Detecting Malicious Node and Secure Data Communication in MANNET using Unique ID

S.P.Vijayaragavan, B.Karthik, M.Sriram

Abstract**:** ***Mobile Ad Hoc network (MANNET) is a basis of wireless communication with two or more devices or nodes without following centralized resources. Most of the mobiles nodes using peer level communication. MANNET allows the node to dynamically form a network and self-forming. Data transaction done using IP address and Request are analyzed and verified using IP address from routing table. Any node can be easily send request to the any node so there is a possible of attacker node can able to access the data from respective node but any how we need a new system to identify attacker node and block those nodes. Proposing new method for identify attacker nodes using unique identity number. Unique identity number are generated by using SHA I algorithm. SHA I algorithm generate number using hashing function. Each node have a unique identity and data request are verified using identity number.***

Index Terms**:** ***Mobile AD HOC network, IP address, SHA-I, hash function, identity number.***

I. INTRODUCTION

MANET remains for Mobile adhoc Network likewise named as remote adhoc organize or adhoc remote system that for the most part has a routable systems direction complaint over a Link Layer especially agreed system. They encompass of set of moveable hubs related distantly in a self-arranged, self-recuperating system without having a established framework. MANET hubs are allowable to move haphazardly as the system topology vagaries every now and again. Every hub carry on as an alteration as they forward crusade to other determined hub in the system.

MANET may work as independent design or they can be the piece of bigger web. They shape very unique self-governing topology with the nearness of one or numerous distinctive handsets between hubs. The principle challenge for the MANET is to prepare all gadgets to consistently keep up the data obligatory to appropriately course movement. MANETs encompass of a shared, self-framing, self-mending system MANET's about 2000-2015 normally impart at radio frequencies (30MHz-5GHz).

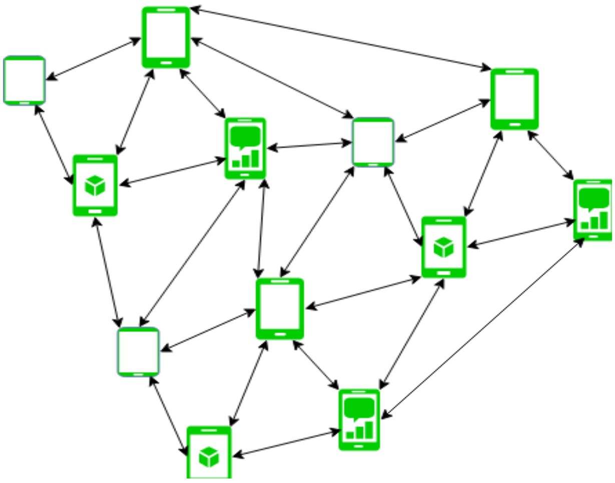

Fig 1. Manetadhoc Network

This can be utilized as a part of street security, going from sensors for condition, home, wellbeing, debacle protect tasks, air/arrive/naval force resistance, weapons, robots, and so on.

Meanwhile the system hubs are transferable, an Ad hoc system resolve commonly have a forceful topology, and which effects will disturb organize attributes. System hubs will regularly be battery powered, which confines the frontier of CPU, data transfer, and memory capability. This will necessitate organize capacities that are ability successful. Besides, the remote (radio) mediums will equally authority the behavior of the system since of variable assembly relocates speed approaching about since of usually high inaccuracy rates. These novel attractive things to see signify a little new complicatedness in the outline of remote Ad hoc organizing caucus. System capacity, for instance, navigation, address distribution, endorsement and agreement must be envisioned to acclimatize to a lively and changeable system topology. Possessions in mind the expiration goal to build up sequences among hubs, which are additional isolated than a solitary jump, extraordinarily considered direct agreements are protected in. The one of a kind constituent of this convention is their competence to pursue course although a dynamic topology. In the most straightforward situation, hubs capacity have the capability to converse particularly with respective other, for request, when they are within remote diffusion possibility of each other. Nonetheless, Adhoc organizes should similarly bolster connection among hubs that are impartial in an approximately way connected by a succession of remote jump over dissimilar hubs.

Revised Manuscript Received on 30 May 2019.
***** Correspondence Author

S.P.Vijayaragavan*, Associate Professor/EEE, Bharath Institute of Higher Education and Research, Chennai.

B.Karthik, Associate Professor/ECE, Bharath Institute of Higher Education and Research, Chennai.

M.Sriram, Associate professor, CSE, Bharath Institute of Higher Education and Research, Chennai.

For illustration, in Fig 2, to build up communication among hubs an and C the system necessity join the director of hub B to transfer bundles among them. The discs exhibit the professed possibility of each hub's radio handset. Hubs A and C are not in organize transmission capacity of every former, subsequently A's circle does not concealment C.

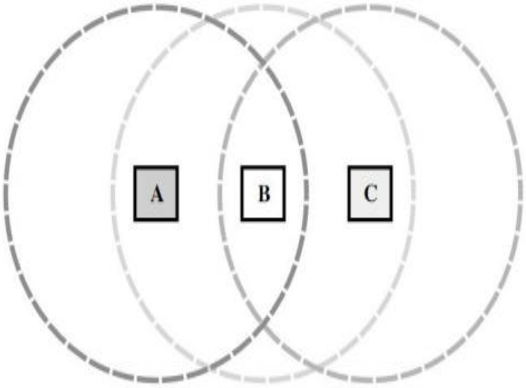

Figure 2: A Mobil Ad hoc network of three nodes, where nodes A and C must discover the route through B in order to communicate. In well-known, an Ad hoc network is a network wherein each node is doubtlessly a router and every node is doubtlessly mobile. The occurrence of wi-fi conversation and mobility construct an Ad hoc community unlike a outmoded stressed out community and necessitates that the routing protocols utilized in an Ad hoc community be based on innovative and special concepts. Routing protocols for outmoded stressed networks are intended to aid wonderful numbers of nodes, however they anticipate that the qualified role of the nodes will typically continue to be unchanged.

II. RELATED WORK

Creator announces a dwindling agreement for unconstrained remote impromptu systems which exploits a half and half symmetric/topsy-turvy plot and the conviction along with clients possession in attention the ending objective to profession the underlying info and to employment the unidentified keys that will be employed to encode the info [1]. Belief depends on the primary visual write to among clients. Our proposition is an entire self-designed protected conference that can make the system and suggest sheltered presidencies with no framework. The gadget licenses sharing property and presenting new presidencies among customers in a safe domain. The agreement includes all dimensions anticipated to paintings with no out of doors help. We have unruffled and fashioned it in gadgets with imperfect property. System formation stages are factor by way of factor and the communication, conference letters, and system supervision are illuminated. Our proposition has been symbolized with a specific stop aim to test the conference approach and execution. Ongoing advances in specially appointed and sensor remote systems have conveyed us new plans and sending introductions. Significantly extra, when the specially appointed (or sensor) remote system incorporate clients and administrations. On one pointer, the Quality of Service for every client must be ensured. Then again, the client conduct and the administrations offered for the clients could influence to the system execution. An unconstrained specially appointed (or sensor) arrange empowers a gathering of clients to convey and cooperate cooperatively near each other, sharing administrations, amid a timeframe [2]. They try to copy human connections with a specific end goal to cooperate in gatherings, running on a current innovation. Gadgets utilized for unconstrained specially appointed (or sensor) remote systems have constrained assets, few processing limit and low vitality utilization. Client situated and benefit arranged unconstrained specially appointed and sensor remote systems can be utilized to tackle an issue, to do a particular errand, or just to segment administrations and assets among clients, with no reliance on a focal server. There is an extensive variety of situations in which these systems can be connected. This extraordinary concern tries to gather the latest investigation of these kinds of systems Creators are propose a safe unconstrained impromptu system [3], in light of direct shared connection, to concede a speedy, simple, and protected entree to the clients to browse into the Web. The articles demonstrate the depiction of our proposition, the technique of the hubs associated with the framework, the sanctuary calculations actualized, and the outlined posts. We have considered the sanctuary and its execution. Albeit a few people have characterized and portrayed the principle highlights of unconstrained specially appointed systems, no one has distributed any outline and recreation until today. Unconstrained systems administration will empower a more characteristic type of remote registering when individuals physically meet in reality. We additionally approve the accomplishment of our proposition through a few recreations and correlations with a normal design, considering the improvement of the assets of the gadgets. At long last, we contrast our proposition and other storing systems distributed in the related writing. The proposition has been created with the principle goal of enhancing the correspondence and combination between various investigation focuses of low-asset networks. That is, it lets impart unconstrained systems, which are occupied cooperatively and which have been made on various corporeal spots. Remote sensor systems have numerous applications, differ in estimate, and are sent in extensive assortment of regions. They are regularly sent in possibly unfriendly or un fluctuating antagonistic condition so that there are worries on sanctuary concerns in these systems. Sensor hubs used to shape these systems are asset compelled, which make sanctuary submissions a testing issue. Productive key dispersion and administration instruments are required other than insubstantial figures [4]. Numerous key foundation procedures have been intended to address the tradeoff among constrained memory and security, however which plot is the best is as yet begging to be proven wrong. In this articles, we give a review of key administration conspires in remote sensor systems. We see that no key circulation system is perfect to every one of the situations where sensor systems are utilized; thusly the strategies utilized must rely on the necessities of target submissions and assets of every discrete sensor organize.

Remote sensor systems (WSNs) have pulled in a great deal of specialists because of their utilization in basic applications. WSN have restrictions on computational limit, battery and so forth which gives extension to testing issues. Uses of WSN are radically developing from indoor arrangement to basic open air sending. WSN are dispersed and sent in a condition, since this WSN are helpless against numerous sanctuary dangers. The conclusions are not entirely trustable since of their organization in separate and unrestrained conditions. In these present articles, we in a general sense concentrated on the sanctuary concern of WSNs and projected a convention in view of open key cryptography [5] for outside specialist validation and assembly key foundation. The planned convention is effective and protected in contrasted with other open key based conventions in WSNs.

Most impromptu systems don't accomplish any system get to regulator, sendoff these systems helpless along side benefit utilization assault where a noxious hub pervades bundles into the system with the impartial of fatiguing the properties of the hubs handing-off the parcels. To upset or prevent such beatings, it is significant to exploit verification mechanism that assurance that exclusive permitted hubs can permeate crusade into the system. In this paper, creator exhibit LHAP, an adaptable and light-weight confirmation convention for impromptu systems [6]. LHAP depends on two procedures: (I) bounce by-jump validation for checking the legitimacy of the considerable number of parcels transmit in the system and (ii) one-way key chain and TESLA for bundle confirmation and for lessening the upstairs to establish belief between hubs. We break down the sanctuary properties of LHAP. Besides, our execution investigation demonstrates that LHAP is an exceptionally lightweight security convention.

Remote work systems guarantee to broaden fast remote availability past what is conceivable with the present WiFi-based foundation. Be that as it may, their special engineering highlights abandon them especially powerless against security dangers. In this article writers depict different types of advanced assaults propelled from foes with interior access to the WMN [7]. At last distinguish conceivable identification and relief components.

Advancement of handheld highlights and portable communication makes Ad hoc arranges broadly embraced, yet security remains a muddled issue. As of late, there are a few proposed arrangements treating confirmation, accessibility, secure directing and interruption location and so on, in Ad hoc organizes. In this paper creator present a securing information convention in Ad hoc arranges, SDMP convention [8]. This arrangement builds the vigor of transmitted information privacy by misusing the presence of numerous ways between hubs in an Ad hoc organize. This paper additionally incorporates an outline of current arrangements and vulnerabilities and assaults in Ad hoc organizes.

The significant capacity of sensor systems is to assemble the information from different sensor hubs which are utilized to transmit the information at various base stations. Because of blame or nearness of malignant hub in the system, gathered information may not be right or commandeered. It is imperative and hard to distinguish the dangerous work done by any malignant hub. There are numerous elements included, for example, bundle conveyance proportion, sticking sign, treating, which help to shield against malevolent hub or to identify the noxious hub. In this paper, noxious hub location in light of bundle conveyance proportion (PDR) has been proposed [9]. The bundles in organize must achieve the goal possession in mind the conclusion goal to give the unwavering quality in arrange, yet the noxious hubs may alter a portion of the parcels and influence the correspondence to come up short. Add up to number of bundles sent by the sender could possibly be gotten by the collector and it relies upon whether there is any malignant hub introduce or not in the system. So one can utilize this conveyed bundle data and compute the parcel conveyance proportion to discover the malignant hub. Reenactment in this paper demonstrates that the proposed conspire finds the vindictive hubs in the system in productive and successful way. In this article, Author suggests a cross layer way to deal with recognize the pernicious hub in MANET [10]. Creator build up a cross layer information checking calculation possession in observance the end goal to correspond the MAC- [Medium Access Control] layer parameters with arrange layer parameters for adequately recognizing malignant hubs from the system. For isolating the malignant hubs, our tactic uses both the single and cross layer parameters. Data about distinguished vindictive hub ids from the system is communicated to alternate hubs in the system. The directing convention which is utilized as a part of the reenactment is AODV (Ad Hoc On-Demand Distance Vector). The execution of our strategy is demonstrated by the recreation of our framework show utilizing the system test system NS-2. Trial investigation uncovers that our planned tactic shields the Black gap assault with healthier execution regarding bundle misfortune proportion, parcel conveyance proportion and Normalized Routing Load.

III. ISSUES IN EXISTING SYSTEM

The remote communication is exceptionally well recognized these days; applying remote can improve rooms look, on the grounds that less links are utilize. The inadequacy of remote connection involve impromptu. Lower information rate, sanctuary, and medium access control are normal problem in the remote transactions. Especially appointee’s behavior source additionally a few concern. The supplementary are the burdens of especially selected organizations. One of most concerning issue of specifically selected systems is diminished info charges. The regular for wave, which is exploited for remote communication, counteracts remote communication to transmit information superior to wired communication. A higher reappearance can communicate more information, yet then it is more helpless against impedance and performs well in short range. Not at all like wired transmission, may the inaccessible transmission manage concern the regular for the electronic wave. In a free room without obstruction the electronic wave proliferates direct autonomously from its reappearance.

There is only occasionally such a circumstance. The hindrance sources investigation, indication, dissipating, blurring, diversion, diffraction of the wave. These multiply may prompt transmit tracts being perplexed and in this technique got in inaccuracy.

Since the topology of the system is continually showing signs and symptoms of trade, the difficulty of directing parcels between any healthy of hubs becomes a testing task. Multicast steerage is another test in mild of the reality that the multicast tree isn't any greater static since of the uneven growth of hubs intimate the system. Sequences among hubs potency also possibly comprise unique bounces, that's greater mind boggling than the single bounce correspondence.

Notwithstanding the primary vulnerabilities of far off affiliation, a particularly appointed gadget has its scrupulous safety issue due to e.g. Dreadful neighbor handing-off wads. The aspect of conveyed challenge requires various strategies of corroboration and key administration. Additional, far off connection potentials present likewise trustworthiness concern, since of the restrained faraway transmission run, the talk impression of the far off medium (e.g. Shrouded terminal difficulty), movability brought on package deal misfortunes, and information transmission mistakes.

In old system focus only fast data connection so we concentrate node security.

MANNET are self configuring their structure because nodes can move their location and each node must update their location.

Data loss may be occurred due to weak signal strength.

Data transaction done using request and response of the nodes.

Traffic management not done properly so this system cannot manage many request at a time then time delay may be occurred.

IV. PROPOSED METHOD

A. problem identification and solution

We introduce new method for our ad hoc network using unique identity. Implemented SHA I algorithm for generating unique id and SHA I algorithm create id simply by means of the hashing functions. In this system each node having unique id. Receiver node send data request to sender node then sender node analyze receiver unique identity number from routing information. If receiver node have valid id number means sender node send data otherwise block the receiver node and finally terminate that node their network. This system enable secure data transaction among the nodes. Data traffic can be reduced by using latest AAODV protocol. AAODV protocol select the best path using the some parameters are following as

Hop count

Signal strength

Battery level

Using this proposed system secure data transmission with high throughput and low error late

B. System architecture

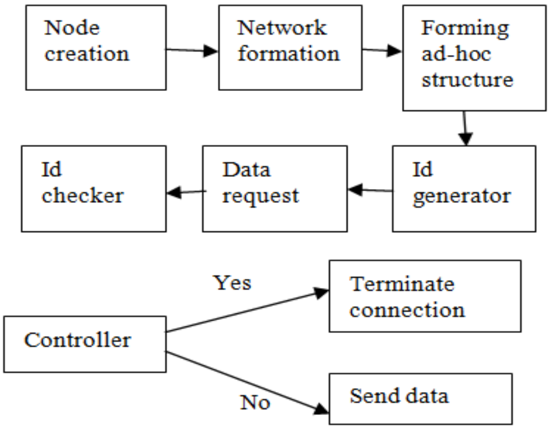

Fig 3: System Architecture

The system consists of subsequent modules:

1. Node creation
2. Network formation
3. TCP/IP connection

1. Node creation

Create n number of nodes using X,Y,Z position. Here we used NS2 simulator so Z position always 0. Configured AAODV protocol with all nodes.

2. Network formation

A remote specially appointed system is a decentralized far off device. The system is specifically appointed for the reason that it would not depend upon a previous framework, for instance, switches in stressed systems or access focuses in treated The decentralized concept of remote impromptu systems makes them appropriate for an assortment of uses where focal hubs cannot be relied on, and may decorate the versatility of remote impromptu systems contrasted with far flung oversaw systems. Every hub refreshes their live area intermittently and in light of that shape a system.

3. TCP/IP connection

The Transmission Control Protocol (TCP) is one of the middle agreements of the Internet convention suite (IP), and is frequent to the point that the complete collection is often called TCP/IP.TCP give strong, asked and mistake checkered transference of a flood of octets among applications walking on PCs connected with a neighborhood, intranet or people in preferred Internet. It live at the automobile layer.

TCP is known as an association organized convention, which implies that an association is set up and kept up till the factor when such time as the message or messages to be traded by the application programs at each end have been traded.

4. id generator

Pseudo random hash function is used to generate id for each nodes in a network. SHA I algorithm easily generate the unique identity.

5. controller

After forming a network structure and any node can send data request to any node in a network. Each node have controller and controller analyze received id number if id is correct means allow for further comm unication otherwise terminate that node from the network.

C. Work flow diagram

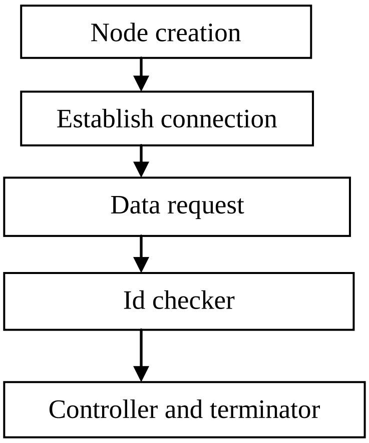

Fig 4: Workflow Diagram

D. SHA I *Algorithm implementation*

```
static string Hash(string input)
{
using (SHA1Managed sha1 = new SHA1Managed())
   {
Var hash =
sha1.ComputeHash(Encoding.UTF8.GetBytes(input));
varsb = new StringBuilder(hash.Length * 2);
foreach (byte b in hash)
        {
            // can be "x2" if you want lowercase
sb.Append(b.ToString("X2"));
        }
returnsb.ToString();
   }
}
```

SHA-1 generate a 160-bit hash fee or message digests from the recorded information (facts that calls for encryption), which resemble the hash fee of the MD5 algorithm. It uses 80 sequences of cryptographic processes to encode and at ease a records item. Some of the protocols that use SHA-1 comprise:
Transport Layer Security (TLS)
Secure Sockets Layer (SSL)
Pretty Good Privacy (PGP)
Secure Shell (SSH)
Secure/Multipurpose Internet Mail Extensions (S/MIME)
Internet Protocol Security (IPSec)

SHA-1 is regularly utilized in cryptographic packages and environment wherein the want for data reliability is extraordinary. It is also used to catalogue hash capabilities and perceive information dishonesty and checksum mistakes.

F. SHA I pseudocode

```
add certain additional data to the end of the input
set the preliminary sha-1 values
for each 64-byte chunk do
extend the chunk to 320 bytes of data
perform first set of operations on chunk[i] (x20)
perform second set of operations on chunk[i] (x20)
perform third set of operations on chunk[i] (x20)
perform fourth set of operations on chunk[i] (x20)
end
return sha-1 values as a hash
```

E. Results and Discussion

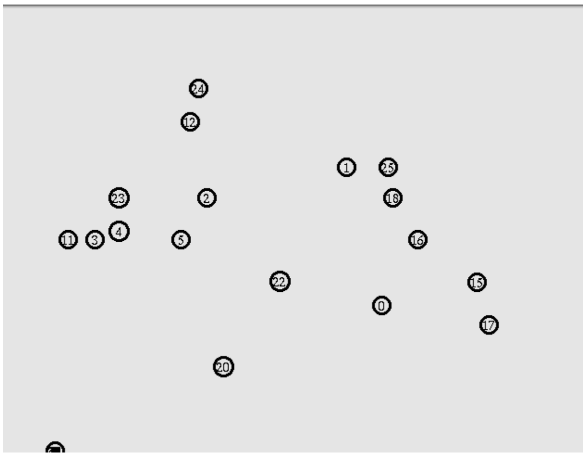

Figure 5. Initial Stage

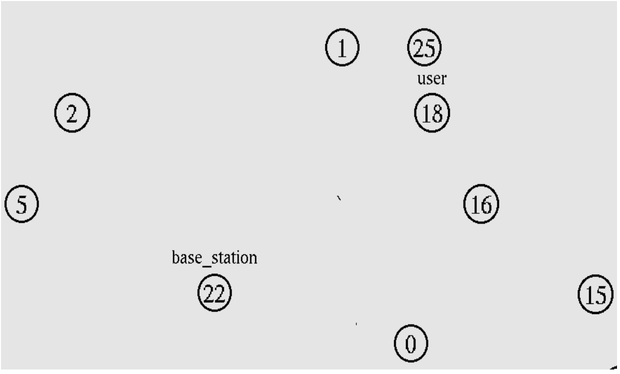

Figure 6. Single comm. With identification

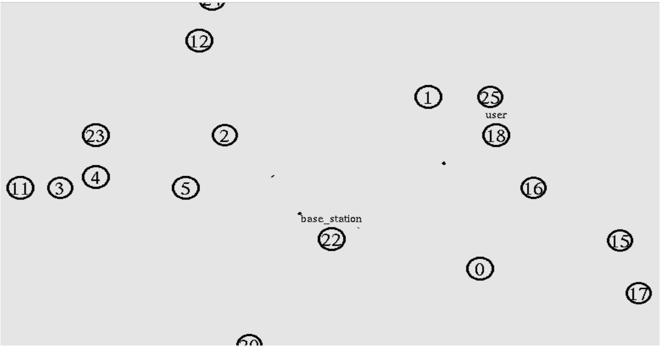

Figure 7. Multi Comm

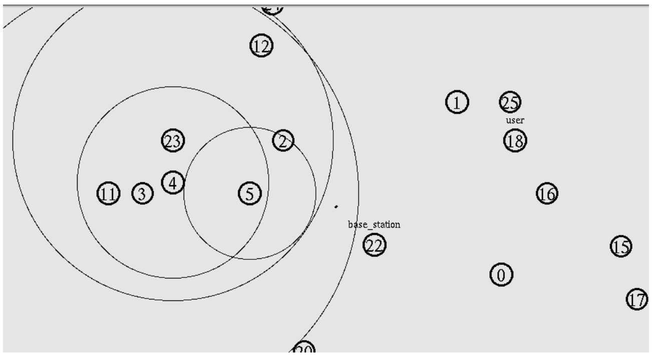

Figure 8. Coverage area

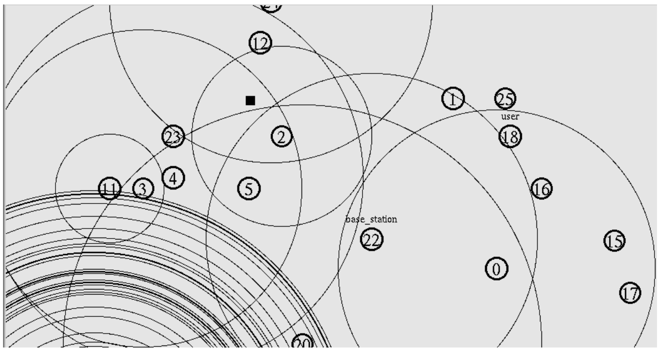

Figure 9. Packet drop

Figure 5 to 9 shows the step by step execution process and the obtained results.

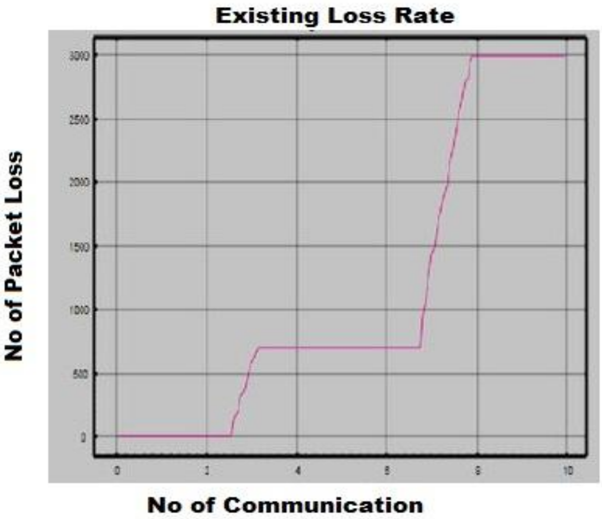

Fig 10: existing loss rate

In figure 10 shows the packet loss due to the bad communication and attacker node. During the data transmission attackers act as a receiver node so sender node send all packets to the attacker's node but original receiver partial packets only. Due to this problem loss rate to be very high in the existing system.

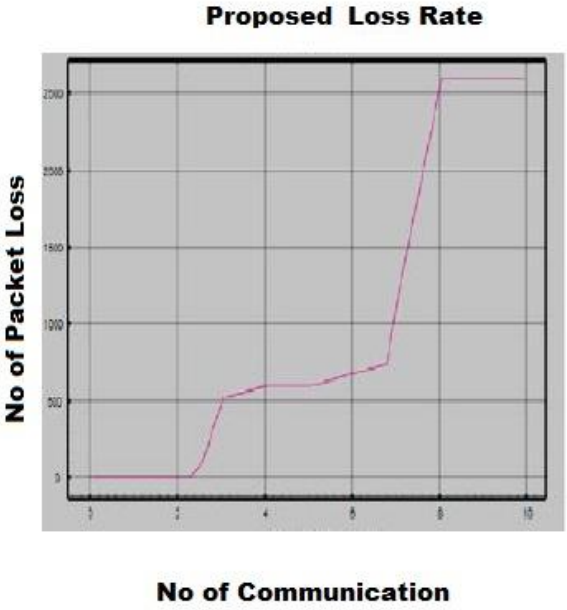

Fig 11: Proposed loss rate

In fig11 shows proposed loss rate and loss rate are minimized when compare to the existing loss rate. In proposed work each should be verified by unique id number. So attackers cannot hack the packets during the transmission.

V. CONCLUSION

In our proposed system implemented SHA I algorithm and AAODV algorithm. Each node verified by using unique id number and block nodes whose doesn't have a correct unique id number. Every user would like to send data and receives data within short time but unfortunately its not done in a existing system but proposed system provides very fast communication using AAODV Protocol. Time consumption is the achieved in this paper. If the any node is dead means sender node again send the data. Data loss is very low when compared to all existing systems.

VI. FUTURE SCOPE

In future going to implement end to end encryption techniques and attackers cannot access the data so we can achieve very high throughput.

REFERENCES

1. Raquel Lacuesta,JaimeLloret,Miguel Garcia, Lourdes Penalver,"A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation, IEEE Transactions on Parallel and Distributed Systems Vol.24,No.4, April 2013.
2. J. Lloret, L. Shu, R. Lacuesta, and M. Chen, "User-Oriented and Service-Oriented Spontaneous Ad Hoc and Sensor Wireless Networks," Ad Hoc and Sensor Wireless Networks, vol. 14, nos. 1/2, pp. 1-8, 2012.
3. R. Lacuesta, J. Lloret, M. Garcia, and L. Pen˜ alver, "A Spontaneous Ad-Hoc Network to Share WWW Access," EURASIP J. Wireless Comm. and Networking, vol. 2010, article 18, 2010.
4. Y. Xiao, V.K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A Survey of Key Management Schemes in Wireless Sensor Networks," Computer Comm., vol. 30, nos. 11/12, pp. 2314-2341, Sept. 2007.
5. Vorugunti Chandra Sekhar , MrudulaSarvabhatla, "Security in Wireless sensor networks with public key techniques," IEEE transaction on Computer Communication and Informatics (ICCCI), 2012.
6. S. Zhu, S. Xu, S. Setia, and S. Jajodia, "LHAP: A Lightweight Hop-by-Hop Authentication Protocol For Ad-Hoc Networks," Ad Hoc Networks J., vol. 4, no. 5, pp. 567-585, Sept. 2006.
7. LoukasLazos, and Marwan Krunz, "Selective Jamming/Dropping Insider Attacks in Wireless Mesh Networks" An International Journal on Engineering Science and Technology Arizona edu, Vol.2, No. 2, pp 265-269, April2010.
8. R.Vidhya, G. P. Ramesh Kumar, "Securing Data in Ad hoc Networks using Multipath routing", International Journal of Advances in Engineering & Technology, Vol.1, No. 5, pp 337-341, November 2011.
9. Sanjay Tyagi , Girdhar Gopal , VikasGarg, "Detecting malicious node in network using packet delivery ratio," Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on IEEE, 2016.
10. Jai Kumar Vinayagam , C. H. Balaswamy , K. Soundararajan, "Adopting cross layer approach for detecting and segregating malicious nodes in MANET." Signal Processing and Communication (ICSPC), 2017 International Conference on IEEE.
11. NIST std. FIPS 180-2, Secure Hash Standard (SHS), National Institute of Standard and Technology (NIST), Oct. 2001.
12. TTA std. TTAK.KO-12.0011/R1, Hash Function Standard - Part 2: Hash Function Algorithm Standard (HAS-160), Telecommunications Technology Association (TTA), Dec., 2000.
13. K. Saravanan, A. Senthilkumar, and P. Chacko, "Modified whirlpool hash based bloom filter for networking and security applications", Devices, Circuits and Systems (ICDCS), IEEE, pp. 1-6, Mar. 2014.

14. D.H. Kim, S.W. Yoon and Y.P Lee, "Security for IoT Service," Journal of The Korean Institute of Communication Sciences, vol. 30, no.8, pp.53-59, July, 2013.
15. J.U. Kim and S.H. Jin, "Internet (IoT) Security Technology for Security Threats in Hyper-Connection Environment," Journal of The Korean Institute of Communication Sciences, vol. 34, no.3, pp.57-64, Feb., 2017.
16. J. He, H. Chen, and H. Huang, "A compatible SHA series design based on FPGA", Electrical Engineering/Electronics Computer Telecommunications and Information Technology (ECTI-CON), IEEE, pp. 380- 384, May 2010.
17. MD. Rote, V. N, and D. Selvakumar, "High performance SHA-2 core using the Round Pipelined Technique View Documen", Electronics, Computing and Communication Technologies (CONECCT), IEEE, pp. 1-6, July 2015.

AUTHORS PROFILE

S.P.Vijayaragavan is an Associate professor in the department of Electrical and Electronics Engineering, Bharath Institute of Higher Education and Research, Chennai, India. He received his PhD(ECE) -Networks in August 2017from Bharath Institute of Higher Education and Research, Chennai, India. He received his Master of Engineering in Applied Electronics in 2011. He is a member of IEEE and IAENG. His area of interests includes Communication, Network Security System Techniques, and Renewable resources.

B.Karthik is an Associate professor in the department of Electronics and Communication Engineering, Bharath Institute of Higher Education and Research, Chennai, India. He received his PhD(ECE) - Image Processing in May 2017. He received his Master of Engineering in Applied Electronics in 2011.He received his Bachelor of Technology in Electronics and Communication Engineering in 2007. He is continuing his research in Image Processing at Bharath Institute of Higher Education and Research, Chennai, India. He is a member of IEEE and IAENG. He is an editorial board member in IJBSE, AJAST, and IJETECE.His area of interests includes Image Processing, Network Security System Techniques.

M.Sriram is an Associate professor in the department of Computer Science Engineering, Bharath Institute of Higher Education and Research, Chennai, India. He received his PhD(IT) in Dec 2018. His area of interests includes Ontology, Data Mining, Network Security System Techniques.