ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

Detection and Removal of Spoofed Data Using VANET

Amudhavalli.D[1], Logeshwari.P[2], Tina Susan Thomas[3]

Department of Information Technology, KCG College of Technology, Chennai, India[1,2].

Department of Information Technology, KCG College of Technology, Chennai, India [3]

ABSTRACT: The project deals with sending secure data information from one node to another through a concept of VANET.In existing system, a VADD protocol and TLO algorithm is used for delay data packet transmission between nodes using NS2 simulation.In this system each node is assumed as a vehicle with having GPS and sending data packets in a secure way using "continuous wavelet transform method".By this method the intruder is detected and removed in NS2 simulation.

KEYWORDS: intruder, continuous wavelet transform, security**.**

I. INTRODUCTION

A VANET (vehicular ad-hoc network) is a technology of sending information among the moving vehicles through connection-less network using Wi-Fi. The source and destination node is identified by calculating the distance between the nodes and which is updated within the routing table. The distance which is far enough from the source node within a cluster is considered to be as a destination node. In VANET there are three main types as inter-vehicular communications, vehicle-to-roadside communications and inter-roadside communications. This project deals with the VANET technology of sending secure information from source to destination vehicle.It was shown that vehicle-to-vehicle and vehicle-to-roadside communications architectures will co-exist in VANETs to provide road safety, navigation, and

other roadside services. VANET relies on intelligent transportation systems (ITS) framework.
In this ITSeach vehicle takes role of sender, receiver, and router. It broadcasts the information among vehicular network for safer network thereby avoiding traffic.For communication to occur between vehicles and Road Side Units (RSUs), vehicles must be equipped with some sort of radio interface or On Board Unit (OBU) that enables short-range wireless ad hoc networks to be formed.

II. CHALLENGES

Real time Constraint: The time constraint is critical in case of VANET while sending the data packets. The transmission must be made with 100ms transmission delay. Thus real time constraint is a challenge for the VANET.

Data Consistency Liability: In VANET sometimes the authenticated person may send unwanted data and cause accidents or traffic. This leads to inconsistency of a network. Hence a mechanism must be used to avoid this. Getting the data from various nodes avoids this inconsistency.

Low tolerance for error: Some protocols are designed on the basis of probability. If any error occurs in the network then it leads to low tolerance in VANET. This is one of the challenges to be noticed.

Key Distribution: All the security mechanisms depend upon the key in VANET. Each data that is sent is encrypted and must be decrypted at the receiver end with using same or different key. Also different manufacturer can install keys

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

in different ways and in public key infrastructure trust on Certificate Authority(CA)become major issue. Therefore distribution of keys among vehicles is a major challenge in designing a security protocols.

Incentives: Manufactures are interested to build applications that consumer likes most. Some of the consumers would agree with a vehicle which reports about the emergency or traffic violation. Hence successful deployment of vehicular networks will require incentives for vehicle manufacturers, consumers and the government is a challenge to implement security in VANET**.**

III. SECURITY REQUIREMENTS

Authentication: Authentication is the process of identifying or verifying the legitimate user. In VANET, the information which comes from the other vehiclemust be authenticated.

Availability: Availability requires that the information must be available to the legitimate users. Denial of service (DOS) attacks can bring down the network and hence information cannot be shared.

Privacy: The privacy of the node should be guaranteed against the authority.

Data Verification: A regular verification of data is required to eliminate the false messaging.

IV. EXISTING SYSTEM

The TLO (The Last One) algorithm provides proper data dissemination in an ad hoc network and effective solution to reduce end to end delay. In this algorithm it is assumed that every node in the network is completely equipped with GPS, i.e. each vehicle knows the exact geographical location of the other vehicles which are in the communication range. Frequent updating of information takes place at closer intervals. Whenever an accident takes place, the accident vehicle broadcasts an alert message to allthe other vehicles within its communication range. So all the vehicles within the communication range of the accident vehicle receives the alert message, after receiving the message it does not rebroadcast it immediately. It waits for some time and performs TLO algorithm and it selectsthe last vehicle within that particular communication range.VADD (Vehicle Assisted Data Delivery Technique with carry forward technique) follows Carry forward technique.In carry forward technique, a node will be generated which will contain forward path for destination node.

V. PROPOSED SYSTEM

In VANET, the data packets are transmitted to the nearby vehicles in case of any accidents or traffic management. While transmitting data, unsecure data dissemination, data packet delay and packet loss happens instantly. Between source and destination node there might be an intruder who gets the data from source and changes the data and acts as like a source node and forwards it to the destination node. A “continuous wavelet transform methodology” is used for the security purpose for identification and removal of intruder between end to end nodes. This method calculates the points of every node. Nodes receiving message is indicated with points. The point increases as and when the nodes receive messages. If intruder is present, it concentrates on same link connectivity which is then indicated with less point. Nodes having fewer points are detected and removed using this methodology**.**The data that is sent from one node to another node will be in a form of text. Some of data information such as traffic identification, accident identification details is sent to other intermediate nodes in the form of text. For example, n1, n2, n3, n4 be the nodes respectively. The node n1 is considered to be as a source node and n4 as a destination node. The nodes n2, n3 are considered to be as intermediate nodes. The node n1 detects the incident in front of them and sends prior information to the intermediate nodes. The information can be “The road is traffic, please take diversion”, “accident has taken place” etc. the pattern would be as node n1 senses and gets the information and sends to the node n2. Then the node n2 sends that data information to the node n3. Then n3 sends to the destination node n4. The source and destination node is decided as and when a cluster is formed. The highest distance from the source node is calculated and stored in a routing table

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

which is considered to be as a destination node. The "continuous wavelet transform methodology" which is applied in this system, is calculated by points in the form of integer type numbering from 1 to n. The points are added to each and every node as and when then data packets reaches them. Initially a node will have point 0, and then it increases by 1 point when message reaches them. The node having fewer points is detected and removed off. Intruder is a hacker who interrupts the link between the nodes and tries to tamper the data packets. It concentrates on the same link connectivity. Thus it will receive fewer points. Nodes having fewer points are detected and removed. The spoofed data and normal secured data are differentiated by using this methodology. The node having high pointsis considered as a normal secured data. Alternatively nodes having fewer points are considered to be as a spoofed data. From the **figure 5,** the source node sends the data to the nearby nodes (intermediate nodes). If intruder is present between the links, it concentrates on the same link connectivity. The "continuous wavelet transform methodology" is applied. So attacker will be receiving less incoming data.Thus Points decreases for attacker node.Nodes having fewer points are detected and removed.Secure information is transmitted now. If the intruder is not present between the links, then secure information is sent. Message is received securely without modifications. The spoofed data and normal secured data are differentiated by using this methodology. When nodes having high points it is considered to be as normal secured data. Alternatively nodes having fewer points are considered to be as a spoofed data.

V. SIMULATION

Transmission phase module:

Initially the wireless nodes are created and a shortest path is figured out. From **figure 1,**the source node to the destination node within a cluster. The source node transmits the data packets to the destination node. During transmission from source node, many intermediate nodes collect those information packets and sends to destination node within the cluster range. In this system, transmission phase module helps to ensure that proper transmission of data packets is made or not without any packet loss or delay in sending data packet.

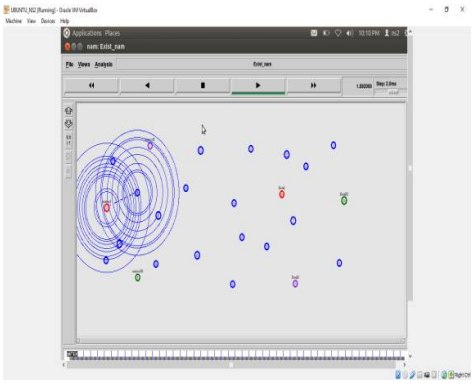

Fig 1: Data transmission between the nodes.

Detection phase module:

Detecting malicious data injections during transmission.In the **figure 2**, a wavelet transform methodology is used which counts the points for every node.Since attacker concentrate on single link connectivity it gets less points. Nodes getting very few points are detected.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

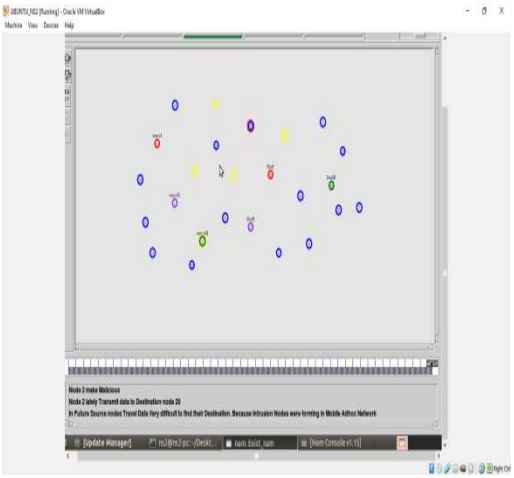

Fig 2: Detection for the malicious node.

Removal phase module:

In the **figure 3,** removal of the spoofed data after detection phase and the intruder having malicious data for secure transmission is made.

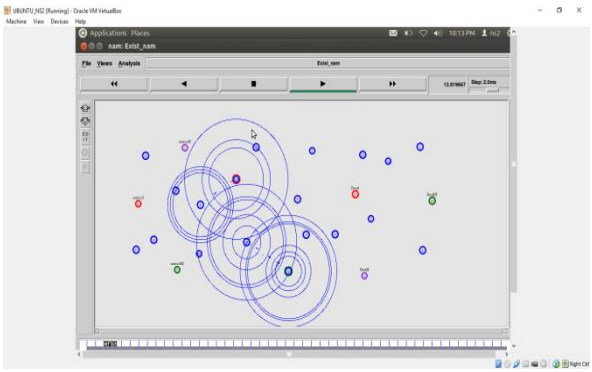

Fig 3: Removal of intruder injecting malicious node.

VI. RESULTS AND CONCLUSION

From the **figure 4,** it is seen that, the complete system is executed in network simulator 2 tools.The intruder injecting malicious data is detected and removed off between the nodes.A secure way of communication is made between the vehicles.Unnecessary traffic collisions are avoided between the nodes.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

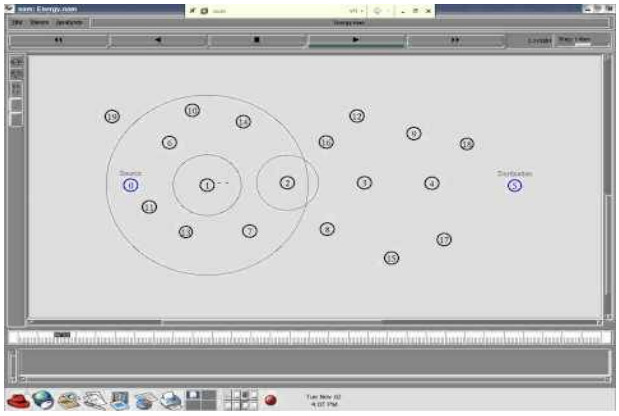

Fig 4: Outcome Result.

APPLICATIONS

1. To monitor traffic in a road, where prior information is sent among vehicles.
2. To track the accidents(Emergency) in a road.

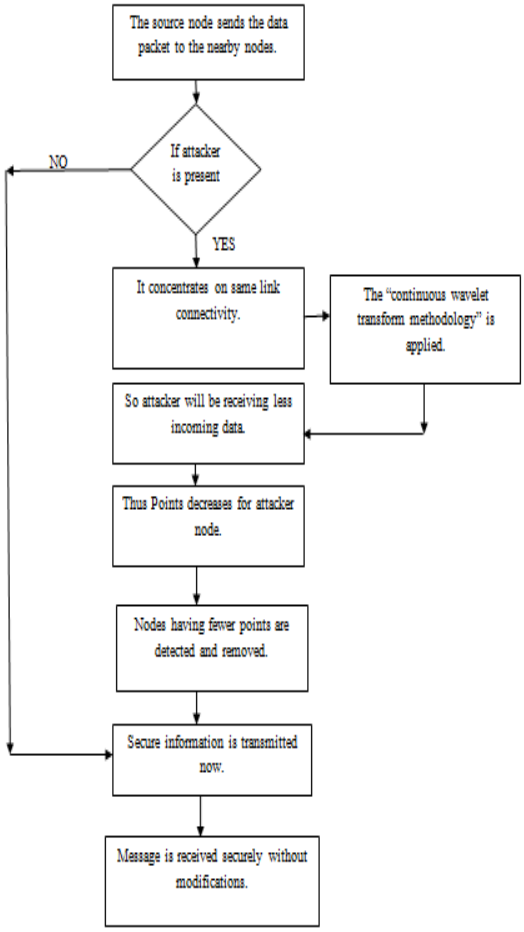

Fig 5: Flowchart of proposed system.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

VII. FUTURE SCOPE

For the future the drunken driven node must be detected and the information needs to be sent to the nearby vehicles within certain range.

REFERENCES

[1] Er.GaganpreetKaur,(2016)," Technique to control Data Dissemination and to support data accessibility in Meagerly connected vehicles in VANET", International journal of advanced research in computer science.
[2] Ali Rakhshan, HosseinPishro-Nik,(2015)," Improving Safety on Highways by Customizing Vehicular Ad Hoc Networks" ,IEEE.
[3] Hamid Reza Arkian,RezaEbrahimiAtani,(2015)," A Stable Clustering Scheme Based on Adaptive Multiple Metric in Vehicular Ad-hoc Networks", Journal Of Information Science And Engineering.
[4] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan "A comprehensive survey on vehicular ad hoc network," Journal of Network and Computer Applications, Vol. 37, 2014, pp. 380-392
[5] Yang Yang, Qian Liu1, Zhipeng Gao1, Xuesong Qiu1, Lanlan Rui1 and Xin Li, "A data dissemination mechanism for motorway environment in VANETs", Springer, 2015.