A Trust Management Scheme for Securing Transport Networks

E. Harika
Department of CSSE
Andhra University
Visakhapatnam

Ch. Satyananda Reddy
Department of CSSE
Andhra University
Visakhapatnam

ABSTRACT
VANET (Vehicular Adhoc Network) a wireless communication network between the vehicles without the need for any network administrator and network infrastructure. Wherein the recent years exchanging information, security and privacy are the most important concerns. To increase the efficiency of road transportation, automobile manufacturers integrated wireless networking into vehicles called VANETS. Vehicular information provided by the different vehicular nodes in the wireless network should be trustworthy all the times. Due to the different attacks possible in the VANET, some nodes may possibly act as malicious. These malicious nodes are handled on the way towards secure and reliable data. In this paper Fuzzy logic trust model is proposed to deal with uncertainties, unreliable, inaccurate and imprecise information collected by vehicles in the VANET. It conducts a series of security checks to make sure of the correctness of information from the authorized vehicles.

Keywords
VANET (vehicular Adhoc Network), RSU (Road Side Units), IDS (Intrusion Detection System), security, privacy, ART (Attack Resistant Trust Management), fuzzy decision making logic.

1. INTRODUCTION
A Vehicular ad-hoc network (VANET) is a self-configuring [1] infrastructure less mobile network where devices are connected by wireless links. In these, dynamic nodes in the networks communicate with one another share and exchange information between other nodes. As the vehicular nodes increases the network between the nodes also increases. Vehicular nodes exchange information among the nodes within its communication range and act accordingly.

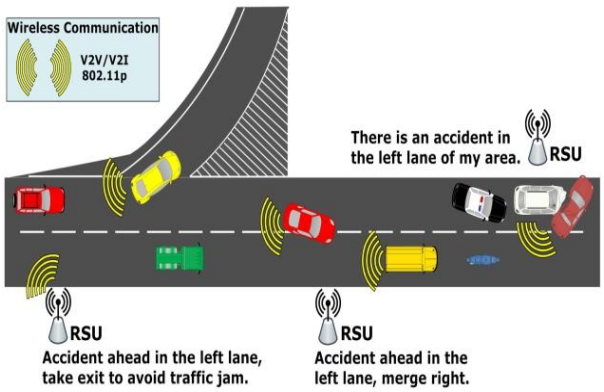


Fig1: Transport Network

1.1 Misbehaviour Detection
VANETs are used in finding traffic information and shortest routes etc.In some scenarios information collected from vehicular nodes within its range may not be same, some mobile nodes act in such a way that we could not get correct information. Some information sent by some nodes may be misleading due to some attacks. These nodes are considered as malicious nodes. The distinctive security and privacy challenges displayed by VANETs include integrity, confidentiality, no repudiation, access control, real-time operational constraints demands, availability, and privacy protection. Vehicles and roadside units are equipped with sensing, processing and wireless communication capabilities. It helps in data sharing among the mobile nodes in the same network services.VANETS are provided with GPS system through which we can send the updates regarding the current traffic conditions.

Security is an essential thing for ad hoc networks [10], mainly for individual's security-sensitive purposes. To protect an ad hoc network, VANETs suppose to have the following characteristics: accessibility, privacy, integrity, verification, and non-repudiation.VANETs are vulnerable to security threats mainly due to dynamic network topology, limited battery power, transmission media .Various mobile nodes participate in the network where some nodes are malicious. These behaviors may be like agreeing to send the data and later failing to do so. These nodes may be selfish, overloaded or broken. Selfish nodes do not spend its resources like CPU cycles, buffer space, battery life and network bandwidth in forwarding packets and it wants other nodes to do its job. Overloaded nodes always lack resources to forward packets. Broken nodes have issues with software and they can't forward packets. Misbehavior detection copes up with this type of behavior in order to maintain vehicle and driver safety and to provide better transportation. One solution to these untrustworthy nodes is to forward the packets from the nodes which has trust relationships.

Misbehaviors are general behaviors which deviate from normal behaviors. Types of misbehaviors may be: Failed node behaviors, badly failed node behaviors, selfish attacks, and malicious attacks. These are passive and active misbehaviors mostly possible in Adhoc networks. These misbehaviors are classified with respect to the node's intent and action. The masquerading attack, replay attack, message tampering attack, hidden vehicle attack, and illusion attack are some attacks which mainly focus on the data that are shared, transmitted nodes in Adhoc networks. Thus another goal of detection approach 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.

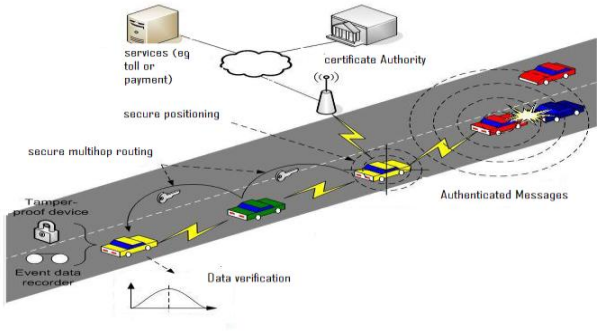


Fig 2: Certificate Authentication

Fuzzy logic is a good solution for the detection of malicious nodes drawback, instead of continuous checking and correcting every node. Proposed trust model detects malicious nodes or fault nodes in the vehicular network by applying fuzzy logic to get trust level of each node. It is obtained by categorizing plausibility and experience level of the sender based on the extracted data. Eventually, it measures the accuracy of the event messages by applying this method to the obtained data .Thus, decision-making fuzzy algorithm decides whether to accept the data from the sender or not.

Steps to getting the trust level of each node 1) Authentication of the node 2) Lifetime checking 3) Experience of node measurement.

The Malicious node can be identified if data sent is invalidated by the validation algorithm. In addition to that, there are some research areas which aim to enhance the security, trust, and privacy of VANET. Most of the existing trust management methods for ad hoc networks mainly target on appraise of trustworthiness of mobile nodes by collecting different shreds of evidence and analyzing the behavioral history of the nodes.

Some of the existing trust management methods are described in the related work.

2. RELATED WORK

The goal of trust management is to verify the actions of other nodes and build a reputation for each node based on the evaluation of the node. This type of reputation can be used to determine the trustworthiness of each node. The trustworthy--ness can be used to make decisions on which nodes should cooperate with, or even punish an untrustworthy node if needed. Observations are made from the direct and indirect trust. Direct trust or firsthand observations obtained from a node by itself, whereas indirect or second hand observation is taken from other nodes. In VANETs, direct trust always cannot provide detailed evaluation of the target node due to external circumstances such as channel conditions, temporary unavailability, interference etc. But indirect trust can always be used to provide secondary information which helps to evaluate the actual trustworthiness of the target node .The presence of nodes which have selfish and malicious behaviors has remarkably motivated in the area of misbehavior detection for mobile ad-hoc networks.[17]

IDS(Intrusion Detection System)is a good solution for finding misbehavior nodes.IDS is proposed by Y.Zhang and W.lee,which is used in detecting diverse misbehaviors of nodes in an ad-hoc network. An Absence of infrastructure made many methods proposed to build an IDS PROBE in each node.

When it is fixed with these IDS, PROBE will continuously monitor network traffic; the problem in here is due to continuous monitoring of network leads to battery power lost. To avoid this case, Huang proposed Cooperative intrusion detection framework with clusters, nodes in each cluster performs IDS task by which power consumption is reduced in every node. Routing misbehavior is other security issue which is studied in the ad-hoc network in an effort to compromise a few part or entire part of the community, some adversary is intruded into the ad hoc network. Marti et al. delivered two applicable techniques, particularly watchdog and path rater, so as to locate and segregate misbehaving nodes, which don't forward packets. There are many other answers, but the main goal is to detect discrete routing misbehaviors. As VANET is wireless community related, distinct computing devices deployed in automobiles keeps calling for monitoring current conditions.

In Buchegger et al.[5] projected the CONFIDENT protocol to encourage the node cooperation and punish misbehaving nodes. Michiardi et al. have given a mechanism with the name CORE to spot selfish nodes, and so compel them to work within the following routing activities. Patwardhan studied an approach within which the name of a node is set by information validation. In our previous analysis Li and Finin, Li Parker projected a multi-dimensional trust management theme for MANETs. During this framework, the trustiness of a node is judged from completely different views (i.e., dimensions), and every dimension of the trustiness comes from varied sets of misbehaviors in keeping with the character of these misbehaviors.

CONFIDANT (Cooperation of Nodes, Fairness in Dynamic Ad-hoc Networks), to encourage the node cooperation and punish misbehaving nodes. A possible disadvantage of CONFIDANT is that an attacker might deliberately spread false alerts to alternate nodes that a node is misbehaving while it is truly a well-behaved node. Therefore, it is vital for a node in CONFIDANT to validate an alert it receives before it accepts the alert. Whereas CONFIDANT permits nodes exchange each positive and negative observation of their neighbors, only positive observations are exchanged amongst the nodes in the CORE. In that way, malicious nodes cannot spread faux charges to frame the well-behaved nodes, and consequently avoid denial of service (DoS) attacks toward the well-behaved nodes. However, very little attention has been paid to evaluate the trustworthiness of the information shared among these nodes similarly. Providing the information reliability and trustworthiness in transportation systems is extremely important as well. The main aim here is to evaluate the trustworthiness of each mobile node.

3. PROBLEM ANALYSIS

VANETs are vulnerable to threats due to increasing reliance in communication, computing and control technologies. Most of the existing trust management methods for ad hoc networks focus on assessing the trustworthiness of mobile nodes by collecting various evidence 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. Trust management schema used in many approaches, although it was the best approach but has some disadvantages such as representing incomplete knowledge, belief updating, and evidence pooling. If partial knowledge is encoded and updated by belief function methods, the resulting

beliefs cannot serve as the basis for rational decisions.

4. PROPOSED SYSTEM

The proposed model maintains integrity and accuracy by performing fuzzy logic. After receiving information from the other vehicles first it verifies authentication of the sender by evaluating the sender node. Next, it checks lifetime of the node by calculating the difference between current time and generation time by applying fuzzy logic. The Accuracy of the location of the event is also taken into consideration. Next, it evaluates the trust based on experience and plausibility. Decision-making module decides whether the event is acceptable or not.

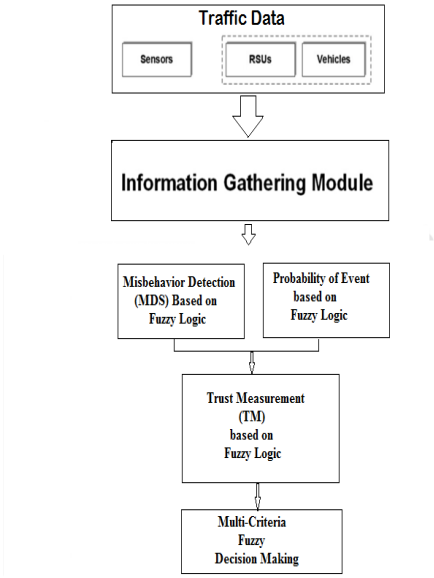


Fig 3: Fuzzy logic analysis

ID authentication helps to avoid certain conditions like congestion, fake information, and illusion. It evaluates sender of event message whether it is authorized or not. Once the ID authentication is executed avoiding specific attacks, such as impersonation and fake nodes, will be simple tasks. Next, identification of life of a message. New message is more reliable than old or expired, lifetime is identified by taking difference between event time(TimeE) of the message and current time (Timecurrent).Using these, the system calculates Time threshold.

For the life time of a message:

Input s(*Msg*, *Time current*, *Type event*)
Timediff = **Calculate-Difference** (*Timecurrent,TimeE*)
Timethreshold= **Extract-Threshold-Time** (*Typeevent*)
if *Timediff* > *Timethreshold* **Then**
Discard Event message
else
Go to next step

For exp measured as sender reliable:

if *EXPcurrent* is Low **then**
EXPnew = (*EXPcurrent -Minl*) +*Minm*
if *EXPcurrent* is Medium **Then**
EXPnew = (*EXPcurrent -Minm*) +*Minh*
if *EXPcurrent* is High **then**
EXPnew = *EXPcurrent* + α (1 -*EXPcurrent*)
if *EXPnew* > 1 **then**
EXPnew = 1

For exp measured as sender un reliable:

if *EXPcurrent* is High **then**
EXPnew = (*EXPcurrent -Minh*) +*Minm*
if *EXPcurrent* is Medium **Then**
EXPnew = (*EXPcurrent -Minm*) +*Minl*
if *EXPcurrent* is Low **then**
EXPnew = *EXPcurrent* + β (1 -*EXPcurrent*)
if *EXPnew* < 0 **then**
EXPnew = 0

To evaluate the Plausibility Level of Sender:

Input (*Msg*)
LVoD = **Location Verification of SENDER** (Distance)
LVoT = **Location Verification of SENDER (Time)**
PLAUS*Level* = **Fuzzy-DM** (fuzzify (LVoD),fuzzify(LVoT))

Output (PLAUSLevel*)*

Experience of the node is also identified by performing fuzzy logic.Experience measurement is based on nodes past interactions. The range of values obtained will be EXPV(w)=0,1 indicates whether the node v trusts or distrusts node W, Experience(Low, Medium, and High) based on positive increment value and negative decrement value *Minl,Minm,Minh* is 0, 0.3, and 0.6 respectively.

Plausibility is also identified based on location and position verification of the sender, the correctness of the information identified by distance and time. Distance between the sender and receiver is identified by GPS information and radio frequency strength. After location information is correct, time verification of expected received message time is also calculated. Suppose when node *W* sends a message to *V* at time t1 and node *V* received the message at time *timerec* .It is expected that node *V* received the message at *timeexp* that is measured using the following.

$$\text{Distance}_{GPS} = \sqrt{|xv-xw|^2 + |yv-yw|^2}$$

$$\text{Time}_{exp} = t1 + \frac{Dist\ (Vt2, Wt1)}{C_{(c=3*10\hat{}8)}}$$

Upon getting the input variables, it is divided into three fuzzy sets (low, medium, high).Based on the obtained parameters if –then rules used to define trust level of the nodes. The Final step of defuzzication is also used to identify trust level. It is also called as centroid defuzzication technique.

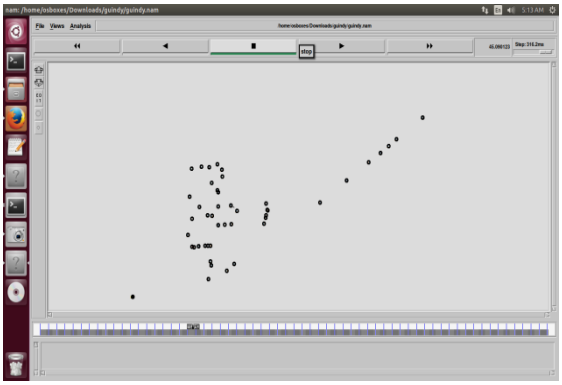
$$Trust\ level = \frac{\int x_i.\mu\ (x_i)}{\int \mu\ (x_i)}$$

U (x_i) and x_i is aggregated membership function and fuzzy value.

5. RESULTS

In the proposed system, NS2 is used as a simulation platform. The fuzzy decision making gives good approach to finding the malicious nodes.

Results show that the proposed model shows better performance accuracy and integrity.



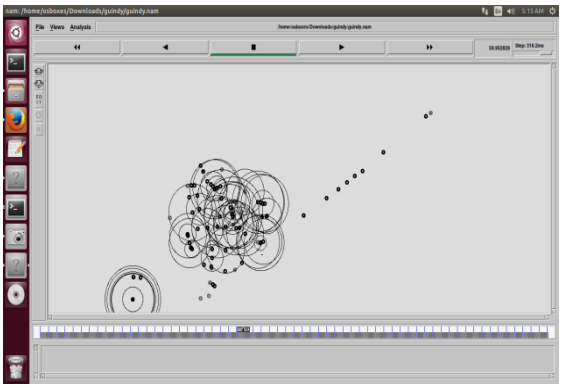


Fig 4: Transmission of data between nodes

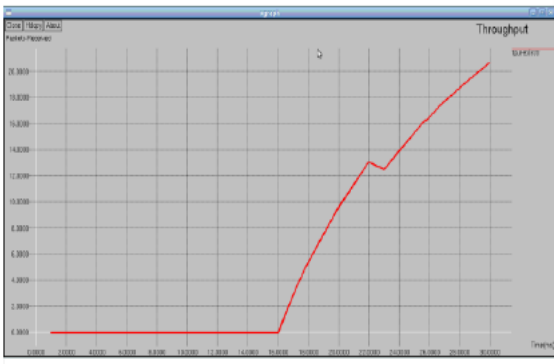


Fig 5: Graph showing Throughput

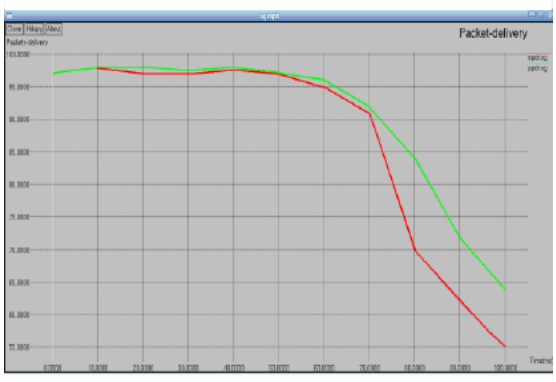


Fig 6: Graph showing packet delivery

6. CONCLUSION

VANETS always suffer from false reports and continues collision. So that providing accurate results regarding traffic updates has become a challenging task. In the proposed paper, the trustworthiness of data and nodes are improved by fuzzy decision making logic. Fuzzy reasoning models have a number of rules based on if-then conditions. In fact, these rules are easy to learn, use and can be modified according to the situation. Our model performs series of tests to give correctness and accuracy of information. This proposed model not only detects malicious nodes but also handles uncertainty and imprecision of data in the vehicular ad-hoc network in both lines of sight and nonline of sight.In addition usage of fog nodes improve accuracy level. Since usage of fog nodes may not be available anytime, so it is not used in the proposed system.

7. REFERENCES

[1] R. G. Engoulou, M. Bellache, S. Pierre, and A. Quintero, "VANET security 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 comprehensive 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,"*J. Comput. Security*, vol. 15, no. 1, pp. 39–68, Jan. 2007.Brown, L. D., Hua, H., and Gao, C. 2003. A widget framework for augmented interaction in SCAPE.

[6] Y. Lin and H. Song, "DynaCHINA: Real-time traffic estimation and prediction,"*IEEE PervasiveComput.*, vol. 5, no. 4, pp. 65–65, Oct.–Dec. 2006..

[7] J. R. Douceur, "The sybil attack," in *International Workshop on Peerto-Peer Systems*, ser. Lecture Notes in Computer Science, P. Druschel,F. Kaashoek, and A. Rowstron, vol. 2429. Berlin, Germany: Springer-

[8] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demandrouting protocol for ad hoc networks," in *Proc. 8th Annu. Int. Conf.MobiCom Netw.*, Atlanta, GA, USA, 2002, pp. 12–23.

[9] S. Buchegger and J.-Y. Le Boudee, "Self-policing mobile ad hoc networks by reputation systems," *IEEE Commun. Mag.*, vol. 43, no. 7, pp. 101–107,Jul. 2005

[10] P.-W. Yau and C. J. Mitchell, "Security vulnerabilities in ad hoc networks," in Proc. 7th Int. Symp. Commun. Theory Appl., 2003,pp. 99–104.

[11] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Veh. Commun.*, vol. 1,no. 2, pp. 53–66, Apr. 2014.

[12] J. Molina-Gil, P. Caballero-Gil, and C. Caballero-Gil, "Aggregation and probabilistic verification for data authentication in VANETs," *Inf. Sci.*,vol. 262, pp. 172–189,Mar.2014.25822589,ISSN00313203,10.1016/j.patco

g.2010.01.008.

[13] Y. Lin and H. Song, "DynaCHINA: Real-time traffic estimation and prediction,"*IEEE PervasiveComput.*, vol. 5, no. 4, pp. 65–65, Oct.–Dec. 2006..

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

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

[16] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks,"*J. Comput. Security*, vol. 15, no. 1, pp. 39–68, Jan. 2007.Brown, L. D., Hua, H., and Gao, C. 2003. A widget framework for augmented interaction in SCAPE.

[17] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks,"in Proc. ACM 6th Annu. Int. Conf. MobiCom Netw., Boston, MA, USA,2000, pp. 275–283.