INCREASING TRUSTWORTHINESS IN DATA TRANSFER OF VEHICULAR AD HOC NETWORKS

Divya A C[1], K Vyshnavi[2], Kusuma N[3], Revathy S[4]

[1] *BE Student, CSE, RRCE, Karnataka, India*
[2] *BE Student, CSE, RRCE, Karnataka, India*
[3] *BE Student, CSE, RRCE, Karnataka, India*
[4] *Assistant Professor, CSE, RRCE, Karnataka, India*

ABSTRACT

Vehicular ad-hoc network (VANETs) is a type of a network that is created from the concept of cars for a specific need or situation. 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. VANETs are used to transform the way vehicles travel from the creation of safe and secured exchange and use of information. VANETs are vulnerable to security threats due to increasing reliance on communication, computing and control technologies. The unique security and privacy challenges posed by VANETs include integrity, confidentiality, non repudiation, access control, real-time operational constraints, demands and privacy protection. In our system, an attack resistant trust management is used that is able to detect and cope with malicious attacks and also evaluate the trustworthiness of both data and mobile nodes in VANETs. Specially, data trust is evaluated based on the data sensed and collected from multiple vehicles.

Keyword: *Trust management, data trust, node trust, security, functionality, misbehavior detection, malicious attack, attack resistance.*

1. INTRODUCTION

In recent years, as the vehicle usage is increasing, need for safety and efficiency of road transportation system have made the manufacturers to implement wireless communications network into vehicles. These wireless networked vehicles form a Ad hoc network called Vehicular Ad hoc Networks (VANETs). In this network, vehicles transfer data messages through multi-hop paths.

Vehicular ad hoc network (VANET) is a communication between Vehicle to Vehicle (V2V) and Road side to Vehicle (R2V).The technology in VANET contains WLAN/cellular and Ad Hoc networks to achieve the continuous connectivity. The ad hoc network is put forth with the novel objectives of providing safety and comfort related services to vehicle users. Collision alert, traffic congestion alert, lane-change warning, road blockage alert (due to construction works etc.) are among the major safety related services addressed by VANET. The other comfort related services are vehicle users are equipped with Internet and Multimedia connectivity.The major challenges lies in design of routing protocol, data transfer, security and privacy,etc.

The wireless products contain remote keyless entry devices, personal digital assistants (PDAs), laptops and mobile telephones. Wireless devices and networks have become increasingly important , the need for Vehicle-to-Vehicle(V2V) and Vehicle- to-Roadside(VRC) or Vehicle-to-infrastructure(V2I) communication grows. VANETS can be used for a wide range range of safety and non-safety applications, allow for value added services such as vehicle safety, automatic toll payment, traffic management, enhance navigation, location based services such as finding the closest fuel station, restaurant or hotel and infotainment applications such as providing access to the internet.

The sensor in a vehicle detects an accident ahead, and then it reports this accident to the system. If there is no accident in any one of the scenario, the vehicle that reports accident to the system is either faulty or malicious. If the trustworthiness of the sensor data cannot be properly evaluated, then it is possible to produce traffic jams or even life-threatening road accidents because most of the vehicles will be incorrectly redirected to the same route if the fake traffic alerts remain undetected and thus effective in VANETs. Therefore, it is important to secure VANETs so that they can better support intelligent transportation applications such as TrEPS.

When compared with the old wired networks, VANETs themselves are more prone to malicious attacks because of their unique features, such as highly dynamic network topology, limited power supply and error prone transmission media. For example, the wireless communication links among vehicles are prone to both passive eavesdropping and active tampering. Moreover, there are other types of more sophisticated attacks that are difficult to detect.

Thus, it is difficult to detect and cope with malicious attacks in VANETs so that the safety of vehicles, drivers, and passengers as well as the efficiency of the transportation system can be better guaranteed. We believe that the trustworthiness of VANETs could be improved by addressing both data trust and node trust.

In this paper, an attack-resistant trust management scheme called ART is proposed to cope with malicious attacks and evaluate the trustworthiness of data as well as nodes in VANETs. In this scheme, we model and evaluate the trustworthiness of data and node as two separate measures, namely data trust and node trust, respectively. Data trust is used to assess whether or not and to what extent the reported traffic data are trustworthy and node trust indicates how trustworthy the nodes in VANETs are. Moreover, the ART scheme can detect malicious nodes in VANETs. To evaluate the performance of the proposed ART scheme, extensive experiments have been conducted. Experimental results show that the proposed ART scheme is able to accurately evaluate the trustworthiness of data and nodes in VANETs, and it is also resistant to various malicious attacks.

The major contributions are,
•First, an attack-resistant trust management scheme is studied in this paper, which can detect and cope with different types of malicious behaviors in VANETs.
•Second, the trustworthiness of traffic data (data trust) is evaluated based on the data sensed and collected from multiple vehicles.
•Third, the trustworthiness of vehicle nodes is assessed in two dimensions. The two dimensions of node trust are functional trust and recommendation trust, which indicate how likely a node can fulfill its functionality and how trustworthy the recommendations from a node for other nodes will be, respectively.
•Finally, few experiments have been conducted, and experimental results show that the proposed ART scheme can effectively evaluate the trustworthiness of both sensed data and mobile nodes in VANETs.

2. RELATED WORK

In recent years, there has been significant research interest in the topics of misbehavior detection as well as trust management for ad hoc networks.

Misbehavior Detection for Ad hoc Networks

There are four types of misbehaviors in ad hoc networks. Namely failed node behaviors, badly failed node behaviors, selfish attacks, and malicious attacks, are the types of these. These are classified with respect to the node’s intent and action. More specifically, selfish attacks are intentional passive misbehaviors, where nodes choose not to fully participate in the packet forwarding functionality to conserve their resources, such as battery power; malicious attacks are intentional active misbehaviors, where the malicious node aims to purposely interrupt network operations. The existence of selfishness and malicious behaviors has remarkably motivated research in the area of misbehavior detection for mobile ad hoc networks (MANETs).

Alternatively, there have been some attacks which primarily focus on the data that are transmitted and shared among nodes in ad hoc networks. Thus, another goal of misbehavior detection approaches is to ensure that data has not been modified in transit, that is, they should make sure that what was sent is the same as what was received. More specifically, some of the widely-studied data trust attacks are masquerading attack, replay attack, message tampering attack, hidden vehicle attack, and illusion attack.

Intrusion Detection System (IDS) is generally used for detecting various node misbehaviors in ad hoc networks. Several approaches have been proposed to build IDS probes. There is usually one IDS probe installed on each node, and each IDS probe is assumed to be always monitoring the network traffic, which is obviously not energy efficient given the limited battery power that each node has in MANETs. There is a proposed cooperative intrusion detection framework. In this framework clusters are formed and the nodes in each cluster fulfill the intrusion detection task in turn. This cluster-based approach can noticeably reduce the power consumption for each node.

Routing misbehaviors are one of the major security threats that have been extensively studied in ad hoc networks. In addition to externally intruding into ad hoc networks, an adversary may also choose to compromise some nodes in ad hoc networks, and make use of them to disturb the routing services to make part of or the network unreachable.

Trust Establishment and Management in Ad hoc Network

The main purpose of this is to assess various behaviors of other nodes and build a reputation for each node based on the behavior assessment. This can be utilized to determine trustworthiness for other nodes, and in many other ways.

Trust management system usually depends on two types of observations to evaluate the node behaviours. First is named as First-hand is the observation that is directly made by the node, and this observation can be collected either passively or actively. If a node observes its neighbors’ actions, the local information is collected passively. In contrast, the reputation management system can also rely on some explicit evidences to assess the neighbor behaviors, such as an acknowledgement packet during the route discovery process. The other kind of observation is called second-hand observation or indirect observation. Second-hand observation is normally obtained by exchanging first-hand observations with other nodes. There are disadvantages linked to it, those are related to overhead, false report and collusion.

Most of the existing trust management methods for ad hoc networks focus on assessing the trustworthiness of mobile nodes by collecting various evidences and analyzing the prior behavioral history of the nodes. However, little attention has been paid to evaluate the trustworthiness of the data shared among these nodes as well. Given that the data reliability and trustworthiness in transportation systems are extremely important as well, we aim to evaluate the trustworthiness of both mobile nodes and data in this work.

3. PROBLEM DEFINITION

All of the nodes in VANETs are equipped with the same wireless communication interface, such as IEEE 802.11p. The nodes are limited in energy as well as computational and storage capabilities.

First of all, the RSUs are assumed to be trustworthy since they are usually better protected. The connected vehicles, on the other hand, are generally more susceptible to various attacks, and they can be compromised at any time after the VANET is formed.

The adversary can be an outsider located in the wireless range of the vehicles, or the adversary can first compromise one or more vehicles and behave as an insider later. The adversary is able to eavesdrop, jam, modify, forge, or drop the wireless communication between any devices in range. The main goals of the adversary may include intercepting the normal data trans-mission, forging or modifying data, framing the benign devices by deliberately submitting fake recommendations, etc. More specifically, the following malicious attacks are considered in this paper.

Simple Attack (SA): An attacker may manipulate the compromised nodes not to follow normal network proto-cols and not to provide necessary services for other nodes, such as forwarding data packets or propagating route discovery requests. However, the compromised node will not provide any fake trust opinions when it is asked about other node’s trustworthiness.

Bad Mouth Attack (BMA): In addition to conduct simple attack, the attacker can also spread fake trust opinions and try to frame the benign nodes so that the truly malicious nodes can remain undetected. This attack aims to disrupt the accurate trust evaluation and make it harder to suc-cessfully identify the malicious attackers.

4. THE ATTACK RESISTANT MANAGEMENT

AODV protocol

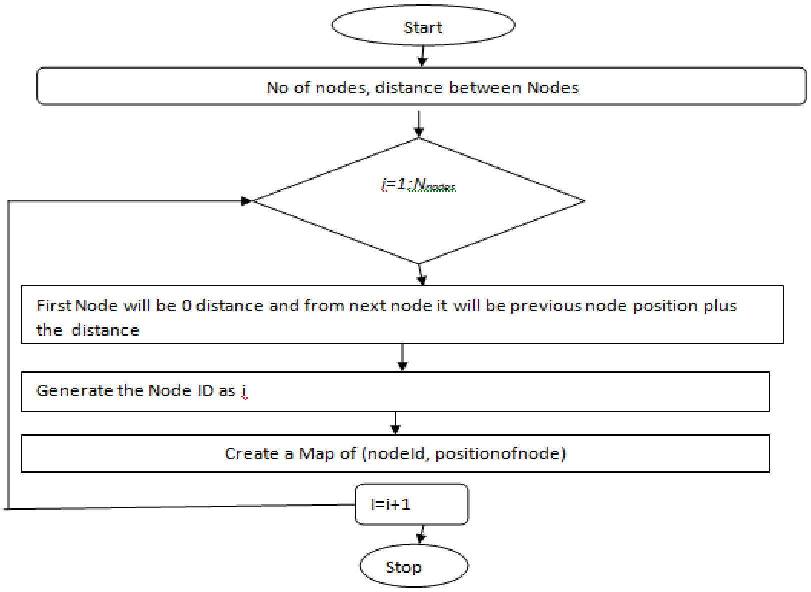
Ad-Hoc On Demand Distance Vector(AODV) protocol is needed when the source node wants to communicate with the destination node which is not in its range, it finds a route through other nodes. AODV works by using Route Request Messages(RREQ) and Route Reply Messages(RREP). If a node is not in range with a node that it wants to talk to, it sends a RREQ to its neighbors. It contains source and destination IP address and sequence number, as well as the life span of the RREQ. If the neighbor of the source doesn't know a route to the destination, it rebroadcasts the RREQ. If a neighbor does know a route to the destination, it sends a RREP back to the source. In specific, AODV is a packet routing protocol designed for use in mobile ad-hoc networks(MANET). Intended for networks that may contain thousands of nodes. Each node maintains a routing table that contains information about reaching destination nodes. There are 4 types of messages

RREP message: When a RREQ reaches a destination node, the destination route is made available by unicasting a RREP back to the source route. A node generates a RREP if it is itself the destination or if it has an active route to the destination. As the RREP goes back to the source node, intermediate nodes update their routing tables. Route Error Message: RRER are used mainly when nodes get moved around and connections are lost. If a node receives a RERR, it deletes all routes associated with the new error. Error messages are sent when a route becomes invalid, or if it cannot communicate with one of its neighbors.

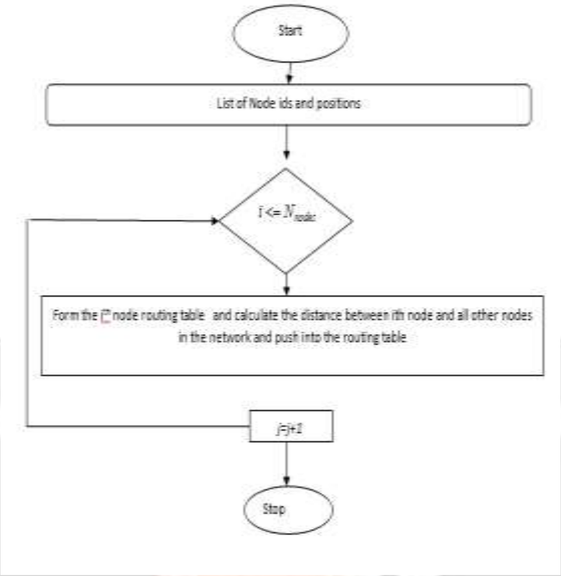
Evidence Combination

Evidence combination is very important for the proposed ART scheme. Because some of the traffic data are not reliable, it is critical to find an evidence combination technique to properly fuse together multiple pieces of evidence in presence of both trustworthy and untrustworthy data. Thus, it is necessary to combine multiple pieces of evidences so that both data trust and functional trust can be properly evaluated.

Node deployment algorithm


Start
No of nodes, distance between Nodes
i=1:Nnodes
First Node will be 0 distance and from next node it will be previous node position plus the distance
Generate the Node ID as i
Create a Map of (nodeId, positionofnode)
I=i+1
Stop

Routing Table Formation Method


Start
List of Node ids and positions
i <= N_{node}
Form the i^th node routing table and calculate the distance between ith node and all other nodes in the network and push into the routing table
j=j+1
Stop

5. SYSTEM DESIGN

The implementation phase of any project is the most important phase as it gives the final solution and solves the problem immediately. The implementation phase involves the actual materialization of the ideas, which are expressed in the analysis document and developed in the design phase. Implementation should be perfect process of the design document in a suitable programming language in order to achieve the necessary final product. Often the product is ruined due to incorrect programming language chosen for implementation or unsuitable method of programming.

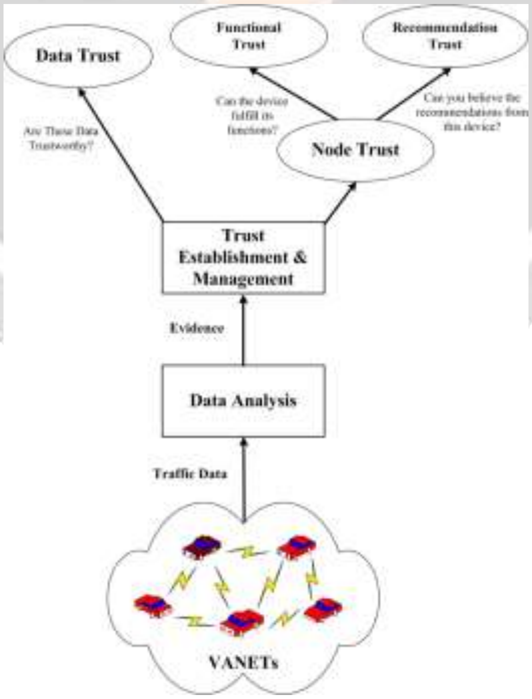

Data Trust
Functional Trust
Recommendation Trust
Can the device fulfill its functions?
Can you believe the recommendations from this device?
Are These Data Trustworthy?
Node Trust
Trust Establishment & Management
Evidence
Data Analysis
Traffic Data
VANETs

Fig-1: System Design

Topology Module

This section contains description of functionality of the scripts used in building topology. This module involves building Wireless Network topology, topology consisting of mobile nodes, each node working with multiple channels.

This module consists of following steps:

- Setting up Wireless Network Topology: This includes environmental settings, node configuration, and topology creation.
- Setting the bandwidth and threshold: Each and every node in the network topology will be assigned with certain bandwidth and topology.
- Identifying the neighbors: In order to identify the neighbors for a particular node Euclidian distance concept is used.
- Specifying the data transmission through single and multi hop: From which node the data has to be sent and which node must receive the data will be specified. Also how much amount of data has to be sent along with the time interval of sending the data will be specified.
- Specifying the simulation start time and end time: In NS 2 the entire transaction takes place within fraction of seconds. The transaction can be viewed through the NAM window at any time. For this the simulation start time and end time will be specified.

6. CONCLUSION

In this paper, a management scheme called Attack Resistant Trust management is proposed to evaluate the trustworthiness of both traffic data and vehicle nodes for VANETs. In the ART scheme, the trustworthiness of data and nodes are modeled and evaluated as two separate measures, namely data trust and node trust, respectively. In particular, data trust is used to assess whether or not and to what extent the reported traffic data are trustworthy. On the other hand, node trust indicates how trustworthy the nodes in VANETs are. To validate the proposed trust management scheme, extensive experiments have been conducted, and experimental results show that the proposed ART scheme accurately evaluates the trustworthiness of data as well as nodes in VANETs, and it can also cope with various malicious attacks.

7.REFERENCES

[1] G. Engoulou, M. Bellache, S. Pierre, and A. Quintero, “VANET secu-rity surveys,” *Comput. Commun.*, vol. 44, pp. 1–13, May 2014.

[2] M. Kakkasageri and S. Manvi, “Information management in vehicular ad hoc networks: A review,” *J. Netw. Comput. Appl.*, vol. 39, pp. 334–350, Mar. 2014.

[3] B. T. Sharef, R. A. Alsaqour, and M. Ismail, “Vehicular communication ad hoc routing protocols: A survey,” *J. Netw. Comput. Appl.*, vol. 40, pp. 363–396, Apr. 2014.

[4] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, “A com-prehensive survey on vehicular ad hoc network,” *J. Netw. Comput. Appl.*, vol. 37, pp. 380–392, Jan. 2014.

[5] M. Raya and J.-P. Hubaux, “Securing vehicular ad hoc networks,”*Comput. Security*, vol. 15, no. 1, pp. 39–68, Jan. 2007.Y. Lin and H. Song, “DynaCHINA: Real-time traffic estimation and pre-diction,” *IEEE Pervasive Comput.*, vol. 5, no. 4, pp. 65–65, Oct.–Dec. 2006.

[6] J. Angwin and J. Valentino-Devries, Apple, Google Collect User Data, Apr. 2011. [Online]. Available: http://www.wsj.com/articles/ SB10001424052748703983704576277101723453610

[7] Waze Mobile, Free Community-Based Mapping, Traffic & Navigation App. [Online]. Available: https://www.waze.com/