International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 3, Issue 4, April 2016

Efficient Cluster based Communication with Plausibility Checks in VANET

[1] Manisha.A, [2] Lekshmi.E, [3] Pavithra.K, [4] Muthumanickam.S
[1] Student, [2] Student, [3] Student, [4] Associate Professor
[1][2][3][4] R.M.K college of Engineering and Technology

Abstract: **-- In a Vehicular Ad Hoc Network (VANET), node trustworthiness in packet forwarding is required for the network to function properly. The trustworthiness of the messages is decided upon using sensors. Only if the event is thought to be prevalent, the trust opinion generator announces this event to the applications. First a node checks whether the event is in its own detection range. If not the decision is made on either the rule of majority or on the trust levels already assigned to the nodes. In case the event is not prevalent, the proposed algorithm also sends a malicious intent information packet in order to inform the neighbour nodes about the detection of a malicious activity. The proposed algorithm is better equipped to handle such attacks. It can detect at least such attacks if the node is itself in the detection range. It eliminates attacks pertaining to false event generation completely by utilizing the plausibility of data collected through sensors as well as the trust value of the sending nodes. The cluster based attack detection and communication is contributed. This scheme applies the attacker detection mechanism only at cluster head node hence it reduces the overhead.**

Index Terms: **-- Attack, cluster based communication, cluster head, false event, genuine event, malicious node, VANET.**

1. INTRODUCTION

Freight has been made very easy with the advent of technology but with the increase in the number of vehicles in the world, the transportation system has become inefficient. This is one of the major problems being faced by the society today. Vehicular ad hoc networks (VANET) can be used to alleviate the problems of vehicle safety as well as the traffic control and optimization. VANET as proposed consists of mobile hosts equipped with wireless communication devices and road side units (RSUs).The security in VANET is of primary concern since an attacker may try to insert or modify life-critical information. The possible misuse of VANET can create a lot of problems and difficulties especially in situations where life critical information is involved. In this paper we propose a novel way of incorporating security in VANET through a trust- based algorithm based on reputation using sensors.

II. RELATED WORK

A. Securing Vehicular Ad Hoc Networks

The author has proposed secure architecture .The architecture consists of the certification authority (CA) where each authority is responsible for a region. Each authority provides certificates to nodes registered with it as well as foreigner certificates to nodes registered with other CAs when these nodes enter its geographical boundary. A node estimates the sender–receiver distance using its own coordinates, the location in the received message and the time of flight. The authors have proposed a position verification approach, based on plausibility heuristics, which is capable of detecting position falsifications. Also pseudonyms changing leads to instability in nodes' neighbour tables which can lead to transmission faults in the next hop. To handle this, call back media access control (MAC) layer mechanism is used where the MAC layer notifies the routing layer about missed neighbours Callback media access control (MAC) layer mechanism is used where the MAC layer notifies the routing layer about missed neighbours. Misbehavior detection and local eviction of attackers by voting evaluators eliminates the attackers locally. No confidentiality for safety information Lack of periodic technical inspection, and liability identification.

B. Secure Vehicular Communications Systems: Design and Architecture

This protocol caters to the two issues, efficient authentication of anonymous safety messages and efficient tracking on the source of a disputed safety message, but makes use of infrastructure. It focuses on location privacy. The protocol is divided into four parts: system initialization, OBU short-time anonymous key generation, OBU safety message generation and sending, and OBU fast tracking algorithm, with each having a separate algorithm. The safety message is level 1 secure to the TA as it can reveal the real OBU identity. With all its merits, the question remains that of the infrastructure which involves implementation cost. Quick tracking and authentication accomplished by the request-response protocol between the OBU and the RSU thus reducing the storage space required. Power control capability of vehicles balances the trade-off between safety/liability and location privacy.

High implementation cost and design complexity. Disputed safety message increases the control overhead.

C. Secure Position-Based Routing for VANETs:
This protocol relies on asymmetric cryptography and digital signatures. When one hop communication is taken into account, only the source is required to sign the packet. The protocol proposes rate-limiting mechanisms to take into account false broadcast floods that could be injected by a malicious node and that could lead to lot of overheads and resource wastage in the network. This is achieved by setting a limit on the rate of data that can originate from a node and by providing private vehicles a much lower rate of data transmission as well as a smaller transmission area as compared to RSUs and emergency vehicles. Series of plausibility checks to ensure the correctness of information. Rate-limiting mechanisms to take into account false broadcast floods. Frequent dissemination of calculating the time difference between any two successive position updates. High routing overhead due to the mechanism of false broadcast flooding.

D. Illusion Attack on VANET Applications: A Message Plausibility Problem
In this paper, a new attack that is specific to VANETs, called Illusion attack is described and a possible solution to address this attack is proposed through a plausibility mechanism. This attack is a type of false message generation attack where the malicious node deceives the sensors in its own car to create the illusion of a false attack. Using this attack a malicious node can cause traffic jams and accidents with ease. A plausibility validation model has been proposed to secure vehicular networks. The input data is obtained by a node either through wireless antenna or through data reported by sensors. The input message is verified through a predefined rule set that is dependent on the type of messages. A number of rules have been proposed to check the plausibility of messages. These include dropping of duplicate messages. The broadcast range of messages is defined based on the type of event and this has been used to calculate the plausibility of the hop count field in a message. The timestamp of the message is checked to ensure that the message is not too old. The velocity field is checked by assuming a maximum permissible velocity. Also, the location is verified by ensuring that the distance covered by the message is greater than or equal to the distance between the positions from where the message was initiated and the current position of the receiving vehicle. If all the fields in the message pass the validation check then the message is accepted else it is discarded. Duplicate packets are identified and dropped efficient. Dissemination of false traffic messages in the network. It is not usable in face of fake events.

E. SBGR: A simple Self-Protected Beaconless
Geographic Routing for Wireless Sensor Networks
This literature proposes a Self-Protected Beaconless Geographic Routing protocol (SBGR). It is based on a simple beaconless protocol where nodes compete in a distributed way to forward the packets. This distributed forwarding is designed to prevent attackers intercepting and dropping packets. The protocol uses two different forwarding schemes: distributed and flooding .The main idea is that neighbours which detect a Sybil attacker start the dissemination of a NOTIFY message. The message is flooded within the coverage area of the potential attacker to make sure that legitimate nodes providing more progress than the false identity created by the attacker can receive the message and continue the routing task. SBGR is a beaconless routing protocol, so partially reduce the routing overhead in the network. The secure data transmission is not considered.

III. ARCHITECTURE

The self-organised cluster formed comprises of the member nodes and the clusterhead which is chosen based on the lowest mobility within a cluster. The clusterhead plays the vital role in the architecture. Occurrence of any event is reported by the member nodes to the clusterhead which then verifies if the reported event is false or genuine and then accordingly updates the trust table. In case of a false event the data is dropped and trust value of the node that reports the event is decreased while in case of a genuine event the trust value is increased and the data is disseminated within the communication range.

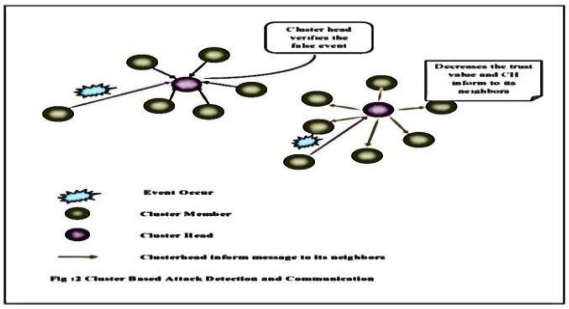


Fig I: Architecture of proposed algorithm

IV. PROPOSED ALGORITHM

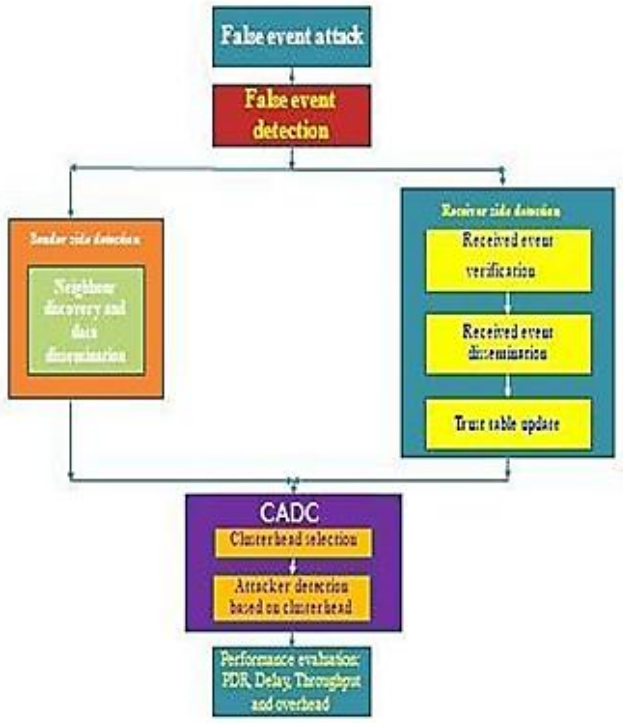


Fig II: Flowchart of proposed modules

A. Attacks in VANET and Detection of False Event in Sender
Side
False Event Generation
Input: Generation of false event
Output: Launch the attacker
False event generation is a type of attack in which a vehicle generates information about an event that actually does not exists.

Event Detection and Dissemination
Input: Event node broadcast to its neighbour node
Output: Identification of neighbour node
In sender side:
Once a node has identified an event in the detectable area using its own sensor, it has to send about the event to its neighbours. It initiates the neighbour discovery phase. In this phase, the sensing node broadcasts a neighbour request packet and waits for the neighbour reply packets with which it recognizes its neighbours. After identification of neighbours, it distributes the data to neighbours.

B. Detection of False Event in Receiver Side
Received Event Verification, Dissemination and Trust Table Update

In receiver side:
When a node receives the event information from its neighbour it carries out the following steps.
Case1: If the packet is received from outside the threshold range:
It means that it is pertaining to an event that is far away then the packet is dropped.
Case2: If the action has already been taken on that event: Then also the packet is dropped.
Case3: If the above two criteria are not met:
Then the node checks whether the event is in its detection range or not where detection range is the range of the node within which the node can detect an event.
a. If the node is itself in the detection range and it has no information about the event then the event is possibly false and it decreases the trust value of the sending node and broadcasts a malicious intent control packet.
b. If the node is itself in the detection range and it has information about the event then the event is genuine and it increases the trust value of the sending node and forwards the information to its neighbours.
c. If the node is not in the detection range but lies within the threshold range, it cannot directly sense the event and it can only get the information from its neighbours. On such condition, it will wait for some time till gets same information from any other neighbours. If any other neighbours also sending about same event information, then the event is genuine and it increases the trust value of sender otherwise it decreases the trust value of the sender.

C. Cluster based Attack Detection and
Communication Clusterhead Selection
Input: number of cluster, broadcast the RREQ and RREP
Output: selection of clusterhead based on speed
Initially each node broadcasts a request message towards all neighbours and with its id, location and speed. In neighbourhood low speed vehicle is chosen as CH selection. In this case, the CH has the least probability (when compared to others within the same cluster) to move out of the cluster

because its speed is close to the average speed of all members of the cluster.

D. Cluster based Attack Detection and Communication Attacker Detection based on Clusterhead Input: clusterhead and false event report Output: Detection of attacker based on clusterhead
In existing work the attacker node sends the false report to its neighbour nodes. On such condition, every node that receives false report will wait for some time till gets same information from any other neighbours. If any other neighbours also sending about same event information, then the event is genuine and it increases the trust value of sender otherwise it

decreases the trust value of the sender. If attacker is detected every node sends an alert message to its neighbours. It increases the overhead.

In proposed system cluster based detection scheme is followed. In this scheme the attacker node sends the false report to its clusterhead. On such condition, CH that receives false report will wait for some time till gets same information from any other members. If any other member is also sending about same event information to CH, then the event is genuine and it increases the trust value of sender otherwise it decreases the trust value of the sender. Instead of sending alert from all neighbours, CH alone sends an alert which reduces network traffic and it reduces the overhead.

E. Performance Evaluation

Packet Delivery Ratio

PDR is the proportion to the total amount of packets reached the receiver and amount of packet sent by source. If the amount of malicious node increases, PDR decreases. The higher mobility of nodes causes PDR to decrease.

PDR (%) = (Number of packets successfully delivered to destination) / (Number of packets generated)

Detection Delay

It is the average delay to detect the attacker making the attack in the network

Throughput

The amount of data successfully received at the destination. Throughput (bits/s) = Total Data / Data Transmission duration

Overhead

It is defined as the number of control packets generated during the communication

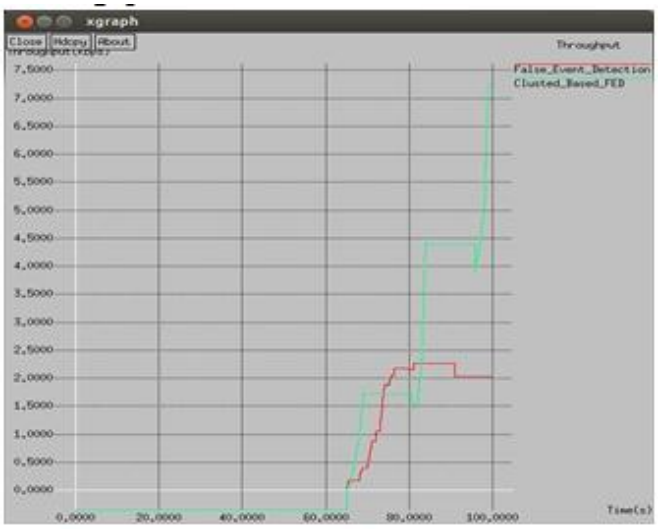
V. SIMULATION RESULTS

Both the feasibility and effectiveness of our approach are shown through a simulation that exemplifies its performance. SUMO and NS2 are the tools used for this simulation. We simulated all the four modules and generated graphs for comparing the existing false event detection and our proposed cluster based false event detection. The comparison is made with four parameters: Delay, Throughput, Overhead, packet delivery ratio.

Delay

Packet Delivery Ratio

Overhead



Throughput

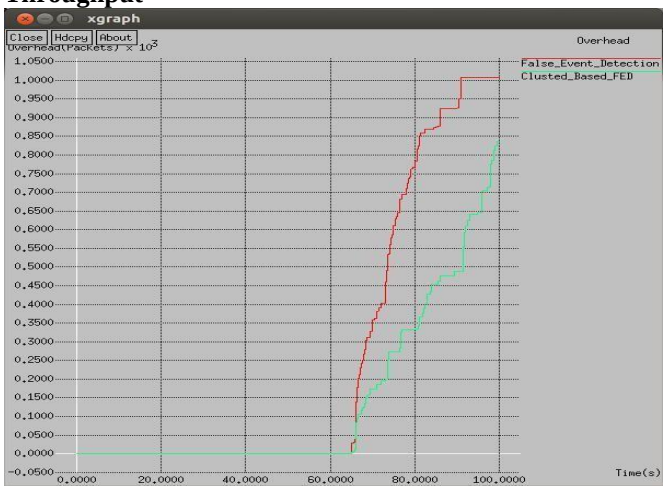


Fig III: Simulation results

On varying the time, the throughput and the packet delivery ratio have significantly increased while the delay and the overhead have drastically decreased. The cluster based false event detection scheme majorly reduces the overhead when compared to the existing false event detection scheme and provides an efficient cluster based secure communication system.

VI. CONCLUSION

Vehicular ad hoc networks (VANETs) enable vehicles to communicate with each other and with roadside units. Service oriented vehicular networks are special types of VANETs that support diverse infrastructure-based commercial services, including Internet access, real-time traffic management, video streaming, and content distribution. Many forms of attacks against service-oriented VANETs that attempt to threaten their security have emerged. The success of data acquisition and delivery systems depends on their ability to defend against the different types of security and privacy attacks that exist in service-oriented VANETs. While most of the algorithms just detect the malicious nodes, VSRP not only detects malicious activity but also eliminates the malicious nodes. VSRP is also the ideal solution to the vehicular problems of developing countries as it is infrastructure less. Since it is infrastructure less, it is more cost efficient and also does not pose the problems associated with RSUs such as the RSU becoming a bottleneck. The control overheads in VSRP are also reduced as each node forwards the data intelligently and does not work in a brute force manner by forwarding the same information from different neighbour nodes a number of times. The cluster based attack detection and communication improves the VSRP and provides an efficient and robust method to secure vehicular networks without using any infrastructure.

REFERENCES

[1] M. Raya and J. P. Hubaux, "Securing Vehicular Ad Hoc Networks", Computer Security, Vol. 15, No. 1, pp. 39–68, 2007.

[2] P. Papadimitrators, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.P.Hubaux, "Secure Vehicular Communications Systems: Design and Architecture", Communication Magazine, IEEE, Vol. 46, No. 11, pp. 100–109, 2008.

[3] C. Harsch, A. Festag, and P. Papadimitratos, "Secure Position-Based Routing for VANETs", In Proceeding Vehicular Technology Conference, pp. 26–30, 2007.

[4] N.-W. Lo and H.-C. Tsai, "Illusion attack on VANET Applications a Message Plausibility Problem", In Proceedings of 2nd Workshop Automation Network Application, pp. 1–8, IEEE, 2007.

[5] Rafael Marin-Perez, Pedro M. Ruiz, "SBGR: A Simple Self-Protected Beacon-less Geographic Routing for Wireless Sensor Networks", In Mobile Ad Hoc and Sensor Systems (MASS), IEEE Transaction and 8th International Conference, pp. 610-619, 2011.

[6] R. Lu, X. Lin, H. Zhu, and X. Shen, "An Intelligent Secure and Privacy-Preserving Parking Scheme Through Vehicular Communications", IEEE Transaction, Vehicular Technology, Vol. 59, No. 6, pp. 2772-2785, 2010.

[7] G. Calandriello, P. Papadimitratos, A. Lioy, and J. P. Hubaux, "Efficient and Robust Pseudonymous Authentication in VANET", In Proceeding Fourth ACM International Workshop in Vehicular Ad Hoc Networks, pp. 19–28, 2007.