International Journal of Research in Engineering, Science and Management
Volume-1, Issue-10, October-2018
www.ijresm.com | ISSN (Online): 2581-5792

Efficient Qos and Secure Routing in VANET Using Group Based Routing Management Protocol

A. Mohamed Suhair[1], P. N. Sundara Rajan[2]
[1]*PG Scholar, Department of Electronics and Communication, PSNACET, Dindingul, India*
[2]*Associate Professor, Department of Electronics and Communication, PSNACET, Dindingul, India*

***Abstract*—Vehicular ad-hoc networks (VANETs) are a specific kind of Mobile ad-hoc network (MANETs) in which each vehicle acts as a nodes. The role of VANETs is to provide security and message authentication between nodes. Message authentication scheme verifies multiple messages at same time. Message authentication in such networking protocol and location-aware services require that each mobile nodes must learn about the position of neighbour nodes. However this process can be disrupted by adversarial nodes. Existing schemes doesn't have efficient transmission capabilities and it never resist impersonation and provides way for malicious nodes to drag the packets. Group based routing management protocol and Trust management scheme can be proposed in order to identify the trusted nodes based on the trusted value by using the sponsor nodes. Role of Group based routing management protocol and Trust management scheme is to testing every nodes for several times in order to improve message authentication. Merits of this scheme is to reduce false rejection ratio and malicious nodes in the network and also it satisfies security and privacy requirements.**

***Index Terms*—VANETs, Group based routing management protocol and Trust management scheme, privacy preserving**

I. Introduction

A. Wireless Sensor Network

Wireless sensor network is a distributed autonomous sensor network to supervise physical and environmental conditions and it can be able to transfer data through the network to the proxy location. Wireless sensor network is a collection of nodes, each node is connected with sensor. Each sensor network node composed of radio transceiver with an internal or external antenna, microcontroller, electronic circuit for sensor interfacing and energy source.

Characteristics of Wireless Sensor Network

1. Ability to overcome node failures
2. Cross layer design
3. Scalability
4. Energy harvesting.

B. Vehicular ADHOC Network

Vehicular ad-hoc network (VANET) created by the principle of MANETs, creation of wireless networks for data exchange between vehicle to vehicle communication. Roadside unit traffic monitors, advanced navigation system, low cost wireless networks provide efficient data transmission. Wireless access in vehicular environment (WAVE) proposed by Intelligent Transportation System (ITS) in order to enable vehicle to vehicle, vehicle to infrastructure, and wireless communication. VANET consist of number of vehicles communicating each other controlled by roadside units (RSU). VANETs is differ from MANETs that vehicles have a fixed path to reach destination. Each vehicles composed of On board unit (OBU), it is a wireless communication device used for data storage and dedicated short range communication (DSRC), it is a wireless communication technology to allow the automobile in the intelligent transportation system (ITS) to communicate with each other.

Every wireless network can face impersonation, attacker in the middle for data robbery and it may leads to traffic chaos, accidents, security and privacy problems. Key management scheme and ID based authentication scheme can be used to provide security and preserving privacy, it may improve the performances. VANETs can ensure security and message authentication through verification of multiple messages at same time in order to reduce the computational overhead.

C. Routing in VANETS

Ad-hoc network is the advanced technique of a dynamic routing protocol that can help to transfer the information from one node to another node. The protocols that designed for MANET have been tested on VANET. The question remains how to reduce delay during transformation of information from one node to another. Implementation of real time applications for VANET can help in overcoming these hurdles. The task in VANET routing is detecting and maintaining the path of the communication. Routing in VANET can be classified in to five categories, they are

1. Ad-hoc protocol
2. Cluster based protocol
3. Geo cast protocol
4. Broadcast protocol
5. Location based routing protocol

Nodes in the network can undergo geographic routing that indicates that every nodes must know the location of the neighboring nodes. Source node can detect the geographically neighboring node to destination in order to enable efficient transmission.

In this paper Group based routing management protocol was proposed, it calculates the trust values of the nodes in the network. Source node requires the acknowledgement from the neighboring node about the packet reception that indicates the node has the trusted value. The neighboring node can transfer the packet to the destination node with minimum energy dissipation. This scheme checks the nodes trust value every time using Trust management scheme. The calculation of trust value detects the malicious nodes in the network and can be able to find the shortest path for packet transmission. Using these scheme message can be authenticated by trust values of the nodes and it provides security & preserving privacy compared to the existing schemes.

II. Security Requirements

A. Message Authentication

Message can be protected from the malicious nodes in order to provide efficient communication in the network. It can be used to improve the performance of the system.

B. Entity Authentication

The receiver must send an acknowledgement about the reception of information from the sender it ensures the trusted network for communication.

C. Access Control

Protocol can be proposed and monitoring the establishment towards the authorization given by the protocol. The role of such protocol is to identify the malicious nodes.

D. Message Confidentiality

Message or information can be protected from the unauthorized node using trust values on the existing nodes in the network.

E. Privacy Preservation

Vehicular communication system cannot disclose private information of their nodes, also it never disclose the future work of the other nodes.

F. Liability

Vehicles can be liable for communication even in the presence of the malicious nodes and to find the shortest path to transfer the information towards the destination node.

III. Proposed System

A. Group Based Trust Management Protocol

Group based trust management scheme is capable of calculating trust value based on direct and indirect interactions. Direct observations means the number of successful and unsuccessful interactions and indirect observations means the need for trusted interaction. For example Source node receives an acknowledgement that the packet is successfully received by the neighbor node and that node can forwarded the packet toward the destination node.

This scheme works on both topologies:

1. Intra group topology
2. Inter group topology

For intra group network, distributed trust management is used, each sensor is a member of the group that calculates the trust values for all group members. Based on the trust values, a node represented by anyone of the three possible states they are trusted, untrusted and uncertain. After this, each node forwards the trust state of all the group member nodes to the Cluster Head.

For intergroup technique, concentrated trust administration approach is used, inverted activity performed unaltered. In view of the trust expresses, a Cluster Head identifies the pernicious nodes and transfer a data to the Base Station. As indicated by this data, each Cluster Head sends trust estimations of other Cluster Heads to the Base Station. When this data achieves the Base Station, it doles out one of the three conceivable states to the entire technique. After this, the Base Station will forward the current condition of a particular technique to Cluster Heads.

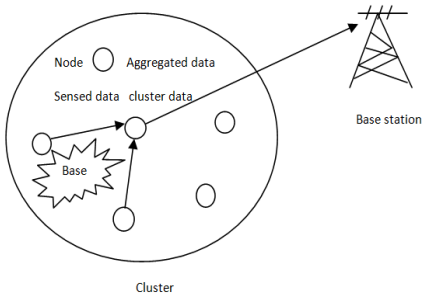

Fig. 1. Intra group to base station

B. Representation of Trusted Value

The trusted value can considered to be numerical quantity lying between 0 and 1 (inclusive) or between 1 and 1 (inclusive). In this paper trust value can be range as 2 for sensor network due to limited memory, transmission, and reception power.

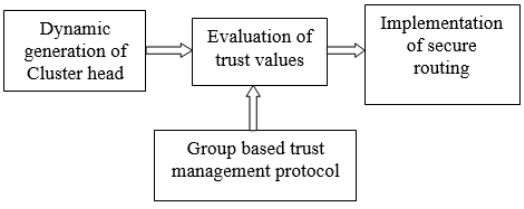

Fig. 2. Flow structure

C. Assumption

Sensor network composed of number of sensor networks, it has unique identities that are placed in open environment. Some of the sensor networks nodes do not have unique identities.

Class based addressing scheme is used to identify sensor networks and perform communication. Base station is a central command authority and it is a attacker resistant. Key management scheme can be used in order to protect trust values from traffic.

D. Trust Calculation at the Cluster Head Level

Cluster Head can be assumed as Sensor Network, it consist of memory and high computational power compared to other Sensor Networks.

1) Trust state calculation of intra group topology

To figure the trust estimation of nodes in a topology, Cluster Head requires the nodes for their trust conditions of different individuals in the topology. The trust states can be utilized rather than the correct trust esteems because of two reasons they are (I) correspondence overhead would be less, (ii) the trust limits of a node may vary from different nodes. Count of trust condition of nodes by utilizing trust states would be more efficient. The Cluster Head will exchange the packet through the topology. After this, all gathering part nodes exchange their trust states s, of other part nodes to the Cluster Head. The variable s, has two conceivable states: trusted and untrusted individually. The Cluster Head keeps up these trust states in a framework shape, as demonstrated as follows.

$$\begin{matrix} \text{T Mch} = \text{sch, 1} & \text{s1, c} & \ldots. & \text{sn, 1} \\ \text{sch, 2} & \text{s1, 2} & \ldots. & \text{sn, 2} \\ . & . & & . \\ . & . & & . \end{matrix}$$

Where TMch speaks to the trust state framework of group head, and sch, 1 speaks to the condition of hub 1 at bunch head. The worldwide trust state to a hub can be relegated by Cluster Head dependent on the relative contrast in trust states for that node. The relative difference can be explained through standard normal distribution. Then the random variable X such that

$$\text{Trust value of the node} = \begin{cases} 0, \text{ when untrusted} \\ 1, \text{ when uncertain} \\ 2, \text{ when trusted} \end{cases}$$

Expecting this as a uniform arbitrary variable, the entirety of m irregular factors as Sm. The standard typical arbitrary variable for node j,

$$Z_j = \frac{\sqrt{3\left(X\left(S_{ch,j}\right) + \sum_{i=1, i\neq j}^{m} X\left(S_{ch,j}\right) - m\right)}}{\sqrt{m}}$$

If Zjє [-1, 1], node j is termed as uncertain,
Zj> 1, it is termed as trusted,
Zj<-1, it is termed as un trusted.

The methodology is to make group heads dependent on vitality profile for secure directing in sensor systems. It requires less vitality utilization and vitality dispersal contrasted with dynamic Trust based administration plans for secure directing in remote sensor organize.50 Nodes can be created in NS-2.34 Version. Each node must have constant energy compared with other node. Node with high energy is considered as a cluster head. The trusted value can be calculated through the direct and indirect interactions. If the trusted value is 2, it can be considered as a trusted node and change in the colour of the node indicates that the node is trusted node. Packet can be transmitted from trusted node to cluster head without energy dissipation.

IV. Trust Management Scheme

Trust management scheme improves security of wireless sensor network. For sensing process, a sensor node need to trust neighboring nodes for checking malicious measurements. For routing process, a sensor node need to which other nodes to trust for forwarding a packet. This scheme is lightweight enough and to provide good performance without affecting functionality of the system.

A. Different Existing Scheme

1) Trust management for resilient geographic routing

This scheme is used for location verification and avoids attacks towards geographical routing. Trusted node provides good communication to the destination node will remain longer time. Node can constructs a routing table, it monitors the neighbouring node it forwards the packets by using overhearing techniques. The calculation of trust value takes less time. Accuracy is less and chance of false positive and false negative is high.

2) Weighted trust evaluation

This scheme is used to detect the attacked (unauthorized) nodes. It is a lightweight algorithm and it composed of little overhead. The attacked nodes provides wrong information that affects the performance of the network. Updating the weight of each sensor node has two purposes, they are (i) Sensor node is attacked and sends an inconsistent report; its weight can be decreased. If a sensor node's weight is lower than the threshold, then it can be identified as a malicious node. (ii) Weight decides how much a report can contribute to the final decision.

3) Hybrid trust and reputation management

This scheme is a combination of behavior based and certificate based approach. Both the schemes can be used to detect the trust node by calculating number of evidences from certificate authority. This paper depicts the trust calculation through direct and indirect interactions. High computational power is required for evaluating behavior and certificate validation.

International Journal of Research in Engineering, Science and Management
Volume-1, Issue-10, October-2018
www.ijresm.com | ISSN (Online): 2581-5792

V. Implementation

A. Dynamic Selection of Cluster Head

Energy of each node can be calculated, node with higher energy can be considered as a cluster head. In front end, energy parameters can be added, then the node configuration set the energy model, initial energy value, power spent in receiving mode, transmit mode, idle mode and sleep mode. Now we will move to the backend code. Our edit can be performed in aodv.cc and aodv.h.

In aodv.h, first include the following header file that contains the procedures to access node position, energy and several other functions. Declare the variables in "protected" scope.

In aodv.cc, initialize the variables that we have declared in aodv.h. This must be done in the AODV constructor. Including the code to access the function in the mobile node.h that can able to fetch the current position of nodes and energy. Incaution of code AODV::forward() function, packet can be transmitted based on the position of node and energy. Output have been redirected to file.

VI. Simulation Procedure and Discussion

VMware is a support of a Dell technologies can be used to provide virtualization and cloud computing software services. Ubuntu is an open source software operating system that runs from desktop to all internet connected networks. It can be used to provide linux distribution and able to compromise linux server. Coding can be aligned for the detection of cluster head and the value of trust nodes in the network then visit the VMware and click power on virtual machine button, after this process ubuntu is opened copy and store the coding in desktop then click application->accessories->terminal. Terminal window can be opened and the alignment of coding opens the simulation window with the formation of cluster head and trusted nodes. Then click the run button, there were 50 nodes get disseminated over the network and having sufficient energy in it. The source and destination node can be detected using the aligned coding, further it can be able to detect the malicious nodes in the network. Then the packet can be transmitted through shortest path for efficient packet transmission with less energy dissipation.

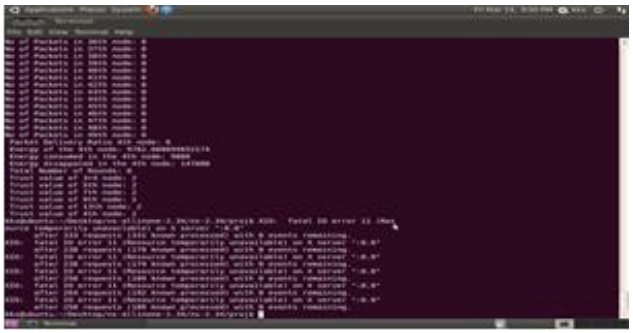

Fig. 1. Terminal window

Fig. 2. Formation of cluster and trusted nodes

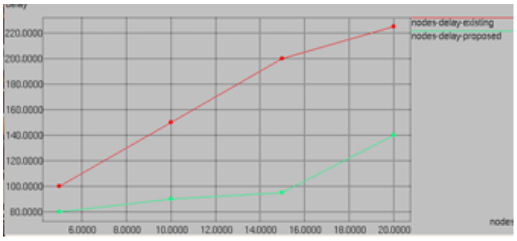

Fig. 3. Nodes delay graph

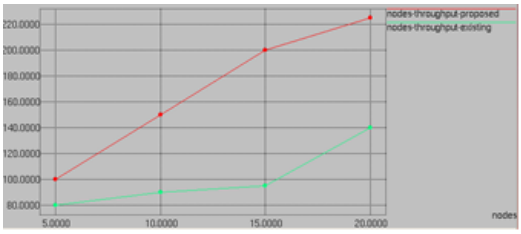

Fig. 4. Nodes throughput graph

VII. Conclusion

The objective of this project is to provide secure routing in VANET from the energy profile, where the energy of the node is given in the terminal after running the code. Energy of the node can be calculated by using function energy model. Group based trust management scheme is validated, the trust value can be calculated and displayed in the terminal and secure routing is done via trusted nodes for secure routing optimization in VANET. In future X graph will take for consideration. The X graph will obtain for cluster throughput, energy dissipated, energy consumed, total energy of the node, packet delivery ratio.

References

[1] Ning Li, Jose-Fernan Martinez-Ortega , Vicente Hernandez Diaz ,Jose Antonio Sanchez Fernandez "Probability Prediction-Based Reliable and EfficientOpportunistic Routing Algorithm for VANETs*" IEEE/ACM Transaction on networking* Vol:26, Issue:4, Year: 2018.

[2] Mohammad Wazid , Ashok Kumar Das ,Neeraj Kumar, , Alavalapati Goutham Reddy "Design of Lightweight Authentication and Key Agreement Protocol for Vehicular Ad Hoc Networks" *IEEE Access Vol:5*, Year:2017.

[3] Fanhui Zeng, Rongqing Zhang, Xiang Cheng, Liuqing Yang "Channel Prediction Based Scheduling for Data Dissemination in VANETs" *IEEE Communicaton Letters Vol:21, Issue:*6, Year:2017.

[4] Shiang-Feng Tzeng, Shi-Jinn Horng, Tianrui Li, Xian Wang, Muhmmad Khurram Khan "Enhancing Security and Privacy for Identity-basedBatch Verification Scheme in VANET" IEEE *Transaction on Vehicular Technology Vol:66, Issue*:4, Year:2017.

[5] Jun Shao, Xiaodong Lin, Rongxing Lu, and Cong Zuo "A Threshold Anonymous Authentication Protocol for VANETs" *IEEE Transactions on Vehicular Technology Vol: 65, Issue: 3*, Year: 2016.

[6] Karim Emara "Safety-aware Location Privacy in VANET: Evaluation and Comparison" *IEEE Transaction on Vehicular Technology Vol: 66, Issue: 12, Year: 2017*.

[7] Hong Zhong , Bo Huang, Jie cui , Yan Xu and Lu liu "Conditional Privacy-Preserving Authentication Using Registration List in Vehicular Ad Hoc Networks" *IEEE Access Vol:6, Year:2018.*

[8] Fengzhong Qu, Zhihui Wu, Fei-Yue Wang, and Woong Cho "A Security and Privacy Review of VANETs," IEEE *Transactions on Intelligent Vol: 16, Issue: 6, Year: 2015.*

[9] Shunrong Jiang, Xiaoyan Zhu, and Liangmin Wang, "An Efficient Anonymous Batch Authentication Scheme Based on HMAC for VANETs" *IEEE Transactions on Iintelligent Transportation System Vol: 17, Issue: 8, Year: 2016.*

[10] Jie cui, Lu wei, Jing zhang, Yan xu, Hong zhong "An Efficient Meaasge Authentication Scheme Based on Edge Computing for Vehicular Ad Hoc Network" *IEEE Transactions on Intelligent Transportation System Issue: 99, Year:2018.*