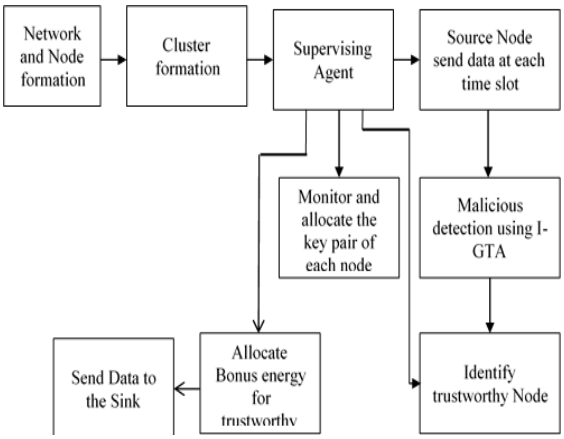


Figure 2: Architecture of Proposed Modeling

The proposed model design is modelled in the above slide. The first step is network initialization and Node formation. The next step is the cluster formation. Cluster is formed using nearest node selection. The next step is to elect the Supervising Agent (SA). Here the usage of the supervising agent is to monitor the behaviours of all the nodes. The next responsibility is used to provide the public and private key pairs to the respected node before transmission. The key is used to check the malicious behaviour of each node while transmitting the data. The next step is to send data by the source node with the respected time slot. While data transmission each cluster SA is used to check the node behaviour using public and private key. If any of the node not sending the data is detected using I-GTA model. I-GTA is used to check the nodes behaviour individually while they are not sending the data. Now the detected malicious node get punished by removing the data from the cluster. The node which truthfully transmit the data get bonus energy by updating the energy value by 5. Likewise the reward and punishment is provided by the supervising agent. The proposed model can help the node to transmit the data efficiently. Now the data that successfully transmitted to the sink.

IMPLEMENTATION

Network Setup

Network formation is the initial step to transmit the data along source to destination. Here source node, destination node and supervising agent performs a major role in network formation. The main responsible of supervising agent is to monitor all the nodes with their keys. Also SA helps to find the trustworthy node in the network formation.

Cluster Formation

The objective of a player is to maximize its own rewards or bonus values earned for successful packet transmission. For misbehaving node detection, the SA will periodically require forwarding history of every node in a cluster. It keeps track of the sequence number of forwarded packets and the number of packets successfully forwarded by each player during the time. Each player earns its bonus based on the action performed. The optimal strategy chosen by each source and destination pair will be affected by the past play strategies as well as the future outcomes of the play. Thus, a player will make decision to cooperate in forwarding packet by comparing current bonus value and its imminent chance to get payoffs. The non-cooperating player will be penalized and gradually isolated from the cluster. The intermediate players will receive a bonus *b* as an incentive from *SA* for successfully forwarding the message. The supervisory game theoretical model is given by the following definition.

Data Transmission

Data transmission is the third module. Here the process of data transmission taken place. It is done based on Hello Packet and Original data transfer manner. Initially the hello packet message will be send to the Supervising Agent node. From here the data to be transferred to other nodes. Here SA acts as supervising of all other nodes.
If SA finds any misbehaving node then it removes the corresponding node from the cluster forming mechanism. For this uses AODV protocol for implement this work. Then the original message will be shared to all other nodes.

Bonus Allocation

At the start of each time slot, each player selects a play strategy to perform its action. The play strategy may dynamically vary according to the player's type and their actions.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

5. RESULT AND DISCUSSION

Final data transmission and their sequence of packet forwarding is simple and efficient for the PDR calculation. The simulation result discussed below.

Simulation Parameters	
Area	870m × 870m
Nodes	50
Nodes Speed	3 m/s
Simulation Time	400 s
Traffic Sources	12
Traffic Type	CBR(Constant Bit Rate)
Packet Size	512 bytes
Start or Traffic	30 s
End of Traffic	380
Transmission Power	1.4 W
Reception Power	1.0 W
Idle Power	0.0 W

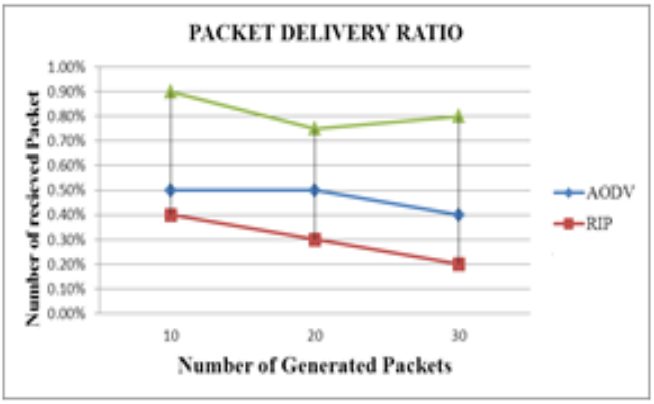
Table 1: Performance Analysis Packet Delivery Ratio

Number of packets transmitted	PACKET DELIVERY RATIO	
	EXISTING SYSTEM	PROPOSED SYSTEM
	RIP	**AODV**
10	0.4%	0.9%
20	0.3%	0.75%
50	0.2%	0.8%

Table 2: Packet Delivery ratio

The packet delivery ratio is used to compare the routing methodology of the above table. The comparison includes the proposed routing table AODV with the existing table and the RIP comparison form of routing information. This model is used to calculate the packet delivery ratio for the above format through which it can be used to process. This can be mentioned and follow by the adaptive mechanism of the above format. The calculation format can also be required for the above mechanism they are derived below

$$\textbf{\textit{Throughput}}=\frac{Numberofpacketsrecieved}{NetwortkOperationTime}$$



Graph Packet delivery ratio

6. CONCLUSION

An integrated supervisory game theoretical approach is proposed for mobile ad-hoc networks. The selfish nodes gain their payoff when they relay packets for other nodes. Nodes have to cooperate with others and relay packets for other nodes to maximize their bonus values. Proposed Model ensure the timely delivery of packets to their destinations in MANETs. Thus the proposed mechanism will provide a simple and data can be used. The main usage of the proposed model can be maintained in the simple transmission protocol. In future this can be further implemented by the proposed mechanism of which it could be enrolled by robust routing protocol namely OLSR routing protocol.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

7. REFERENCES

[1]. K. Gaj and P. Chodowiec, "FPGA and ASIC Implementations of AES," Cryptographic Engineering, pp. 235-294, Springer, 2017.
[2]A. Shamir, How to Share a Secret, Communications of the ACM, 22(11): 612-613, November 2016.
[3].L.Lamport, Password Authentication with Insecure Communication, Communications of the ACM, 24(11): 770-772, November 2014.
[4]. A. J. Menezes, P. C. van Oorschotand S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, October 2016.
[5]. H. Deng, W. Li and D. P. Agrawal, Routing security in wireless adhoc networks, IEEE Commun. Mag., 40(10): 70-75, October 2016.
[6].SuparnaBiswasSubhajitAdhikari Department of ComputerScience& Engineering MaulanaAbulKalam Azad University ofTechnology, W.B Department of Software Engineering Maulana AbulKalam Azad University o fTechnology, W.B. A Survey of Security Attacks, Defenses and Security Mechanisms in Wireless Sensor Network International Journal of Computer Applications (0975 – 8887) Volume 131 – No.17, December2015
[7].B.Ramakrishnan ,R.S Rajesh ,R.S ShajiA Efficient Vehicular Communication Outside The City Environment. [8].Dr.B.Ramakrishnan.,M.selvi.,R.BhagavanthNishanth Efficient Measure Of Routing Protocols In Vehicular Ad Hoc Networks Using Freeway Mobility Model.
[9]. Dr.B.Ramakrishnan., Performance Analysis Of AODV Routing Protocol In Vehicular Ad Hoc Network Services Discovery Architecture
[10]M.Milton Joe .,Dr.B.Ramakrishnan ., Dr.R.SShaji Modeling GSM Based Network Communication In Vehicular Network.
[11].TaoShuand Marwan Krunz,Fellow,IEEE, "Privacy Preserving and Truthful Detection of Packet Dropping Attacks in Wireless AdhocNetworks", IEEE Transactions on Mobile Computing,vol.14,no.4,April 2015.
[12].B.Awerbuch,R.Curtmola,D.Holmer,C.Nita-Rotaru, and H.Rubens, "ODSBR: An on demand secure byzantine resilient routing protocol for wireless ad hoc networks",ACMTrans.InformSyst.Security,vol.10.no.4,pp.1-35,2017
[13].K.Balakrishnan,J.Dengand,P.K.Varshney,TWOACK:Preventing selfishness in mobile ad hoc networks,"inProc.IEEEWirelessCommun.netw.Conf.,2015,pp.2137-2142.
[14]. E.GerhardsPadilla, N.Aschenbruck, P.Martini, M.Jahnke and J.Tolle. Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs, InProc. Of the 33rd IEEE Conferenceon Local Compute rNetworks(LCN), Dublin ,Ireland,and October 2017. [15].ResulDaş Department of Software Engineering, Technology Faculty, Firat Univ., 23119 Elazığ, Turkey Abubakar Karabade ; Gurkan Tuna Common network attack type and defense mechanisms
[16].W.Yu,Y.Sun and K.R.liu ,HADOF:Defense Against Routing Disruptions in mobile ad hoc networks,InProc.24thIEEEINFOCOM,Miami,USA,March 2015. [17].Dr.B.Ramakrishnan.,S.R Sri Dhivya.,M.SelviAdaptive Routing Protocol Based On Cuckoo Search Algorithm(ARP-CS)For Secure Vehicular Ad Hoc Network(VANET).
[18] A new packet loss concealment algorithm in VoIP, Qingsong Xie, Wei Wei, Quji Chen Xi'an Communication Institute Shanxi,2016
[19]Rami Cohen and Yuval Cassuto, "Coding for Improved Throughput Performance in Network Switches," Introduction to Wireless and Mobile Systems, Brooks/Cole-Thomson Learning, 2015
[20]Xiaofeng Gao, Xudong Zhu, and I. Wassell, Fan Wu, Guihai Chen, Ding-Zhu Du and Shaojie Tang "A Novel Approximation for Multi-Hop Connected Clustering Problem in Wireless Networks," in Proceedings. SIGCOMM'04 Workshops, pp. 191-196. 2016,
[21]Miao Zhao, Yuanyuan Yang, and Cong Wang, "Mobile Data Gathering with Load Balanced Clustering and Dual Data Uploading in Wireless Sensor Networks," in Proceedings. 1st Int. Symp. Modeling and Optimization in Mobile, Ad-Hoc and Wireless Networks (WiOpt'03), 2015.
[22]Prashant Dewan and Partha Dasgupta, "On Using Reputations in Ad hoc Networks to Counter Malicious Nodes", Communication and Multimedia Security 2002, Slovenia, September 26-27, 2014
[23]Y.-C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless AdHoc networks", In Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications, IEEE, Calicoon, NY, June 2014.
[24]P. Dewan, P. Dasgupta & A. Bhattacharya, "On using reputations in Adhoc networks to counter malicious nodes", QoS and Dynamic Systems, (IEEE ICPADS), Newport Beach, USA, 2014.
[25]L.Buttyan and J.-P.Hubaux, "Nuglets: a virtual currency to stimulate cooperation in self-organized ad hoc networks", Technical Report DSC/2001/001, Swiss Federal Institute of Technology – Lausanne
[26]Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks", in The 8th ACM International Conference on Mobile Computing and Networking, September
[27]R. M. P. Michiardi, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile Ad hoc networks", In Communication and Multimedia Security, IEEE, Portoroz, Slovenia, pp.107-121
[28] P. Marbach and Y. Qiu, "Cooperation in wireless adhoc networks: a market-based approach," IEEE/ACM Transactions on Networking (TON), vol. 13, issue 6, pp. 1325-1338, 2015.
[29]R. Molva and P. Michiardi, "Security in Ad hoc Networks," Proceedings. Pers. Wireless Commun., 2013.
[30]H. Deng, W. Li, and D. P. Agrawal, "Routing Security in Wireless Ad Hoc Networks," IEEE Commun. Mag., vol. 40, no. 10, Oct. 2016, pp. 70–75.
[31]S. Buchegger and J.Y. Le Boudec, "Performance analysis of the CONFIDANT protocol (Cooperation of nodes— Fairness in dynamic ad hoc networks)," in Proceedings. IEEE/ACM MobiHOC, 2012.